Je ve virtuálním světě bezpečno?

- **Rizika a nástrahy sociálních sítí**
- **Doporučení, jak jim předcházet**
- **Důležití odkazy, kde hledat pomoc**

KRAJSKÉ ŘEDITELSTVÍ POLICIE
JIHOMORAVSKÉHO KRAJE

Jak předcházet rizikům na sociálních sítích

Používání internetu a mobilních telefonů je v dnešní době téměř samozřejmostí každého jedince. S nadměrným užíváním zmíněných technologií mohou souviset i určitá rizika. Online prostředí neboli virtuální svět má svá neodmyslitelná pozitiva, ale na druhou stranu se zde skrývají nebezpečí, která nemůžeme ignorovat.

Nejčastější rizika, se kterými se můžeme my, resp. naše děti ve virtuálním světě setkat:

1. Kyberšikana
2. Zveřejňování osobních údajů na sociálních sítích
3. Komunikace s cizím člověkem
4. Osobní schůzka s cizím člověkem (domluvená přes sociální sítě)
5. Fake news

KRAJSKÉ ŘEDITELSTVÍ POLICIE
JIHOMORAVSKÉHO KRAJE

BEZPEČNĚ V @ KYBERPROSTORU

Kyberšikana

Kyberšikana je specifickým druhem klasické šikany, která je **realizována v rámci služeb internetu nebo GSM sítí (mobilní telefony).**

Pod samotnou kyberšikanou se může skrývat řada různorodých projevů, které mohou probíhat samostatně nebo v kombinaci.

Mezi nejčastější projevy kyberšikany patří:

- Verbální útoky (ztrapňování, urážení, nadávání, zesměšňování, ponižování…)
- Zastrašování, vyhrožování, vydírání…
- Průnik na účet
- Krádež identity
- Zveřejňování ponižujících, intimních fotografií, příp. videí

Jak se bránit před kyberšikanou:

- **Nebýt** přehnaně důvěřivý.
- **Nesdělovat** citlivé informace, které by mohly být zneužity (osobní údaje, fotografie, hesla k elektronickým účtům…).
- **Seznámit se** s pravidly služeb internetu a GSM sítí.

KRAJSKÉ ŘEDITELSTVÍ POLICIE JIHOMORAVSKÉHO KRAJE

BEZPEČNĚ V KYBERPROSTORU

- **Seznámit se** s riziky, která hrozí s neuváženým používáním internetu a sociálních sítí.
- **Ukončit** nepříjemnou komunikaci.
- **Blokovat** – zamezit útočníkovi přístup k oběti i k dané službě (kontaktovat poskytovatele služby, zablokovat si přijímání útočníkových zpráv nebo hovorů, změnit svou virtuální identitu).
- **Používat** bezpečná hesla.
- **Oznámit** – oznámit útok dospělým, schovat si důkazy pro vyšetřování (zprávy, odkazy na weby, facebook archiv…).

Nejčastější formy kyberšikany

- **Cyber grooming** – chování, které v dítěti vyvolává falešnou důvěru. Někdo se vydává za někoho jiného, někoho mladšího s úmyslem zneužití získaných informací, fotografií, možné pozvání na schůzku a následné zneužití.
- **Cyberstalking** (pronásledování) – opakované intenzivní obtěžování a ponižování spojené s vyhrožováním nebo zastrašováním.
- **Happy slapping** (fackování pro zábavu) – nečekané fyzické napadení osoby spojené s nahráváním na mobilní telefon nebo kameru. Získané video je poté publikováno na internetu se zesměšňujícím komentářem.

KRAJSKÉ ŘEDITELSTVÍ POLICIE
JIHOMORAVSKÉHO KRAJE

BEZPEČNĚ V @ KYBERPROSTORU

- **Sexting** – elektronické rozesílání SMS, fotografií, videí se sexuálním obsahem.

