## Rizika sociálních sítí – upozornění pro rodiče

**V posledních letech zažívají sociální sítě obrovský boom a výrazně tak přispívají k proměnám společnosti. Tyto proměny se týkají zejména mladých uživatelů, kteří s oblibou sociální sítě využívají. Často tak mezi mladými platí tvrzení, že kdo není na Facebooku, jako by nebyl.**

Nutno podotknout, že v souladu s podmínkami užívání Facebooku musí být uživateli 13 a více let. **České děti začínají s Facebookem již ve věku 10–11 let.** Pokud si tedy tyto mladší děti zřizují účet na Facebooku, vědomě při registraci uvádí nepravé údaje a jednají v rozporu s podmínkami užívání této služby. Mladí často také využívají více profilů současně nebo zakládají profily druhým, ať už fiktivním či reálným osobám, a to z rozličných důvodů.

V České republice je dále z nadnárodních sociálních sítí mezi mladými populární také [**Twitter**](https://twitter.com/), [**Google+**](https://plus.google.com/collections/featured), [**Instagram**](https://www.instagram.com/), [**Ask.fm**](https://ask.fm/) a [**Badoo**](http://badoo.com/cs/). Tyto služby však vykazují řádově méně uživatelů než dominantní Facebook. V poslední době mezi mladými zažívá rozmach aplikace na mobilní telefon s názvem **WhatsApp**, která nahrazuje SMS zprávy a využívá tak zasílání krátkých zpráv prostřednictvím mobilního internetu.

Na sociálních sítích se pohybujeme ve virtuálním světě, kde platí jiná pravidla než pro svět reálný. Platí zde jiné pojetí času a prostoru (viz příklad Libimseti.cz, kde i přes smazání fotografií z vlastních alb tyto fotografie již kolují po internetu po neomezeně dlouhou dobu a v neomezeném prostoru). Lidé se také ve virtuálním světě mohou chovat jinak než ve světě reálném. Mohou využívat i technických možností internetu (oslovit řadu uživatelů současně, využívat nedostatky technického zabezpečení a získat tak osobní a citlivá data, která mohou být následně zneužita).

**Mezi nejzranitelnější skupiny patří zejména děti a mládež.** Mají často nižší smysl pro zodpovědnost a ne vždy si mohou uvědomit různé důsledky. Méně také řeší otázky soukromí a v tomto ohledu **odpovídající nastavení profilu**. Častým případem je, že řada dětí sahá po nastavení soukromí, až když si je chce do přátel přidat jeden z rodičů. Potomek tak bývá zděšen, že rodič uvidí fotky a komunikaci s kamarády a že ho touto formou bude špehovat. Děti tak často neřeší ochranu svých dat vůči neznámým osobám, ale právě vůči rodičům.

**Mladí také tolik neuvažují nad tím, zda je informace o nich zveřejněné nemohou poškodit v budoucnosti například při hledání zaměstnání.** V dnešní době je již běžné, že personalisté si prověřují uchazeče nejen podle zaslaného životopisu, ale vyhledávají informace o uchazeči komplexně, a to právě za pomoci sociálních sítí. Je tedy namístě myslet na zlaté pravidlo „dvakrát měř a jednou řež“ a rozmyslet si možné důsledky nejen pro daný moment, ale i z hlediska budoucího života.

Problémem je také samotná obranyschopnost dítěte. **Děti často vstupují do světa sociálních** **sítí nadšené. Nechají se jimi pohltit.** Setkání se s něčím negativním může dítě vysoce poznamenat po psychické stránce. Dochází tak k jakési ztrátě iluzí a tvrdému dopadu na dno. Děti bývají na internetu rovněž vyhledávanou komoditou pro jisté skupiny lidí, proti kterým se častou nedokážou efektivně bránit, či se vlastní vinou dostanou do svízelné situace.

