



# KYBERAKADEMIE

PRO PRACOVNÍKY OBCÍ, OBEČNÍCH POLICIÍ A DALŠÍ  
CÍLOVÉ SKUPINY VE ŠKOLNÍM PROSTŘEDÍ

**KYBERAKADEMIE pro pracovníky obcí, obecních policíí a další cílové skupiny ve školním prostředí**

Autoři: Kamil Kopecký, René Szotkowski, Lukáš Kubala

Institut výzkumu a vzdělávání v oblasti digitálních technologií a kyberbezpečnosti

Pedagogická fakulta Univerzity Palackého v Olomouci

ve spolupráci s Ministerstvem vnitra ČR

© 2025

Verze 2.0 (2. rozšířená verze)

## Obsah

Slovo úvodem.....	6
1 Internetová agrese.....	10
1.1 Kybershikana.....	10
1.1.1 Jak řešit kybershikanu (z pohledu oběti).....	13
1.1.2 Vybrané případy kybershikany zaměřené na děti.....	15
1.2 Hating a předsudečná nenávisť.....	23
1.3 Body shaming.....	26
2 Sexting a jeho rizika.....	29
2.1 Sextortion.....	30
2.2 Revenge porn.....	31
2.3 Webcam trolling a webcam blackmailing.....	34
2.4 Sebe-natáčení v intimních situacích a jeho rizika.....	36
3 Online seznamování a kybergrooming.....	40
3.1 Kybergrooming.....	40
3.1.1 Kde ke kybergroomingu dochází?.....	41
3.1.2 Kdo jsou pachatelé?.....	42
3.1.3 Kdo jsou oběti?.....	43
3.1.4 Jak dlouho probíhá manipulace dítěte?.....	43

3.1.5	Etapy manipulace .....	43
3.1.6	Současné trendy v kybergroomingu .....	46
3.1.7	Vybrané případy kybergroomingu zaměřené na děti .....	47
4	Rizikové výzvy v online prostředí.....	54
5	Online podvody.....	62
5.1	Phishing .....	62
5.2	Vishing .....	64
5.3	Scam419.....	64
5.4	Romance scam.....	65
5.5	CEO scam (BEC scam, Boss scam) .....	69
5.6	Invoice scam.....	70
5.7	Reverzní internetové podvody (R.I.P.).....	72
5.8	Prevence a boj proti online podvodům.....	73
6	Děti, sociální média a sociální sítě .....	75
7	Rizika spojená s umělou inteligencí.....	77
7.1	Nástroje generativní umělé inteligence dělají chyby .....	77
7.2	Problém s autorskými právy .....	78
7.3	Podvádění ve škole.....	78
7.4	Tvorba škodlivého obsahu včetně dezinformací.....	79

7.5	Zneužití pro podvodnou činnost.....	81
7.6	Závislost na používání technologie.....	82
8	Digitální stopa.....	83
9	Sharenting.....	87
10	Zásady efektivní prevence.....	94
11	Důležité odkazy a další materiály.....	97
12	Reference .....	100

## **Slovo úvodem**

Vítáme vás v nové publikaci, která je metodickým průvodcem klíčovými tématy prevence rizikového chování v online prostředí. V publikaci shrneme problematiku kybernetické šikany (kyberšikany), kybergoomingu či sextingu, pozornost věnujeme také např. vydírání, vyhrožování a dalším formám agrese, se kterými se děti v online světě setkávají. Výklad je doplněn o kazuistiky a metodické rady pro lektory (např. městské policisty). Tuto publikaci jsme vytvořili pro všechny, kteří se věnují všeobecné primární prevenci a pracují s dětmi a dospívajícími – ať již ve školním prostředí či mimo něj.

Až budete svému publiku představovat jednotlivá témata, seznamovat je s kazuistikou a vysvětlovat, jak by mohlo dané problémy řešit, nezapomeňte dodržovat základní preventivní zásady – prevence by neměla žáky strašit a měla se opírat o fakta a objektivní informace, zároveň by měla probíhat v bezpečném prostředí (každý žák by měl mít právo projevit svůj názor, ať už je jakýkoli). Preventivní pracovník by dětem neměl nic zakazovat, ale upozorňovat je, jaké důsledky může mít rizikové chování na jejich život a proč je výhodné chovat se v online prostředí zodpovědně a bezpečně.

Věříme, že tato publikace poskytne znalosti a dovednosti, které pomohou zvýšit kvalitu vašich vzdělávacích akcí. Ať se daří!

Za realizační tým  
Kamil Kopecký, René Szotkowski, Lukáš Kubala, Lucie Kosová  
Univerzita Palackého v Olomouci

Vážené kolegyně, vážení kolegové,

jako národní gestor problematiky prevence kriminality v České republice jsme byli často tázáni řadou z vás, kteří se věnujete prevenci kriminality a rizikového chování v přímém kontaktu s cílovými skupinami, zda vám můžeme poskytnout nebo vás odkázat na již existující materiály, se kterými byste mohli kvalitně realizovat své preventivní aktivity a přednášky v oblasti prevence kybernetické kriminality a rizikového chování v online prostoru.

Abychom vytvořili co nejlepší podmínky pro vaši práci, rozhodli jsme se spojit s předními odborníky, týmem E-Bezpečí Univerzity Palackého v Olomouci, využít jejich odbornosti, výzkumné činnosti a zkušeností z poradenství v této oblasti a společně jsme připravili tuto Kyberakademii pro pracovníky obcí a obecních policií (ale i další pracovníky) pohybující se ve školním prostředí (nebo obecně pracující s dětmi a mladistvými, a to i mimo školní prostředí).

Kromě základních a podrobných informací, vysvětlení, kazuistik a doporučení, obsažených v primárním metodickém materiálu, jsme vám chtěli co nejvíce usnadnit i přímou práci a připravili jsme i pomůcky ve formě předpřipravené prezentace či letáků. Ty si můžete graficky doplnit o vlastní loga a kompletní materiál uložit do připravených desek.

Budeme rádi za zpětnou vazbu ([opk@mv.gov.cz](mailto:opk@mv.gov.cz)), jak se vám s materiálem pracuje a jak bychom jej mohli ještě případně vylepšit či na co myslet při přípravě podobných materiálů do budoucna.

Věříme, že tyto materiály budou přínosem a přejeme hodně úspěchů při vaší práci!

JUDr. Michal Barbořík  
ředitel odboru prevence kriminality  
Ministerstva vnitra ČR



## 1 Internetová agrese

V internetovém prostředí se běžně setkáváme s různými formami agrese, ať už jde o nejrůznější formy příspěvků cíleně vyvolávajících nenávist, nenávistné komentáře či pokročilejší formy agrese, ke kterým patří například **kyberšikana** – včetně jejich vysoce toxických forem, které mohou přerůst až v konkrétní trestné činy (vydírání, vyhrožování apod.).

Děti se s online agresí setkávají poměrně běžně, a to jak na straně pasivních přihlížejších, tak na straně obětí, či dokonce agresorů.

### 1.1 Kyberšikana

K jedné z nejčastějších forem agrese, se kterou se setkávají děti v online prostředí, patří tzv. kybernetická šikana = kyberšikana. Slovem **kyberšikana označujeme nejrůznější formy agresivních útoků na jednotlivce** (či skupiny žáků), které **k útoku využívají moderní komunikační technologie**, především mobilní telefony (ale také např. počítače, tablety apod.). Co je důležité – u kyberšikany **dochází k útokům opakovaně**, útoky jsou **intenzivní** a mají na dítě skutečně **dopad, dítě útoky vnímá jako ubližující**. V praxi se pak mohou projevat třeba tím, že je dítě zamlklé, objevují se u něj fyziologické projevy (špatně spí, budí se, přejídá se, či naopak hladoví, bolí ho hlava), mění se jeho chování apod. Kyberšikana je často zaměňována s tzv. online obtěžováním, tímto termínem označujeme **jednorázové útoky**, jejichž dopad na oběť je pouze dočasný.

Kyberšikanu **zažívá přibližně 8–10 % dětí v České republice** a podle zpráv České školní inspekce se objevuje zhruba v polovině českých škol.

**Pachatelem kyberšikany** zpravidla bývá někdo z okolí oběti – např. její **spolužáci, žáci ze stejné školy či jiní vrstevníci**. K nejčastějším motivům pachatelů patří především pomsta, dále např. představa pachatelů, že oběti si kyberšikanu zaslouží, mezi motivy nalezneme i nudu, v řadě případů vzniká kyberšikana pod vlivem skupinového tlaku ve třídě. U kyberšikany se objevuje tzv. přepínání rolí – z obětí tradičních forem šikany se mohou stávat pachatelé kyberšikany.

**Pachatelé často věří, že je díky internetové anonymitě nelze vystopovat a chytit**, ve skutečnosti však za sebou zanechávají řadu tzv. digitálních stop. Anonymita je ve skutečnosti pouze zdánlivá.

Kyberšikana je zpravidla definována jako činnost záměrná, může však vzniknout i nezáměrně – třeba jako **nevhodný vtíp**, který se v online prostředí vymkne kontrole.

Dítě si nemusí uvědomit, jak mohou rádoby vtipné fotografie či videa ublížit, pokud se začnou nekontrolovaně šířit internetem a začnou být masově komentovány.