Sociální sítě

Komunikace přes sociální sítě je v dnešní době nejrozšířenější způsob komunikace. Využívá ji prakticky polovina světové populace. Nejrozšířenější a nejpoužívanější sociální sítí na světě je stále Facebook a dále Youtube.
Další užívané sociální sítí – Google+, Twitter, LinkedIn, Instagram, Pinterest, Tumblr, Instagram, Snapchat, WhatsApp, Viber, Flickr, Ask.fm, Musical.ly, Steam, Foursquer, Vkontakte, Plurk…
Pokud hovoříme o sociálních sítích a internetu vůbec, musíme si uvědomit, že jde o veřejný prostor.
Znamená to, že cokoliv na sociální síť umístíte, zůstává tam napořád a k danému materiálu se může dostat kdokoli.
Samotná hrozba jakékoli sociální sítě nespočívá v její existenci jako takové, ale vždy v chování jednotlivých uživatelů. Jde o to, jak zodpovědně se daný uživatel na sociální síti chová, jaké informace o sobě zveřejňuje a jaký materiál dává k dispozici do veřejného prostoru. Při nezodpovědném užívání jakékoli sociální sítě hrozí ztráta soukromí, únik osobních a citlivých údajů a případné zneužití.

Hrozby pro soukromí jsou velké a zejména děti a mládež neumí dostatečně rozpoznat, kde začíná hranice „nezveřejňovat“.

Na sociální sítě děti uvádějí mnoho osobních údajů (jméno, příjmení, adresu bydliště, adresu školy…), zveřejňují své fotografie a nedomýšlí důsledky, tedy to, že tento citlivý materiál může kdokoli zneužít.

Značnou nevýhodou je fakt, že starší generace neumí sociální sítě používat, obávají se jich, vyhýbají se jim. A nevědí tedy, jakým způsobem fungují, nemohou dětem a mládeži poradit, nevědí jak reagovat, čeho si všímat a dětem raději užívání sociální sítě zakáží. Takový zákaz však může mnohdy způsobit více škody než užitku.
I dospělá populace by se měla se sociálními sítěmi seznamovat (internet nabízí mnoho manuálů, jak správně a bezpečně nastavit profil na sociální síti). Komunikace rodičů a dětí je vždy výhodnější a méně rizikové, než striktní zákazy. Je nezbytné, aby rodiče s dětmi rizika komunikace na sociálních sítích a důsledky zveřejňování osobních údajů a fotografií probrali a dostatečně vysvětlili.

KRAJSKÉ ŘEDITELSTVÍ POLICIE
JIHOMORAVSKÉHO KRAJE

BEZPEČNĚ V KYBERPROSTORU

Nadužívání počítačů a mobilních telefonů

Dnešní děti a mládež jsou s počítači a mobilními telefony spojeni nebývalou měrou. Nadměrné používání internetu, počítačů a sociálních sítí může v řadě případů u dětí a mládeže přerůst v závislost.

- **Netolismus** – chorobná závislost na internetu.

- Riziko nadužívání FCB = rozvoj **FAD** (Facebook Addiction Disorder) – závislostní chování spojené s používáním FCB (jedná se o podskupinu závislosti na internetu zaměřené na konkrétní internetovou službu).

- **Nomofobie** – chorobná závislost na mobilním telefonu (potřeba mít mobil stále u sebe, neustálá kontrola příchozích zpráv, funkčnosti mobilu, kontakt s mobilem hned po probuzení, abstinenční příznaky tam, kde není signál – nervozita).

- **Syndrom FoMO** – z anglického „fear of missing out“, tedy strach z toho, že něco zmeškáme, propásneme, neustále chceme mít přehled o dění v prostředí sociálních sítí. Jiné vnímání času, uživatel je neustále online.

Příznaky FoMO:

- Nervozita
- Podrážděnost
- Netrpělivost
- Špatná nálada
- Stavy úzkosti
- Pocit deprese
- Bušení srdce

Reakce na FoMO:

- Negativní dopad je zejména u přecitlivělých osob (nedostanou pozvánku na společnou akci a jejich sebevědomí klesne na minimum)
- Rezignace
- Snaha dostat se na úroveň obdivovaných (nákup drahých věcí, sdílení virtuálního světa = značné vyčerpání, žijí život někoho jiného)

Co s tím:

- Buďte sami sebou!
- Nenapodobujte někoho jiného.
- Sociální sítě používejte pro komunikaci s přáteli – nemonitorujte životy jiných, žijte svůj vlastní život!