**Chyby někdy bohužel pramení i z nedostatečného přístupu rodičů. Pokud dítě dostane nové kolo, rodiče si spíše ověřují, zda dítě může vyrazit do provozu na silnici. V případě nového počítače se způsobilost dítěte k jeho používání neprověřuje až tak často. Rodiče bývají naopak rádi, že dítě je doma, v bezpečí, a ne na nebezpečné ulici. Paradoxně tak může vzniknout situace, kdy se rodič zeptá dítěte: „Co děláš na tom počítači?“ Odpověď může být: „Povídám si s kamarádkou.“ Rodič je klidný. Jenže dítě rodiči nesdělí, že se jedná o novou kamarádku nalezenou přes internet, se kterou se má zítra poprvé sejít. Bohužel ne vždy nová kamarádka musí být čtrnáctiletá dívka z vedlejší ulice, může jít například o padesátiletého pána, který se za mladou dívku vydává. Dítě tak ve skutečnosti doma u počítače v bezpečí není.**

### Kybergrooming - s názvem kybergrooming**, kdy se jedná o manipulaci nejčastěji s dětskou obětí za účelem sjednání schůzky a následného sexuálního zneužití** **či ublížení na zdraví**. Kybergrooming je jednou z metod takzvaného sociálního inženýrství (způsob manipulace lidí za účelem provedení určité akce nebo získání informace), kdy na základě falešné identity, která je pro oběť atraktivní, je oběť manipulována a zpracovávána.

**Co by měli vědět rodiče?**

Rodič by měl především své dítě upozornit na možné hrozby, že ne vždy se dítě může setkat s někým, koho opravdu potkat chce. Nabádat děti k opatrnosti a být především oporou. Zde je pouhá restrikce spíše kontraproduktivní. Při restrikci s největší pravděpodobností dítě začne vše tajit. Z obou stran je tedy otevřený vztah základem.

### Kyberšikana - **je šikana realizovaná prostřednictvím moderních informačních technologií.** Nutno podotknout, že jde o dlouhodobou činnost. Pokud tedy o vás někdo napíše na sociální síti nelichotivý příspěvek, je to jeho názor. Jestliže v tomto jednání dále pokračuje s cílem vás zdiskreditovat a uškodit vám, jedná se již o kyberšikanu.

**Co by měli vědět rodiče?**

Základem je opět otevřený vztah s dítětem, kde dítě nalezne v dospělém oporu. Rodič by celou věc měl řešit taktně a ve vší diskrétnosti. Častou chybou bývá, že rodiče oběti mají snahu vše řešit s rodiči útočníka. Nedoporučuje se z důvodu, že rodič útočníka se k dané věci může stavět odmítavě, popřípadě může promluvit s útočníkem. Oběť tak může být následně označena za „práskače“ a vše tak může být ještě horší. Kyberšikana je velice závažný jev a je namístě celou věc řešit například s výchovným poradcem či psychologem. Při vzniku závadného obsahu na internetu by rodič měl s dítětem spolupracovat na jeho odstranění, viz níže.

**Kyberstalking neboli nebezpečné pronásledování oběti prostřednictvím moderních informačních technologií** se může objevit například při nevydařeném vztahu. Oběť je tak sledována kupříkladu prostřednictvím sociálních sítí, e-mailu a SMS. Dochází k bombardování různými vzkazy, často ke zneužití například citlivých fotografií a videí, které si pár vyměňoval v průběhu vztahu.

**Co by měl vědět rodič?**

Opět budeme apelovat na otevřený vztah dítě–rodič. Rodič by celou věc měl řešit s rozvahou a s ohledem na psychiku dítěte. Měl by být dítěti oporou a spolupracovat například při odstranění  poškozujícího obsahu z internetu. Rodič by měl dítěti vysvětlit, jak kyberstalking může být nebezpečný, a probrat s dítětem všechny možné další hrozby. V případě ohrožení dítěte je na místě kontaktovat policii. Kyberstalking může být klasifikován jako trestný čin Nebezpečné pronásledování dle §354 Trestního zákoníku ([zákon č. 40/2009 Sb., trestní zákoník](http://www.sancedetem.cz/srv/www/content/pub/cs/odborna-knihovna/zakon-c-402009-sb-trestni-zakonik-6670.html)).