## CO PATŘÍ DO KYBERŠIKANY?

PONIŽOVÁNÍ,  
NADÁVÁNÍ A URÁŽENÍ  
V ONLINE PROSTŘEDÍ

VYHROŽOVÁNÍ  
A ZASTRAŠOVÁNÍ  
V ONLINE PROSTŘEDÍ

VYDÍRÁNÍ V ONLINE  
PROSTŘEDÍ

ŠÍŘENÍ PONIŽUJÍCÍCH  
FOTOGRAFIÍ

ŠÍŘENÍ PONIŽUJÍCÍCH  
VIDEÍ

TVORBA FALEŠNÝCH  
PROFILŮ

ZVEŘEJŇOVÁNÍ CIZÍCH  
TAJEMSTVÍ

Pachatelé kyberšikany si často neuvědomují, co svým chováním oběti působí – prostřednictvím internetu nevidí, že oběť pláče, že nemůže spát, že se trápí apod. **To, co z pohledu útočníka vypadá jako legrace, může oběť vnímat jako skutečné násilí** – jako šikanu či kyberšikanu. A u některých citlivějších dětí může vést až k sebevraždě.

Síla kyberšikany spočívá v tom, že se do ní zapojuje skutečně velké množství lidí – a to jak z okolí oběti, tak těch, kteří oběť vlastně vůbec neznají a pouze ponižující materiály šíří a komentují.

Kdyby pachatelé cítili, co oběti prožívají, pochopili by, jak bolestivá kyberšikana může být a co může způsobit. A možná by si své chování rozmysleli.

**Pamatujte si, za své chování vždy neseme odpovědnost!**

### **1.1.1 Jak řešit kyberšikanu (z pohledu oběti)**

Pokud dítě zažívá kyberšikanu, je třeba **zachovat klid** a **pořídit si důkazy** o tom, že kyberšikana skutečně probíhá (např. uložit si screeny komunikace apod.). Poté je dobré **zjistit příčinu**, proč k útoku dochází – někdy může jít o nedorozumění, které se snadno vysvětlí a kyberšikanu půjde rychle zastavit. Určitě je vhodné **omezit komunikaci s agresorem**, hlavně mu nenadávat, nenapadat ho, nemotivovat k dalšímu útoku. Pokud pachatel neustává v šíření nenávisti, můžeme ho zablokovat (ale až po pořízení důkazů). Dobré je také **oznámit útok dospělým** (rodiči, učiteli) – mohou pomoci s řešením. Z pohledu oběti je také důležité **žádat konečný verdikt** – dítě potřebuje vědět, jak byla kyberšikana dořešena, zda byli agresoři potrestáni a jak je zajištěno, že už se tento problém

nebude opakovat. Školy a školská zařízení jsou povinny zajišťovat bezpečnost a ochranu zdraví dětí, žáků a studentů v průběhu všech vzdělávacích a souvisejících aktivit, vytvářet podmínky pro zdravý vývoj a předcházet vzniku rizikového chování. Proto by se měly **kyberšikanou zabývat vždy, když se o ní dozví**. Na druhou stranu kompetence školy jsou ohraničeny a limitovány:

**Škola nemůže udělovat kázeňské tresty, popř. snížené známky z chování za činnost, která se nestala během vyučování nebo v rámci akcí organizovaných a zajištěných školou, kde učitel vykonává nad žáky dohled**[1] – při kurzech, exkurzích a jiných činnostech vyplývajících ze školních vzdělávacích programů nebo učebních dokumentů, při účasti na soutěžích, přehlídkách, popřípadě při jejich přípravě a na jiných akcích organizovaných školou nebo školským zařízením. Zároveň však může trestat i **v situaci, kdy je kyberšikana propojena se šikanou probíhající ve škole** – tj. dítě je šikanováno a kyberšikana je rozšířenou formou této šikany, šikana tedy pokračuje ve virtuálním světě.[2]

**ŠKOLA NESMÍ  
KYBERŠIKANU  
IGNOROVAT!**



## 1.1.2 Vybrané případy kyberšikany zaměřené na děti

### Případ: Ghyslain Raza (Kanada, 2003)

První mediálně známou obětí kyberšikany se stal 13letý chlapec z Kanady **Ghyslain Raza** alias Star Wars Kid, a to po zveřejnění videozáznamu (viz obrázek vlevo), na němž předvádí bojovou scénu Dartha Maula z filmové ságy Hvězdné války (Star Wars). Chlapec si nahrávku pořídil pro svou potřebu, ale naneštěstí se dostala do rukou jeho spolužákům, kteří ji zveřejnili prostřednictvím P2P sítě Kazaa. Videonahrávku zhlédlo velké množství lidí, mezi nimiž byl i herní vývojář z firmy Raven Software Bryan Dube, který ji opatřil světelnými a zvukovými efekty (obrázek vpravo), čímž přispěl k jejímu masovému rozšíření.



Obrázek: Ukázka z originální a upravené nahrávky (Zdroj: YouTube.com)

Video bylo následně upravováno ještě několikrát, například vznikly remixy z různých filmů a seriálů – Matrix, Star Wars, Star Trek, Kill Bill, Mortal Kombat, Pán prstenů, Indiana Jones atd. V roce 2006 se video stalo nejpopulárnějším internetovým videem na světě s více než 900 miliony zobrazení (Star Wars Kid is top viral video 2006) a v roce 2007 bylo vyhlášeno nejoblíbenějším internetovým videem na světě (Vinson 2010).

**Upravenou videoukázku můžete nalézt např. zde:**

[https://www.youtube.com/watch?v=3GJOVPjhXMY;](https://www.youtube.com/watch?v=3GJOVPjhXMY)

[https://www.youtube.com/watch?v=GRiJVMASwjl;](https://www.youtube.com/watch?v=GRiJVMASwjl)

Mimo upravené videoukázky vznikla i řada parodií ve známých animovaných seriálech jako např. South Park, American Dad apod.



*Obrázek: South Park (epizoda Canada on Strike) a American Dad (epizoda All About Steve)*

Když se chlapec dozvěděl o své nečekané popularitě, utrpěl těžký psychický otřes a musel se podrobit dlouhodobému léčení. Nahrávka totiž opravdu nebyla zrovna povedená a velmi okatě demonstrovala jeho nadváhu a neohrabanost, což navíc řada diváků z internetového světa neváhala ventilovat na svých stránkách a blozích.

## Případy kyberšikany z poradny E-Bezpečí

### Kyberšikana Petra 13 let (ČR, 2022)

Dobrý den, obracím se na vás s prosbou o pomoc při řešení podezření z šikany, ke které dochází ve třídě naší dcery. Jedná se o ZŠ XY, kde je již delší dobu z našeho pohledu šikanován chlapec ze strany ostatních chlapců. Do WhatsApp třídní skupiny chodí zprávy od jeho spolužáka Adama.

**PETR JE NAŠE  
BUZNIČKA**



**MÁ MINIATURNÍHO  
PTÁČKA**

**ON VLASTNĚ ŽÁDNÝHO  
PTÁČKA NEMÁ**



**ANI HOLČÍČÍ KLIK  
NEUDĚLÁ**



Chlapci chodí výzvy ke rvačkám po škole, ve škole se mu taktéž posmívají. Třídní učitelka se na třídních schůzkách vyjádřila v tom smyslu, že nemohou situaci řešit, protože k šikaně dochází online, tedy mimo školu, a i přes dohodu, že bude o situaci informovat vždy rodiče, vím od maminky Petra, že k žádnému setkání s rodiči druhého chlapce nedošlo a situace se dále neřeší. V okamžiku, kdy se některé děti spolužáka zastaly, začaly i jim chodit urážející zprávy. Ráda bych tedy věděla, jakým způsobem můžeme postupovat, aby k podobnému jednání už nedocházelo a škola se k tomu postavila čelem. Děkuji a jsem s pozdravem.

Komentář: **Škola může kyberšikanu řešit v situaci, kdy toto jednání probíhá během školního vyučování (zpravidla v budově školy), případně v rámci akcí organizovaných školou (školní výlety, divadelní a filmová představení apod.).** Může zasáhnout také tehdy, kdy kyberšikana probíhá jako doprovodný jev šikany – tedy v tomto případě. Škola i učitelka postupovaly špatně.

## Vybrané případy kyberšikany zaměřené na dospělé:

### Případ: Jiří Pacholík (ČR, 2008)

Bývalý ředitel základní školy v Železném Brodu Jiří Pacholík upozornil 15letého žáka na nepořádek, který měl pod školní lavicí. Ředitel žáka vyzval k úklidu nepořádku, ten mu agresivně odpověděl: „**Proč bych si to skládal, ty šmejde?!**“ Ředitel na toto vyjádření žáka zareagoval pohlavkem, načež žák demonstrativně utekl ze třídy. Ředitel si uvědomil své pochybení, žáka přivedl zpět do třídy a za své chování se omluvil. Spolužáci situaci natočili na mobilní telefon a zveřejnili na internetu, ovšem bez ředitelovy omluvy.



*Obrázek: Ukázka natočeného a zveřejněného videa*

Situaci začal řešit otec napadeného žáka, který se rozhodl celý případ medializovat.

Následoval mediální hon na pana ředitele, který se zhroutil, delší dobu pobýval v pracovní neschopnosti a nakonec **spáchal sebevraždu**.