KRAJSKÉ ŘEDITELSTVÍ POLICIE
JIHOMORAVSKÉHO KRAJE

BEZPEČNĚ V KYBERPROSTORU

Falešné profily

Ve většině případů dnešní děti a mládež ví, nebo alespoň tuší, co špatného je může na internetu a sociálních sítích potkat, nicméně jsou ochotni toto riziko podstoupit. Nedomýšlí a hlavně podceňují důsledky svého počínání.

Děti a mládež neumí na internetu a sociálních sítích rozeznat podvodníky, zejména nedokáží rozpoznat, zda se někdo nevydává za někoho jiného. Ve většině případů platí, že se děti a mládež ochotně „stávají přáteli" na sociálních sítích prakticky s kýmkoliv, kdo o to požádá. Jakkoliv v reálném světě učíme děti, že nemají věřit cizím lidem na ulici, tato důležitá součást výchovy u sociálních sítí zcela chybí. Riziko hrozí stejné, ne-li větší.

Největší problém je v tom, že děti a mládež ve virtuálním světě nerozeznávají, kdo je přítel a kdo cizí člověk. Mnohdy stačí pouhý „like"  k tomu, aby děti začaly cizího člověka považovat za kamaráda, to, že je to pořád cizí člověk neberou v potaz.

1. Nejbezpečnější je nekomunikovat ve virtuálním světě s cizím člověkem.
2. Pokud chceš ověřit pravost profilu, zadej tomu na druhé straně nějaký úkol (na papír nakresli sluníčko, napiš aktuální čas, datum, vyfoť se a pošli mi to. Pokud přijde jakákoli výmluva druhé strany, značí to problém a komunikaci ukonči).

3. Pokud chceš ověřit pravost profilu, využij video hovor (webkamera). Pozor na webcam trolling (falešné video smyčky tvářící se jako pravý video hovor, bývá problém se zvukem).

Stejně tak, jak je pro děti obtížné odhalit falešné profily, je pro ně nesnadné vyfiltrovat ve virtuálním světě pravdivé informace, rady, typy a návody. V dnešní době se na sociálních sítích objevuje obrovské množství informací a různých doporučení, jejich kvalita a pravdivost je však různá. Mnoho z těchto informací je nepravdivých, vymyšlených, zavádějících a mohou být i nebezpečné. Proto je nezbytně nutné, aby rodiče i v této oblasti na děti dohlédli a vysvětli, že ne všechny informace na internetu jsou pravdivé.
Velký problém je v tom, že v poslední době se primárním zdrojem informací stávají právě sociální sítě. Ty neoddělují pravdivé a nepravdivé informace (rozdíl od seriózních médií). Často tedy narážíme na informace nepravdivé, vymyšlené, manipulující = fake news a hoaxy.

Hoax

V počítačovém světě slovem HOAX nejčastěji označujeme poplašnou zprávu, která varuje před neexistujícím nebezpečným virem.

Typický text poplašné zprávy obsahuje většinou tyto body:

- Snaží se přesvědčit svojí důležitostí
- Šokující informace, nové nebezpečí, naléhavá pomoc…
- Důvěryhodné zdroje varují
- Nebo naopak tajná informace unikla
- Údajná informace, o které oficiální média mlčí a nesmí se o ní mluvit, ale autor zprávy ji objevil a vyzývá k jejímu sdílení
- Výzva k dalšímu rozeslání

Rady pro bezpečné chování na internetu pro rodiče

V dnešní době moderních technologií a elektronických prostředků se komunikace stále častěji odehrává ve virtuálním světě prostřednictvím sociálních sítí. S tímto nadužíváním internetu, mobilních telefonů a sociálních sítí souvisí i možné riziko kyberšikany. Dítě dnes prakticky žije internetem a většinu informací přijímá právě z tohoto prostředí. Rodiče by měli se svými dětmi o komunikaci na sociálních sítích mluvit a rizika, která v tomto světě hrozí, jim vysvětlit. Mnohdy však znalosti dětí převyšují znalosti rodičů a rodiče na jakékoli snahy o ochranu ve virtuálním světě rezignují. Rodiče by však neměli rizika kyberprostoru podceňovat a i v této oblasti se vzdělávat, mít přehled a držet s dětmi krok.