### Sexting - samotné slovo „sex“ je jedno z nejpopulárnějších slov vyhledávaných na internetu. **Pojem sexting souhrnně označuje sdílení textového či audiovizuálního obsahu se sexuálním podtextem.** Právě děti dnes objevují svou sexualitu velice brzy a nebojí se k tomu využít i moderních informačních technologií. **Sexting může být velmi nebezpečný, protože takto poskytnutý obsah může být zneužit, a to ať už v rámci nepodařeného vztahu (viz kapitola kyberstalking), nebo i osobou, která vyloženě s dítětem komunikuje s cílem získat takový materiál.**

Děti, které si takto chtějí vydělat, si často stanovují hranice typu „do spodního prádla, ale dále už ne“. „Klient“ se samozřejmě nespokojí jen s fotkami ve spodním prádle a začne dítě dále zpracovávat. **Děti si často dostatečně nechrání své soukromí.** Může tak dojít k podobné situaci: „Jestli mi nepošleš více, našel jsem si Tě na Facebooku a to, co si tady píšeme, pošlu tvým rodičům, ať vidí, co tu děláš.“ Dochází tím přímo k vydírání a hranice se lehce může posunout i za již zmiňované spodní prádlo a celý problém tak může eskalovat a nešťastně skončit.

**Internet a sociální sítě jsou také místem, kde mladí hledají reálný sex za úplatu.** Častější nabídky jsou od dívek. Chlapci přijímají nabídky spíše pasivně. Virtuální sex přes webkameru za úplatu je rovněž velmi populární. Dívky nabízejí za úplatu předvedení se při masturbaci. Chlapci jsou spíše lákáni, že si virtuálně užijí s dívkou přes webkameru. Zde nastupuje opět fakt, že ona dívka na druhé straně může být pouze falešná videosmyčka (viz webcam trolling) a chlapec tak může být manipulován pomocí chatu, aby předvedl to, co předvádí dívka, a podobně. Video chlapce tak může být druhou stranou nahráváno a následně zneužito. V takovém případě se už dostáváme do trestní roviny.

**Co by měl vědět rodič?**

Důležité je opakovaně nabádat dítě k obezřetnosti a vysvětlit mu možná rizika. Rodič by měl také důsledně dbát na zabezpečení počítače z hlediska ochrany dětí před věkově nepřiměřeným obsahem pomocí nástrojů rodičovské kontroly především u menších dětí.

### Podvody a další trestná činnost

Internet a sociální sítě jsou rovněž místem, kde se všichni z nás mohou setkat s řadou podvodů a různorodou trestnou činností. **Pro mladé uživatele je jednou z nejdůležitějších oblastí problematika ochrany osobních a citlivých údajů a jejich následného zneužití.**

V úvodu článku jsme již zmínili, jak problematická mohou být metadata a jak mohou být pozvánkou pro nezvané hosty. Určitě tak **není vhodné, aby děti například na Facebook psali svou adresu** a na svou stěnu vložili příspěvek typu „Patnáctého odjíždíme s celou rodinou na týden k moři“.

Doby, kdy se byty a domy vytipovávaly k vykradení pomocí sušenky pod rohožkou a zvonění na zvonek, jsou již dávno pryč. **Ochrana osobních a citlivých údajů je tedy na prvním místě.**

Mezi další podvodné jednání, které využívá především prostředí sociálních sítí, patří phishing a pharming a obecně malware.

**Co by mělo vědět dítě?**

V první řadě **nedůvěřovat, ale prověřovat**. Pokud si neví rady, zkusit vyhledat informace na internetu, probrat danou věc se zkušenějším kamarádem, s rodiči. Důsledně chránit osobní a citlivá data. Vyhýbat se návštěvám pochybných stránek. Při registraci číst podmínky užívání.