JABLONECKÝ

**deník.cz** [Vzbrat deník](#) [Katalog firem](#) [Napište nám](#)

### Ředitel školy fackuje žáky

Železný Brod – Na stránkách YouTube.com visí video, které pořídili žáci ZŠ Pelechovská v Železném Brodě. Ředitel nejdříve strká a poté fackuje jednoho z nich



*Budoucí prvňáčci u zápisu. Vědí rodiče, jakého má škola ředitele?*

*Obrázek: Ukázka medializace případu*

## Případ: Zdeněk Svěrák (ČR, 2013)

Počátkem listopadu 2013 podal herec Zdeněk Svěrák trestní oznámení na zakladatele facebookového profilu „**Znásilnil mě Zdeněk Svěrák**“, který o něm šířil falešné zprávy. Facebooková stránka obsahovala v okamžiku zveřejnění několik obvinění ze znásilnění, zaslaných z fiktivních a anonymně vytvořených uživatelských účtů. Profil například informoval o tom, že Zdeněk Svěrák zneužíval děti při natáčení dětských pořadů a za sexuální praktiky jim platil.



Obrázek: Falešná Facebooková stránka dehonestující Zdeňka Svěráka

## 1.2 Hating a předsudečná nenávisť

S kyberšikanou souvisí také tzv. hating, tedy nenávistné projevy, které mohou mít řadu variant a forem.

1. Běžná agrese (zpravidla jednorázová)
2. Kyberšikana
3. Přestupek
4. Trestný čin

Hating obvykle souvisí se **svobodou projevu**, což je ústavní právo, které umožňuje lidem vyjadřovat svobodně své názory. Uživatelé internetu se však často mylně domnívají, že na základě tohoto práva mohou na internetu psát vše bez jakýchkoli hranic a limitů. To však není pravda – Listina základních práv a svobod ve svém článku 17 (odstavec 4) tyto hranice definuje:[3]

### Listina základních práv a svobod – Článek 17

(1) Svoboda projevu a právo na informace jsou zaručeny.

(2) Každý má právo vyjadřovat své názory slovem, písmem, tiskem, obrazem nebo jiným způsobem, jakož i svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu.

(3) Cenzura je nepřipustná.

**(4) Svobodu projevu a právo vyhledávat a šířit informace lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro**

## **ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti.**

(5) Státní orgány a orgány územní samosprávy jsou povinny přiměřeným způsobem poskytovat informace o své činnosti. Podmínky a provedení stanoví zákon.

V praxi to tedy znamená, že pokud např. **vyhrožujeme, vydíráme, napadáme, pronásledujeme, šíříme poplašné zprávy, překračujeme hranici svobody slova a můžeme být potrestáni.**[4]

Hating je velmi často spojen s trestnými činy, např. § 355 TZ Hanobení národa, rasy, etnické či jiné skupiny osob či § 355 TZ Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod.



**Policie České republiky**

28. listopad v 9:52 · 🌐

Neomezená virtuální svoboda a anonymita má i na sociálních sítích právní rámec a hranice. Svým příspěvkem či jen komentářem můžete naplnit skutkovou podstatu hned několika paragrafů trestního zákoníku. Myslete na to, než napíšete nějaký ten „jed“ - děkujeme!

§ 181 - poškození cizích práv

§ 184 - pomluva

§ 345 - křivé obvinění

§ 355 - hanobení...

§ 356 - podněcování k nenávisti...

§ 357 - šíření poplašné zprávy

§ 364 - podněcování k trestnému činu

§ 365 - schvalování trestného činu

§ 404 - projev sympatií k hnutí směřujícímu k potlačování práv a svobod člověka

## **Vybrané případy hatingu zaměřeného na děti:**

### **Případ: ZŠ Plynářská z Teplic (ČR, 2017)**

Typickým případem hatingu je kauza tabla prvňáčků ze ZŠ Plynářská z Teplic – zveřejněné tablo s etnicky smířenou skupinou dětí se v online prostředí stalo terčem stovek nenávistných projevů (hatingu), někteří autoři komentářů byli také vyšetřováni PČR za podezření ze spáchání trestných činů či přestupků.



*Obrázek: Fotografie prvňáčků ze ZŠ Plynářská z Teplic použité k hatingu*

### 1.3 Body shaming

K internetové agresí patří také tzv. body shaming. **Body shaming je forma ponižování, kritiky nebo urážení člověka kvůli jeho tělesnému vzhledu.** Tento jev se obvykle vyskytuje v souvislosti se společenskými standardy krásy a ideály tělesnosti, které jsou často nezdravé, nereálné a diskriminující.

#### **Formy útoků na tělesný vzhled:**

- přehnaná očekávání související s tělesnou váhou nebo tvarem těla,
- urážlivé poznámky týkající se vzhledu nebo porovnávání s jinými lidmi.

#### **Vliv body shamingu na člověka:**

- může vést k nízkému sebevědomí, sociální izolaci, úzkosti, depresi a dalším psychickým problémům,
- může mít vliv na chování lidí,
- může vést ke snaze změnit své tělo tak, aby vyhovovalo společenským standardům krásy,
- citlivé jedince může dohnat k nevhodným, a dokonce nebezpečným praktikám, jako jsou extrémní diety, chirurgické zákroky, užívání nebezpečných látek nebo vysilující cvičení,
- může mít vážný dopad na tělesné i duševní zdraví jednotlivce.

## Body shaming a internet

Body shaming se stal běžnou součástí komunikace také v prostředí internetu, především pak na sociálních sítích, které aktivně pracují s fotografiemi a videi (typicky Instagram a TikTok). Internet uživatelům poskytuje anonymitu a bezprostřednost, což může vést k tomu, že lidé jsou ochotnější kritizovat ostatní a ponižovat je kvůli jejich vzhledu nebo postavě. Když se tato kritika stane veřejnou, může to vést k dalšímu šíření negativních názorů na určitou osobu nebo skupinu lidí.

### Podoby online body shamingu:

- urážky a narážky na vzhled lidí v diskusních fórech, na sociálních sítích, v komentářích pod příspěvky, v online chatovacích místnostech a dalších místech,
- napadání ostatních uživatelů kvůli váze, výšce, barvě pleti, tvaru těla, vzhledu obličeje, vlasů a dalším vlastnostem, které mohou být vnímány jako odlišné nebo neobvyklé.

Body shaming také může být součástí kyberšikany.

Informace o tom, jak je body shaming rozšířen v populaci českých dětí, poskytuje např. výzkum Centra prevence rizikové virtuální komunikace s názvem **Děti a kult krásy v on-line světě** (Univerzita Palackého v Olomouci a O2, 2022): třetina českých dětí potvrdila, že v online prostředí čelila posměškům týkajícím se jejich online profilu, 14 % dětí zažilo negativní komentáře spojené s obličejem a vlasy, 11 % dětí zažilo urážky spojené s jejich postavou.

## **Co můžeme dělat, abychom se chránili před body shamingem?**

- 1. Přemýšlejme o tom, co říkáme a jak se chováme, a to jak k sobě, tak k ostatním:** Je důležité, aby lidé omezili urážlivé chování a jednali vůči sobě i ostatním s respektem.
- 2. Budujme zdravé sebevědomí:** Budování sebevědomí může být klíčové při ochraně před body shamingem.
- 3. Hledejte pozitivní vzory:** Najděme si inspirativní osobnosti, které nám mohou poskytnout dobré příklady chování a přístupu k životu.
- 4. Budme proaktivní:** Pokud se setkáme s někým, komu body shaming ublížil, nabídněme mu podporu a povzbuzení.
- 5. Respektujme tělesnou rozmanitost:** Je důležité respektovat různorodost těl a bojovat proti společenským standardům krásy, které jsou často nezdravé, nereálné a diskriminující.

## 2 Sexting a jeho rizika

Za **sexting** označujeme **dobrovolné sdílení vlastních intimních materiálů (fotografií, videí, má však i textovou podobu) – a to zpravidla v online prostředí.**[5] Ačkoli se sextingu věnují především dospělí, a to zejména v rámci partnerských vztahů, stále častěji se s ním setkáváme i u dětí.

Se sextingem je spojena celá řada rizik:

- v online prostředí **snadno ztratíme kontrolu nad šířeným materiálem,**
- **materiály mohou po internetu kolovat desítky let,**
- **sexting může poškodit naši prestiž a způsobit ztrátu zaměstnání,**
- **v rámci sextingu se můžeme stát pachateli přestupků či trestných činů** (v rámci zákona **č. 251/2016 Zákon o některých přestupcích** je to např. § 7 Přestupky proti občanskému soužití, v rámci zákona **č. 40/2009 Sb. Trestní zákoník** je to např. § 192 Výroba a jiné nakládání s dětskou pornografií, § 191 Šíření pornografie, § 201 Ohrožování výchovy dítěte, § 193b Navazování nedovolených kontaktů s dítětem, § 193a Účast na pornografickém představení, § 186 Sexuální nátlak apod.).

Sexting bývá součástí kyberšikany, kybergroomingu a dalšího rizikového chování v online prostředí. Podle trestního zákona **§ 126 Dítě** se dítětem rozumí **osoba mladší 18 let**, pokud trestní zákon nestanoví jinak. Pakliže nezletilá osoba pořizuje nebo zveřejňuje materiály sexuální povahy (textové, obrazové, videa

apod.), může se sama dopustit výše uvedených trestných činů. **Každý případ je nezbytné posuzovat individuálně podle konkrétních okolností.**

## **2.1 Sextortion**

Termínem **sexortion (sex + extortion)** označujeme vydírání, které využívá **intimních materiálů oběti.**[6] Sextortion má mnoho variant a podob, v některých případech je propojeno s tzv. **kybergroomingem** (dále v textu).