KRAJSKÉ ŘEDITELSTVÍ POLICIE
JIHOMORAVSKÉHO KRAJE

BEZPEČNĚ V @ KYBERPROSTORU

1. Mějte přehled o aktivitách svých dětí ve virtuálním světě.

- děti neumí rozlišit a vyfiltrovat pravdivé informace na internetu, proto je důležité, aby rodiče se svými dětmi o virtuálním světě hovořili a na možná rizika a nástrahy je upozornili.

2. Využijte možnost nastavení rodičovské kontroly na PC.

- nastavení omezeného režimu na PC (Youtube, Google) – filtrování nevhodného obsahu z výsledku vyhledávání
- programy na „hlídání“ dětí v online prostředí (Family by Sygic, Kaspersky Safe Kids, Norton Online Family, Protect-You, ManicTime, PC Screen Watcher, Activity Mon, Net Nanny)

3. Držte tempo se svými dětmi a vzdělávejte se

- v dnešním světě moderních technologií, je nezbytností zajímat se o technické novinky, ale zároveň i o hrozby ve virtuálním světě
- požádejte své děti o vtažení do problematiky sociálních sítí

4. Naučte své děti chránit si své soukromí

- vysvětlete dítěti, jaká rizika souvisí se sdělováním osobních údajů a co všechno patří do osobních a citlivých údajů
- myslete i na bezpečná hesla

KRAJSKÉ ŘEDITELSTVÍ POLICIE JIHOMORAVSKÉHO KRAJE

BEZPEČNĚ V KYBERPROSTORU

5. Nezakazujte dítěti komunikaci ve virtuálním světě

- není řešením dítěti zakázat používání sociálních sítí, o to více se bude snažit do virtuálního světa proniknout
- zákazem bychom mohli dítě vyčlenit z kolektivu a vystavit ho posměchu
- komunikujte s dítětem a vysvětlete mu rizika a hrozby, upozorněte ho na bezpečnou komunikaci a dále na etiketu (pravidla slušného chování na internetu)
- vysvětlete dítěti, že porušováním pravidel internetu se může snadno dostat do problému (protiprávní jednání, např. porušování autorského zákona)

6. Buďte svému dítěti oporou

7. Nastavení omezeného režimu na počítači

- Filtrování nevhodného obsahu z výsledku vyhledávání.
- **Omezený režim** je povolený na úrovni prohlížeče – musí se aktivovat zvlášť v každém prohlížeči v počítači.
- Pokud prohlížeč podporuje více profilů, je nutné jej aktivovat u každého profilu samostatně.

KRAJSKÉ ŘEDITELSTVÍ POLICIE
JIHOMORAVSKÉHO KRAJE

BEZPEČNĚ V KYBERPROSTORU

V případě, kdy budete potřebovat pomoc, můžete využít následující stránky:

- **www.linkabezpeci.cz (116 111)**
- **www.stoponline.cz**
- **www.rodicovskalinka.cz (840 111 234, 606 021 021)**

Důležité odkazy, kde k uvedené problematice naleznete více:

- **http://www.kr-jihomoravsky.cz/kyber/**
- **www.e-bezpeci.cz**
- **www.saferinternet.cz**
- **www.bezpecnyinternet.cz**
- **www.seznamsebezpecne.cz**
- **www.internetembezpecne.cz**
- **www.hoax.cz**

KRAJSKÉ ŘEDITELSTVÍ POLICIE JIHOMORAVSKÉHO KRAJE

BEZPEČNĚ V KYBERPROSTORU

Použité zdroje:

www.e-bezpeci.cz
http://www.e-bezpeci.cz/index.php/veda-a-vyzkum/1103-czech-children-facebook-research-report-2015

KRAJSKÉ ŘEDITELSTVÍ POLICIE JIHOMORAVSKÉHO KRAJE

BEZPEČNĚ V KYBERPROSTORU

KRAJSKÉ ŘEDITELSTVÍ POLICIE
JIHOMORAVSKÉHO KRAJE

B | R | N | O