**Co by měl vědět rodič?**

Rodič by měl upozornit dítě na případná již výše zmíněná rizika. Také by měl dbát, aby zařízení, které dítě používá, mělo nainstalovaný kvalitní a aktualizovaný antivirový program. V případě problému by měl rodič zachovat chladnou hlavu a postupovat dle kapitoly Jak naložit s nezákonným obsahem.

**Jak problémům předcházet?**

* Obezřetně nakládat se svými osobními a citlivými údaji.
* Využívat možnosti nastavení soukromí a uchovat tak soukromé to, co opravdu soukromé je.
* Číst podmínky užívání, zejména co se týče pasáží poskytování údajů třetím stranám.
* Vždy zachovat chladnou hlavu, nepouštět se do sporů a neoplácet stejnou mincí.
* Nedělat na internetu to, co byste nedělali v reálném životě.
* Průběžně sledovat svou digitální stopu, respektive co o sobě na internetu můžete nalézt.
* Využívat možnosti technické ochrany počítače (kvalitní a aktualizovaný antivirový program, aktualizovaný operační systém, aktivovaná brána firewall, programy rodičovské kontroly).

**Jak naložit s nezákonným obsahem?**

* V první řadě je nutné pořídit důkazy, a to v odpovídající kvalitě a formě pomocí takzvaného printscreenu ([snímek obrazovky](http://cs.wikipedia.org/wiki/PrintScreen) ). Důležité je uchovávat důkazy nejen o samotném aktu, ale i o jeho původci (například profil na Facebooku).
* Dalším krokem je kontaktování poskytovatele služby (například funkce nahlášení na Facebooku) s požadavkem o odstranění závadného obsahu.
* Další možností je kontaktování tzv. horkých linek, které jsou kontaktními místy pro nahlašování nezákonného obsahu, kde pomocí krátkých formulářů můžete nahlásit incident. Tyto portály Vám pomohou s odstraněním závadného nebo nezákonného obsahu.
* Kontaktování policie, pokud se jedná o případy v trestní rovině. Policie České republiky mimo jiné provozuje rovněž kontaktní místo pro nahlášení, které je dostupné [zde](http://aplikace.policie.cz/hotline/) .
* Pokud se jedná o případy, kde hrozí dítěti psychická újma, se doporučuje vyhledat pomoc psychologa, v případě kyberšikany mezi spolužáky je určitě vhodné o celé věci vyrozumět školu, respektive výchovného poradce či školního psychologa.

Abychom v závěru článku nebyli pouze negativními. Sociální sítě jsou skvělým nástrojem, můžete zde například najít přátele, které jste již dávno neviděli. Zkuste se třeba nechat poučit dětmi o jejich používání. Možná zjistíte řadu cenných informací a možností pro jejich používání.

Zdroj: <http://www.sancedetem.cz/srv/www/content/pub/cs/clanky/deti-a-rizika-socialnich-siti-112.html>

Autor: Bc. Roman Máca, upravila Mgr. Lenka Hanyšová, školní metodik prevence

[www.msmt.cz](http://www.msmt.cz/)

[www.pomocppp.cz](http://www.pomocppp.cz/)

[www.e-bezpeci.cz/index.php/rodice-ucitele-zaci](https://www.e-bezpeci.cz/index.php/rodice-ucitele-zaci)

[www.seznamsebezpecne.cz/desatero](http://www.seznamsebezpecne.cz/desatero)

[www.bezpecnyinternet.cz/deti/rady-pro-tebe/test.aspx](http://www.bezpecnyinternet.cz/deti/rady-pro-tebe/test.aspx)

[www.kpbi.cz/](http://www.kpbi.cz/)

<http://www.sancedetem.cz/srv/www/content/pub/cs/clanky/deti-a-rizika-socialnich-siti-112.html>

.