Pachatelé vyhledávají své oběti na online seznamkách, videochatovacích službách, sociálních sítích jako např. Snapchat či instant messengerech jako např. Telegram.

Obětí vydírání skrze intimní materiály mohou být ženy i muži, ovšem podle dat poradny [www.napisnam.cz](http://www.napisnam.cz) projektu E-Bezpečí postihuje tento fenomén daleko častěji mladé chlapce a muže, a to zejména na seznamovacích platformách.

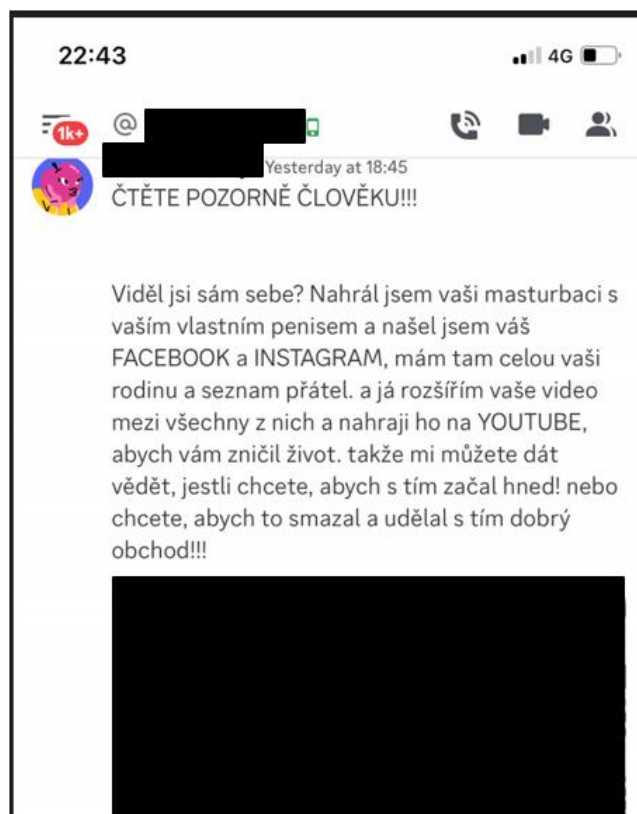
### **Případ z poradny E-Bezpečí:**

#### **Radek 16 let**

*Byl jsem kontaktován na Snapchatu údajnou Kanadankou žijící v ČR. Ptala se mě na různé věci, např. kde bydlím apod. Řekl jsem jí jenom, že chodím na gymnázium (nespecifikoval jsem to).*

*Pak se mě ptala na sexuální otázky a já jsem byl tak hloupý, že jsem jí poslal nahou fotku.*

*Potřebuji pomoci, děkuji.*



*Obrázek: Ukázka vyděračské zprávy, kterou obdržela oběť sextortionu*

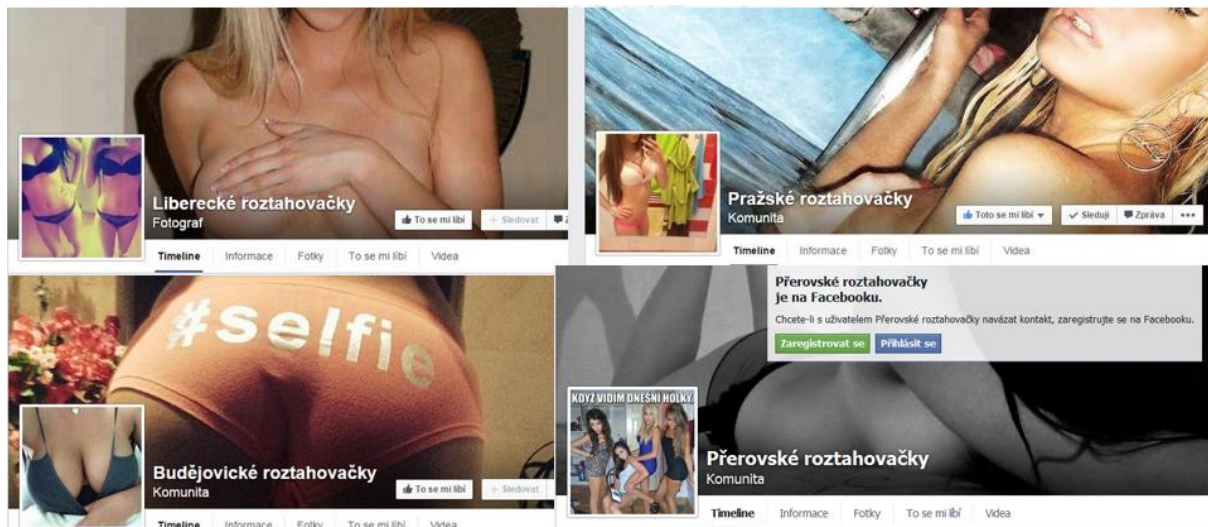
## 2.2 Revenge porn

**Revenge porn** (porno-pomsta) označuje typ útoku, při němž dochází ke kyberšikaně konkrétních osob prostřednictvím šíření dehonestujících sexuálně explicitních fotografií či videí obětí jejich expartnerů či dalšími osobami. Revenge porn je průvodním jevem tzv. „nezvládnutých rozchodů“ (rozchod, který nekončí

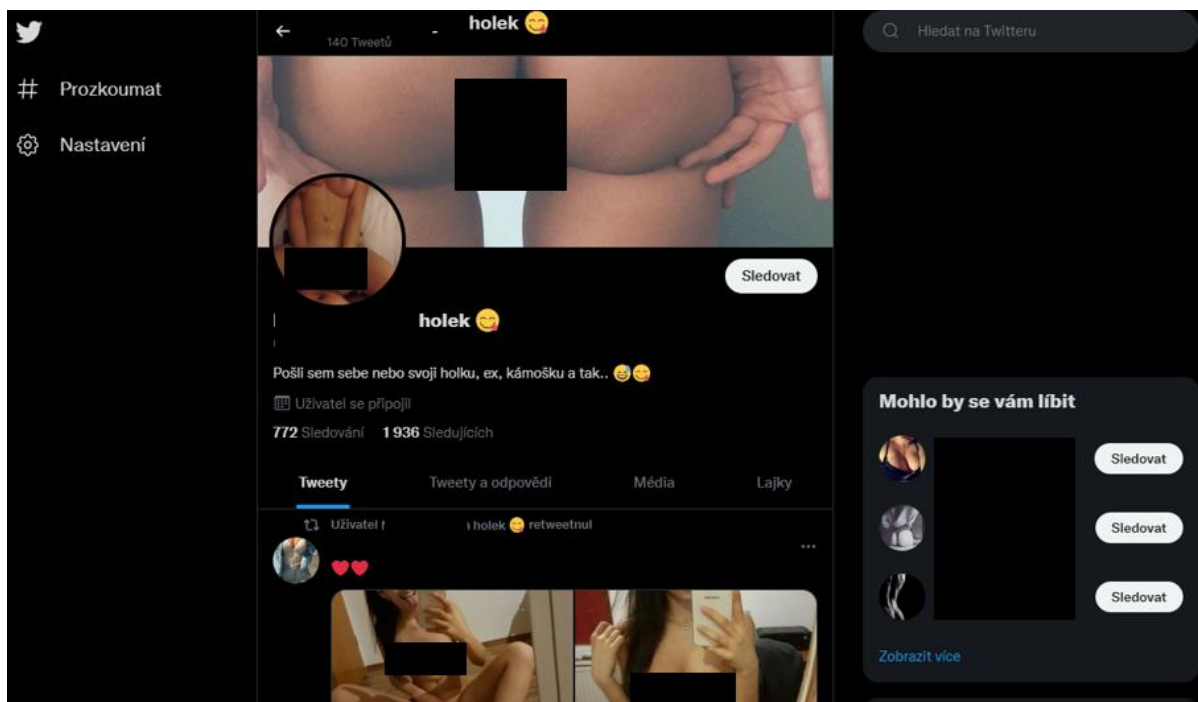
smírem mezi partnery), či přímo trestného činu nebezpečného pronásledování (tzv. stalking).

Pomsta skrze intimní materiály může postihnout ženy i muže, ovšem podle dat poradny [www.napisnam.cz](http://www.napisnam.cz) projektu E-Bezpečí je tento fenomén daleko častější u mladých dívek a žen.

V České republice se tento fenomén masově objevil v souvislosti s kauzou tzv. „**roztahovaček**“ – otevřených skupin v prostředí sociálních sítí, ve kterých docházelo k masivnímu šíření sexuálně explicitních materiálů dívek. Velká část obsahu byla tvořena materiály na hraně pornografie (často zachycujícími i osoby mladší 18 let).



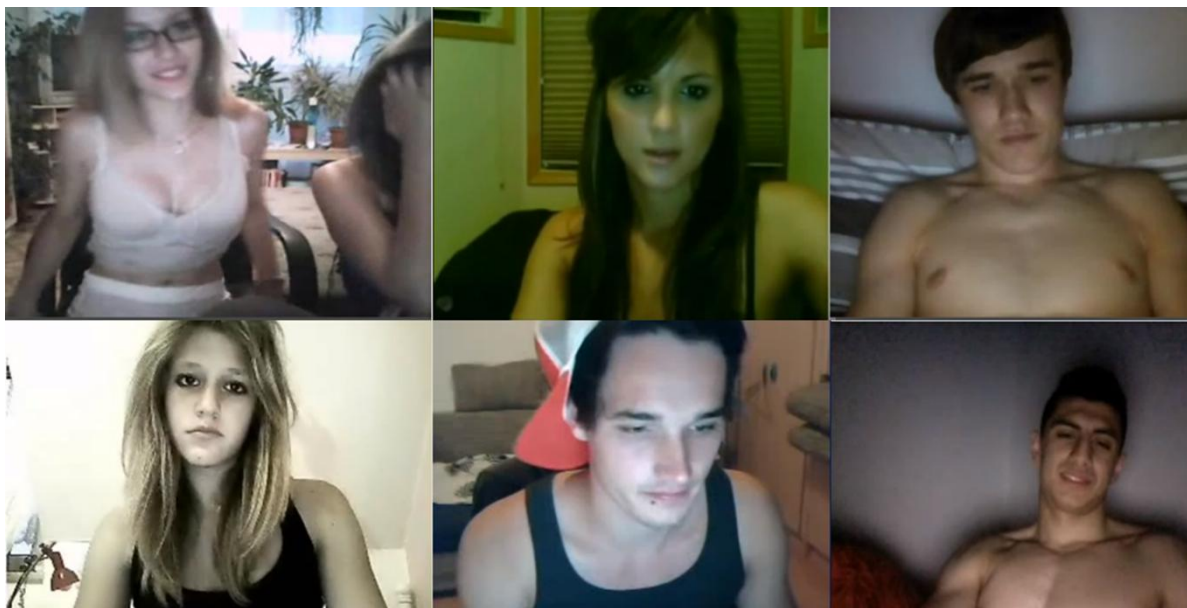
Obrázek: Ukázka profilů tzv. „roztahovaček“ na sociální síti Facebook



*Obrázek: Ukázka profilu dehonestujícího bývalé partnerky na sociální síti X (dříve Twitter)*

### 2.3 Webcam trolling a webcam blackmailing

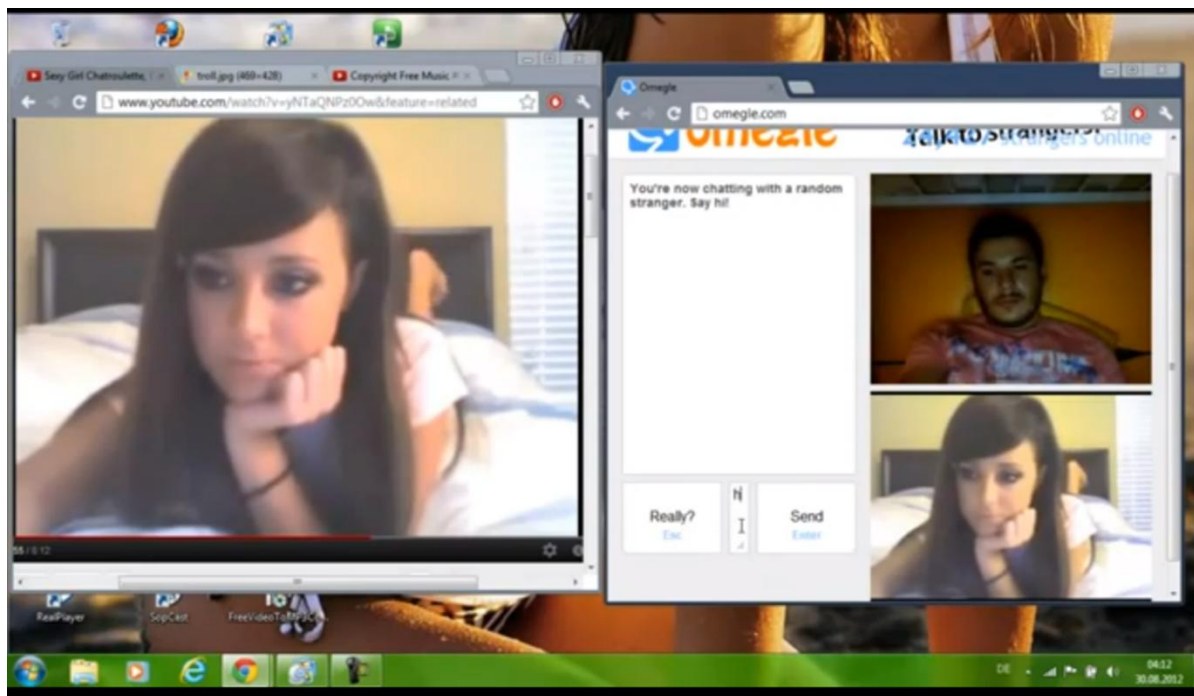
Webcam trolling je **druh podvodu, při němž útočník používá k oklamání oběti podvržený videozáznam, který oběť považuje za reálný obraz z webkamery.**[7, 8] Jedná se zpravidla o videosmyčku, která zachycuje reálnou dívku či chlapce při chatování.



*Obrázek: Ukázka podvržených videozáznamů (videosmyček)*

K připojení falešného záznamu do videochatu je potřeba mít speciální aplikaci, která simuluje **virtuální webkameru** a umožňuje do ní nahrávat videozáznamy. Tuto virtuální kameru lze propojit s webovými videochaty nebo instant messenger. S podvrženými videi se můžeme setkat na sociálních sítích

a službách, jako jsou např. Snapchat, Instagram, WhatsApp, Facebook, Telegram apod.



*Obrázek: Reálná ukázka použití virtuální webkamery s podvrženou videosmyčkou v prostředí již blokové (zrušené) videochatovací služby Omegle.*

**Cílem pachatele je vylákat z oběti co nejvíce osobních a citlivých údajů** – např. ji donutit, aby se před webkamerou svlékla, případně plnila jeho příkazy. Pachatel si po celou dobu videohovoru nahrává záznam oběti, který pak může dále zneužít, např. pro vydírání, vyhrožování, kyberšikanu, stalking apod. Webcam trolling řadíme mezi techniky tzv. sociálního inženýrství (sociotechniky).

## 2.4 Sebe-natáčení v intimních situacích a jeho rizika

V posledních letech se u dětí a dospívajících stále výrazněji prosazuje trend sebe-natáčení v intimních situacích, a to prostřednictvím webkamer, mobilních telefonů či živých streamovacích platform. **Tento nebezpečný trend potvrzují i sami policisté zaměřující se na sexuální a mravnostní delikty.** Samotný fenomén souvisí se zvyšující se dostupností technologií, kulturou vizuální komunikace a tlakem vrstevnických skupin na sdílení atraktivního či „dospělého“ obsahu. Pro děti a dospívající však představuje zásadní riziko, ať už jde o okamžité ohrožení, nebo dlouhodobé psychické a sociální dopady.

Motivace k takovému chování je různorodá. Často jde o snahu zapadnout do vrstevnické skupiny, získat uznání nebo být vnímán jako „dospělejší“. Řada dětí zkoumá svou identitu a sexualitu právě prostřednictvím online prostředí, které jim poskytuje pocit anonymity a menšího sociálního tlaku než interakce tváří v tvář. Důležitým faktorem, který může přispívat k tomu, že se děti a dospívající snadněji obnažují či natáčejí v intimních situacích, je **disinhibiční efekt** online prostředí. Tento psychologický jev popisuje tendenci lidí chovat se v prostředí internetu odvážněji, spontánněji a rizikověji než při osobním kontaktu. Dalším důležitým faktorem může být i **vliv současných influencerů, celebrit či online médií, kde je veřejné sdílení intimních materiálů mnohdy prezentováno jako běžné či atraktivní.** Do této aktivity navíc vstupují pachatelé, kteří mohou děti pomocí souboru manipulativních technik přimět k obnažování či jinému chování, jež si samotné děti původně ani nepřály. Podrobněji manipulaci

popisujeme v kapitole 3 Online seznamování, kybergrooming v podkapitole 3.1.5 Etapy manipulace.

Jakmile dítě jednou odešle nebo zveřejní intimní materiál, ocitá se v situaci vysokého rizika dalšího zneužití. Pachatelé často **pořizují skryté záznamy videohovorů či streamů** a následně je **používají jako prostředek k vydírání (sextortion)**. Typickým jednáním pachatele je postupné budování důvěry vedoucí ke stále intimnějším projevům dítěte a následné vyhrožování zveřejněním obsahu. V posledních letech se objevuje i trend v podobě sextortionu za účelem finančního obohacení, kdy pachatel požaduje peníze výměnou za nezveřejnění materiálu. **Děti v takové situaci zažívají silný stres, paniku a mnohdy se snaží situaci řešit samy, a to např. zasíláním dalších materiálů nebo platbami požadované částky, což jejich zranitelnost dále prohlubuje.**

Psychické dopady tohoto typu zneužití mohou být velmi závažné. Děti často pocítují **stud, vinu a strach z reakce rodičů či učitelů**, a to i přesto, že odpovědnost za vzniklou situaci nese pachatel. U poškozených dochází zpravidla k výrazným **úzkostným či depresivním stavům** a v některých případech také k **sebepoškozování nebo suicidálnímu jednání**. Oběť si může dlouhodobě nést narušenou sebeúctu a pocit nedůvěry ve vztazích, což může ovlivňovat i její budoucí partnerský či společenský život. Častým problémem je rovněž to, že děti se zdráhají o situaci komukoli říct kvůli strachu z trestu, což znesnadňuje včasné zásah a oblast prevence.

Z pohledu policie je nezbytné chápat tento fenomén jako komplexní problém, který přesahuje rámec samotného technologického zneužití. **Vyšetřování podobných případů vyžaduje citlivý přístup k oběti**, jež často jedná pod silným psychickým tlakem a může mít obavu o svou pověst či bezpečí. Policie by měla úzce spolupracovat se školami, OSPOD a dalšími odborníky, aby bylo dítěti poskytnuto adekvátní psychologické i sociální zázemí. **Důležitým prvkem je také prevence, zejména vysvětlování principů rizikového sdílení, důsledků ztráty kontroly nad digitálním obsahem a možností obrany proti manipulaci online.** Významný je i mezinárodní přesah tohoto fenoménu, jelikož řada pachatelů působí ze zahraničí a využívá anonymizační nástroje a globální platformy.

Celkově lze konstatovat, že sebe-natáčení dětí v intimních situacích představuje jeden z **nejrychleji se rozvíjejících fenoménů online rizik**. Propojuje zranitelnost dítěte, dynamiku dospívání a sofistikované postupy pachatelů. Schopnost policie porozumět motivacím dětí, mechanismům zneužití a psychickým dopadům je zásadní pro efektivní vyšetřování i prevenci dalších případů.



### 3 Online seznamování a kybergrooming

K moderním formám komunikace v online prostředí jednoznačně patří různé druhy seznamování – ať již prostřednictvím nejrůznějších komunikačních nástrojů, sociálních sítí nebo specializovaných seznamovacích aplikací (např. Tinder). Přestože může být online seznamování velmi efektivní cestou k nalezení ideálního protějšku, může také představovat nepříjemný a často traumatizující zážitek – a to především proto, že osoba, se kterou se seznamujeme, se za našeho kamaráda/kamarádku či přítele/přítelkyni pouze vydává a její úmysly nejsou vždy čisté. Zvláště nebezpečné je online seznamování pro děti, které se mohou stát terčem nejrůznějších více či méně sofistikovaných útoků – vydírání, vyhrožování či nebezpečného fenoménu, který se nazývá kybergrooming.

#### 3.1 Kybergrooming

Kybergrooming (child grooming) je **riziková forma komunikace v online prostředí, cílem je zmanipulovat vyhlédnutou oběť (dítě) a přimět ji k osobní schůzce v reálném světě**. Cílem pachatele je především přinutit dítě k osobnímu setkání mimo virtuální svět.

Na této schůzce pak může dojít např. k:

- **sexuálnímu zneužití oběti,**
- **zneužití dítěte k výrobě dětské pornografie,**
- **zneužití dítěte pro dětskou prostituci,**
- **fyzickému mučení,**
- **zneužití dítěte např. k terorismu.**

Kybergrooming je druhem **psychické manipulace**, ve které komunikuje dospělý uživatel (často pod falešnou identitou) s dítětem, přičemž využívá celou řadu **strategií** – např. **zrcadlení (mirroring), phishingu, profilování oběti, vábení a uplácení (luring), strategie snižování zábran dětí a mládeže zaváděním sexuálního obsahu do konverzace, izolační metody, strategie manipulace dětí prostřednictvím fotografií opačného pohlaví, webcam trollingu** apod.

Kybergrooming zahrnuje řadu **trestných činů, jako je § 175 TZ Vydírání, § 353 TZ Nebezpečné vyhrožování, § 186 TZ Sexuální nátlak, § 193b TZ Navazování nedovolených kontaktů s dítětem apod.** U kybergroomingu existuje vysoký stupeň latence, velké množství obětí tohoto typu útoku incident nenahlásí. Seriózní odhady hovoří o tom, že kybergrooming ohlásí maximálně 10 % zneužitých.

### **3.1.1 Kde ke kybergroomingu dochází?**

Kybergrooming zpravidla začíná v prostředí veřejné komunikační služby (např. běžně sociální sítě – Instagram, TikTok, Snapchat, Facebook, ale také na seznamkách apod.) a poté komunikace přechází do více soukromého prostředí (např. Instant Messengeru – WhatsApp, Telegram apod.). Ke kybergroomingu dochází i v prostředí veřejných chatů, internetových sezonek, inzertních a herních portálů a různých specializovaných portálů pro nezletilé uživatele.

**Co je důležité zdůraznit: Nebezpečné nejsou samotné služby, ale uživatelé, kteří je zneužívají!**

### 3.1.2 Kdo jsou pachatelé?

Pachatelé kybergroomingu tvoří heterogenní skupinu zahrnující uživatele s nízkým i vysokým sociálním statusem. V drtivé většině případů jsou pachatelé **muži**. Často jde o svobodné/rozvedené osamělé muže, existují však i případy, kdy měli pachatelé rodinu a děti. Komunikaci a vztahy s dětmi vnímají kybergroomeré jako méně ohrožující, cítí se ve vztazích s dětmi bezpečněji než ve vztazích s dospělými.

V řadě případů oběť útočníka zná (příbuzní, známí rodiny apod.). U většiny útočníků byl diagnostikován patologický zájem o děti (na různé úrovni, z různých důvodů – nejenom sexuálních). Maximálně 10 % pachatelů trpí pedofilní deviací s orientací na děti předpubertálního věku (Pozor, drtivá většina pedofilů dětem neubližuje!), zbytek pachatelů pak tvoří poměrně heterogenní skupinu zahrnující hebefily, efebofily, sadisty, jedince trpící asociální poruchou osobnosti, infantilismem, ale také např. různými sexuálními agresemi, exhibicionismem apod.

Pachatelé zahrnují všechny věkové skupiny, od 17 do 70 let. V řadě případů jsou pachatelé věkově blízcí oběti.

V českém prostředí se v kontextu s kybergroomingem a filmem **V síti** hovoří o pachatelích jako o tzv. **online predátorech**. Tento termín je poměrně široký, jelikož zahrnuje osoby nejen s nízkým, ale i vysokým stupněm společenské nebezpečnosti.

### 3.1.3 Kdo jsou oběti?

K obětem **patří jak dívky, tak chlapci v poměru zhruba 50:50, nejčastěji ve věku 11–17 let.**

K typickým obětem patří děti s nízkou sebeúctou, nedostatkem sebedůvěry či s emocionálními problémy, děti v nouzi, děti naivní a přehnaně důvěřivé, ale také např. ty, které jsou materiálně zabezpečeny, ale rodiče na ně nemají čas. Velmi častými oběťmi jsou pak děti, které v online prostředí hledají informace o sexu (pachatelé jim je rádi poskytují).

Podle výzkumu [Sexting a rizikové seznamování českých dětí v kyberprostoru](#) (Univerzita Palackého v Olomouci & O2 Czech Republic, 2017) je primárním zdrojem informací o sexu pro české děti právě internet.[9]

### 3.1.4 Jak dlouho probíhá manipulace dítěte?

Kybergrooming zakončený osobní schůzkou zpravidla trvá delší dobu, od **3 měsíců po několik let.** Ve filmu V síti trvala nejkratší manipulace dítěte (od prvotního seznámení k osobní schůzce) měsíc, průměrně jsou to 3 měsíce. Délka manipulace rovněž závisí na dosažení hranice zletilosti oběti.

### 3.1.5 Etapy manipulace

Manipulaci dítěte v rámci kybergroomingu lze rozdělit do 4 hlavních etap, ne všechny pak musejí proběhnout.

## **A. Příprava kontaktu**

V úvodní fázi pachatel **navazuje kontakt s vyhlédnutou obětí**. Může využít např. masivního spamování dětských uživatelů a náhodně je oslovovat, velmi často však také pracuje s **falešnou identitou** (předstírá, že je dítě) či **falešnou autoritou** (předstírá, že je pracovník nějaké významné instituce, firmy apod.).

## **B. Kontakt s obětí, budování vztahu**

V další fázi se snaží získat si sympatie oběti a stát se jejím virtuálním kamarádem, kterému se může s důvěrou svěřit. Současně pachatel usiluje o získání co největšího množství osobních a citlivých materiálů o dítěti (fotografie, videa). Využívá k tomu celou řadu manipulativních technik:

- **Zrcadlení (mirroring)**
- **Získávání osobních a dalších citlivých údajů (phishing)**
- **Profilování oběti (profiling)**
- **Vábení a uplácení oběti (luring)**
- **Snížování zábran dětí a mládeže zaváděním sexuálního obsahu do konverzace**
- **Snaha o izolaci oběti**
- **Strategie lákání skrze fotografii osoby opačného pohlaví**
- **Webcam trolling**

### **C. Příprava na osobní schůzku**

V této fázi je dítě vyzváno, aby šlo s pachatelem na osobní schůzku, např. na veřejném či neveřejném místě. Pozvánka na schůzku může být nenásilná, oběť však může být ke schůzce nucena (vyhrožováním, vydíráním apod.). V některých situacích pachatel využívá techniky překonávání věkového rozdílu mezi útočníkem a obětí (předstírá, že je např. rodič oběti, který jde dítě na schůzku vyzvednout).

### **D. Osobní schůzka**

Na první osobní schůzce nemusí automaticky dojít k útoku, může jít o test, zda dítě na schůzku skutečně dorazí (pachatel situaci sleduje z bezpečné vzdálenosti). Na osobní schůzce zpravidla pokračuje manipulace dítěte (různé formy přemlouvání, nabídek, focení dítěte apod.), případně dochází k útoku na oběť (sexuálnímu, fyzickému). Pozor, zážitek z první schůzky může být pozitivní, pachatelé dětem nosí např. různé dárečky, platí za ně občerstvení atd. Ke zvratu může dojít daleko později.

**Pozor, děti v online prostředí samozřejmě komunikují také se svými vrstevníky (jinými dětmi), se kterými si domlouvají schůzky. Vždy však existuje potenciální riziko! Proto doporučujeme na všechny schůzky chodit s dospělou osobou – ideálně rodičem.**

### 3.1.6 Současné trendy v kybergroomingu

V posledních letech dochází k výrazné proměně způsobů, jakými pachatelé navazují kontakt s dětmi v online prostředí. Zkušenosti z praxe a zejména z činnosti specializovaných útvarů Policie ČR ukazují, že **dnešní kybergroomeři stále častěji upouštějí od motivace setkat se s dítětem osobně**. Namísto toho **zůstávají téměř výhradně v digitálním prostoru, kde se cítí bezpečněji, co se týče rizika odhalení a anonymity**. **Cílem jejich jednání tak není fyzický kontakt, ale získání intimních materiálů dítěte, manipulace, vydírání nebo dlouhodobé udržování kontroly nad obětí.**

Jedním z nevyraznějších trendů je využívání **falešných videosmyček** (viz. podkapitola 2.3 Webcam trolling a webcam blackmailingu), které pachatelé prezentují jako živý obraz své osoby. Používají předem připravené záznamy (videosmyčky) atraktivních vrstevníků, často převzaté z veřejně dostupných videí, sociálních sítí či pornografických platforem. Pachatelé tyto smyčky spouštějí během videohovorů, čímž vytvářejí iluzi autentické komunikace. Dítě tak může nabýt dojmu, že interaguje s vrstevníkem, a snáze se nechá přesvědčit k obnažování nebo sexuálnímu projevu. Tento způsob komunikace značně ztěžuje okamžité odhalení pachatele a snižuje šanci, že oběť odhalí manipulaci včas.

Dalším významným trendem v online komunikaci pachatele s obětí je úsilí o **rychlé získání intimního materiálu, nikoli o dlouhodobé navazování vztahu, jak bývalo typické v minulosti**. Tento „zrychlený online grooming“ pracuje s intenzivním tlakem, flirtováním a psychologickým nátlakem, často

během několika minut či hodin od zahájení komunikace. Jakmile pachatel získá obrazový materiál, přechází k jeho zneužívání, např. k již zmiňovanému sextortionu, dalšímu vynucování intimního obsahu nebo předávání materiálů do uzavřených komunit.

Trend setrvávání pachatelů pouze v online prostředí má **zásadní dopady pro vyšetřovací praxi**. Pachatelé se vyhýbají fyzickému kontaktu, čímž snižují riziko, že budou identifikováni obětí, rodiči či policií. Často operují ze zahraničí, využívají anonymizační služby, VPN a účty navázané na jednorázové e-mailové adresy. Kombinace těchto faktorů vede k vyšší technologické anonymitě a často i k přeshraničnímu rozměru trestné činnosti. Vyšetřování tak vyžaduje rozsáhlou mezinárodní spolupráci a detailní analýzu digitální stopy.

### **3.1.7 Vybrané případy kybergroomingu zaměřené na děti**

#### **Případ: Piškot a Meluzín (ČR, 2007–2012)**

Homosexuálně orientovaní skautští vedoucí **Martin Mertl (22 let)** a **Milan Machát (20 let)** si na Facebooku vytvořili fiktivní dívčí profil, jehož prostřednictvím navazovali kontakt s nezletilými dětmi včetně 12letého heterosexuálního chlapce, který chodil do jejich oddílu.



*Obrázek: Martin Mertl (22 let) a Milan Machát (20 let)*

Chlapci pod falešnou identitou psali, jak se jim líbí, a postupně si s ním utvořili vztah. Chlapec se po čase chtěl s dívkou sejít, musel však podat „dva důkazy lásky“ (nahou fotografii a fotografii z homosexuálního sexu). Fiktivní dívka posléze chlapce prostřednictvím Facebooku vydírala.

Chlapec se s vydíráním svěřil vedoucím oddílu (pachatelům), kteří mu přislíbili pomoc tím, že mu pomohou společně fotografovat a natáčet homosexuálně laděné fotografie a videa. Za tímto účelem s chlapcem provozovali sex a u toho se fotili a natáčeli. Vzniklé materiály poté chlapec zasílal fiktivní dívce, aby se vyhnul dalšímu vydírání.

Po zhlédnutí filmu *Seznam se bezpečně* chlapec celou situaci oznámil matce, která věc předala Policii ČR, jež případ rozkryla. Podle obžaloby skautští vedoucí z Ústí nad Labem zneužili celkem **39 dětí (36 chlapců a 3 dívky)** nejčastěji ve věku 10–13 let. V listopadu 2013 byli odsouzeni na 10 let odnětí svobody. „Docházelo k análnímu styku, orálnímu styku, točení videa, fotografování nahého těla,“ vypověděla matka týraného chlapce. Muži chlapci hrozili, že pokud jim nebude po vůli, jeho fotografie pošlou všem kamarádům a spolužákům. Ze strachu je poslouchal na slovo.

Okresní soud v Brně 19. září 2019 podmíněně propustil Martina Mertla (od listopadu 2019 je na svobodě). Odseděl si 7 let a 8 měsíců (2,5 měsíce za jedno zneužití dítě).

V dubnu 2021 byl propuštěn i Milan Machát. Vězení opustil po 9 letech a 10 dnech. Za bývalého skautského vedoucího se před soudem zaručili také jeho rodiče. Jejich dobrozdání bylo součástí samotné žádosti o propuštění.

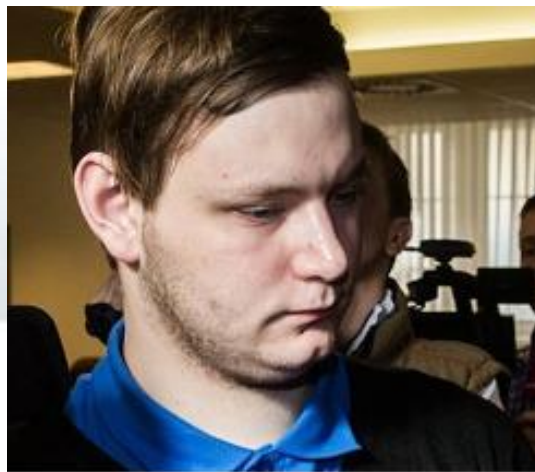
### **Případ: Lukáš Bako (ČR, 2014)**

Lukáš Bako (21) od roku 2010 do svého zadržení 18. 8. 2014 prostřednictvím sociální sítě Facebook a služby Skype zneužil desítky dívek ve věku 10–18 let.

Na Facebooku a Skype se s dívkami nejprve seznámil, vylákal od nich intimní materiály, a pokud dívka odmítla osobní setkání, začal ji vydírat.

Byl obžalován např. z vydírání, sexuálního nátlaku, znásilnění, pohlavního zneužívání, zneužití dítěte k výrobě pornografie apod. Poškozených dívek bylo v žalobě 47, skutků přes 60 a trestných činů cca 90. Podle státní zástupkyně nebyl počet zneužitých dívek zdaleka konečný.

V roce 2016 odsouzen na 8,5 roku ve věznici s ostrahou.



*Obrázek: Lukáš Bako (21)*

## Prevence

U kybergroomingu je naprosto klíčová úloha prevence. Dítě by mělo pochopit, **jak se na internetu chovat co nejbezpečněji, jakou hodnotu mají osobní údaje, jak si ověřit, s kým ve skutečnosti komunikujeme, a jak mohou být schůzky s online přáteli, které neznáme z reálného světa, nebezpečné.**

### Pravidla pro děti:

1. Nenechte se oklamat sliby virtuálních útočníků (mohou vám slibovat přátelství, lásku, pokračování vztahu v reálném světě, peníze, dárky apod.). Uvědomte si, že lidé na internetu mohou lhát!
2. Všimněte si nesrovnalostí v komunikaci (útočník například udává různý věk, mění informace, které vám o sobě sdělil dříve apod.).
3. Uvědomte si, proč by někdo chtěl za každou cenu udržet internetový vztah nebo obsah komunikace v tajnosti.
4. Vytýčte si své osobní hranice s ohledem na sex. Nepřijímejte ani neodesílejte jiným uživatelům materiály sexuální povahy.
5. Ve virtuálním prostředí nikomu nesdělujte své osobní údaje (zejména své fotografie).
6. Nikdy nechodte na osobní schůzku bez vědomí rodičů. Uvědomte si, co všechno se vám na schůzce může stát a jak to může být riskantní.

7. Dejte si pozor na to, s kým se bavíte a o čem. Internetová komunikace vypadá jako anonymní, ale není. Nechcete přece, aby vás „internetový známý“ vystopoval v reálném světě nebo aby vás nutil dělat něco, co nechcete.

8. Otestujte si osobu, se kterou komunikujete – např. pomocí fotografie, webkamery apod.

### **Pravidla pro rodiče:**

1. Komunikujte se svými dětmi o tom, co dělají na internetu. Uvědomte si, že i když je vaše dítě doma a sedí u počítače, nemusí to znamenat, že je v bezpečí!

2. Počítač dítěte nechejte na veřejně dostupném místě, například v obývacím pokoji, kde jej můžete namátkou kontrolovat (v závislosti na věku).

3. Vysvětlete dětem, jaká rizika může internet představovat.

4. V případě, že se vaše dítě dostane do problémů spojených s kybergroomingem, nepoužívejte nefunkční metodu zákazu práce s počítačem a internetem! Uvědomte si, že když dítěti doma zakážete počítač a internet, najde si jinou cestu, jak se k těmto nástrojům dostat (u kamaráda, ve škole, prostřednictvím mobilního telefonu atd.).



## 4 Rizikové výzvy v online prostředí

Rizikové výzvy (tzv. dangerous challenges) představují fenomén, který může být skutečně nebezpečný a v extrémních případech může končit vážnými zraněními, či dokonce smrtí. Jedná se o rizikové a v některých případech **nebezpečné online návody, rady a doporučení** vybízející k napodobování nežádoucího chování.[10, 11] Často je součástí dané výzvy vytváření fotografií či videí jako důkazu splnění zadaného úkolu a následné sdílení na internetu. Tímto způsobem se mohou výzvy šířit mezi široký okruh dalších lidí.

### Seznam vybraných rizikových výzev na internetu:

- TikTok Fire Challenge
- Fireball Challenge
- Tide Pod Challenge
- Ice bucket challenge
- Eyeballing challenge
- Kylie Jenner Lip Challenge
- Condom Challenge
- Duct Tape Challenge
- Cinnamon Challenge
- Choking Game
- Blackout Challenge
- Salt and Ice Challenge
- The Snorting Challenge
- Ghost Pepper Challenge

- Planking
- Blue Whale challenge
- MOMO Challenge

## **Vybrané rizikové výzvy v prostředí internetu:**

### **A. Kylie Jenner Lip Challenge**

Výzva nabádá k tomu, aby si děti po vzoru modelky Kylie Jenner zvětšovaly rty, a to tak, že si k ústům přiloží nádobku, ze které odsají vzduch, a podtlakem dosáhnou dočasného zvětšení rtů.



*Obrázek: Ukázka důsledků výzvy Kylie Jenner Lip Challenge*

**Možné následky:** hrozí riziko poškození rtů – popraskání, krvácení apod.

## **B. Ghost Pepper Challenge**

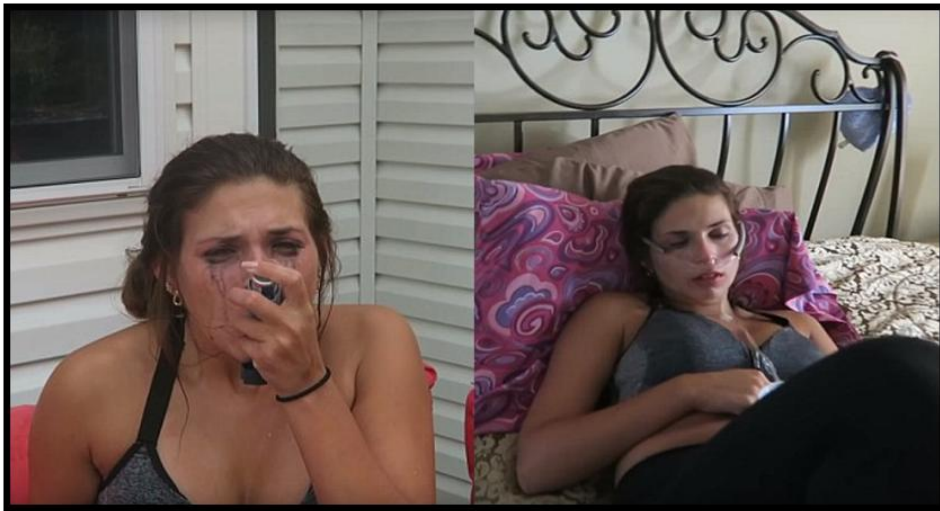
Výzva k požívání velmi pálivých papriček.

**Možné následky:** potraviny s vysokým obsahem kapsaicinu mohou kromě děsivého pálení přivodit i dechové potíže, nevolnost, případně až zvracení. V extrémních případech smrt.

### ***Případ: Lizza Wurst (18) a Sabrina Stewart (22)***

Dvě mladé dívky Lizzy Wurst (18) a její kamarádka Sabrina Stewart (22) se rozhodly uskutečnit velmi nebezpečnou challenge – sníst papričku Carolina Reaper. Jedná se o třetí nejpálivější papričku na světě (2,2 milionu jednotek pálivosti Scovilleovy stupnice – vysoký obsah kapsaicinu).

Dívky začaly okamžitě panikařit. Jedna měla hysterický záchvat, nemohla dýchat, dostala křeče, brečela a chtělo se jí zvracet. Byla přivolána lékařská pomoc. Její kamarádka se snažila pálivost překonat vodou, což není vhodné řešení, po chvíli zaháněly pálivost kusem suché housky.



*Obrázek: Ukázka důsledků výzvy Ghost Pepper Challenge*

### C. Duct Tape Challenge

Výzva nabádá k tomu, aby si dítě či dospívající nechali oblepit tělo lepicí páskou a snažili se z této pozice vyprostit.

**Možné následky:** při snaze vyprostit se ze sevření lepicí pásky bývá celá řada vážných úrazů (aktér výzvy nemůže reflexně při pádu využít ruku).



*Obrázek: Aktéři výzvy Duct Tape Challenge*

## **Případ: Skylar Fish (14)**

Skylar Fish z USA si při realizaci této výzvy vážně poranil hlavu o rám okna a byl hospitalizován. Utrpěl mozkové aneurysma (operace si vyžádala 48 stehů), zároveň si vážně poškodil levé oko, na které již pravděpodobně nebude vidět.



*Obrázek: Skylar Fish – důsledky výzvy Duct Tape Challenge*

## **Prevence**

Preventivní programy pro žáky jsou zaměřeny zejména na bezpečnost v online světě a na projevy rizikového chování na internetu, jako jsou kyberšikana, kybergrooming (online predátoři), seznamování, sexting, závislosti, well-being, online podvody.

Téma rizikových výzev je velmi obtížné zařadit do preventivních aktivit zaměřených na děti. Hrozí nebezpečí nápodoby, tudíž je nutné k danému tématu přistoupit velmi obezřetně, a pokud možno v podobě aktivit, které omezí již

zmíněnou nápodobu. Velmi efektivně se dají využít pracovní listy, které pro ilustraci uvádíme v publikaci **Bezpečné chování na internetu pro kluky a pro holky**. [12]



107

© Bagoš – Bezpečné chování na internetu pro kluky a pro holky  
www.bagoš.cz

- KDO JE VLADNĚ ZODPOVĚDNÝ ZA TO, CO SE DĚTI STANOU A PROČ?  
No jo, kdo za to vlastně může?  
To je docela těžká otázka...
- MĚL BY TUKTOR (A DALŠÍ SOCIÁLNĚ SÍTĚ) TENTO TYP OBRABU BLOKOVAT A PROČ?
- ZKOUŠELA JSTE NĚKDY VY SAMI NÁPODOBIT CHOVÁNÍ NĚKTERÉHO INFLUENCERA, KTERÉHO ZNÁTE ZE SOCIÁLNÍCH SÍTÍ? DOKÁZALI BYSTE POPSAT, CO JSTE SE ZKOUŠELI A PŘLO TO POKLE VĚL NEBEZPEČNĚ?
- SETKALI JSTE SE S VY SAMI S NĚKTERÝMI NEBEZPEČNĚMI VÝZVAMI, ANEŽ BYSTE JE TŘEBA PŘEHLÍDLI A KDE NA NĚ NA INTERNETU NAJÁZDĚTE?

**NÁVY ČALLENGA**

**KDE JE S NĚ MŮŽEME SETKAT?**

• ČALLENGE MŮŽOU BŮT UVĚŠTĚNÉ I PROTI VĚCÍM. DOKÁZALI BYSTE UVĚŠTĚT PŘEKLAD NĚKTERÉ POUŽITĚNĚ VÝZVY?

108

© Bagoš – Bezpečné chování na internetu pro kluky a pro holky  
www.bagoš.cz

**AKTIVITA: NEBEZPEČNĚ VÝZVY (CHALLENGE)**

- PŘEČTĚTE SI ČLÁNEK O TOM, CO SE STALO TĚLE DĚTI DĚTI ČRANOVĚ, NĚKTERĚ OTVÁRETE TUKTORŮ. POUĚ JODPOVĚTE NA NĚKTERÉ Z OTÁZEK.

• TO, CO SI DĚTI VYKROUĚLA, BYLA BĚHÁ PĚV. **NEBEZPEČNĚ VÝZVY (CHALLENGE)**, KTERĚ KLUKE TUKTORĚM. DOKÁZALI BYSTE UVĚŠTĚT, VĚM JE VLADNĚ TAKO VÝVA NEBEZPEČNĚ?

• PŘEČ VLASTNĚ LIDE TYTO VÝVY PŘEČ, CO JE K TOMU MOTIVUJET?

• JAK BYSTE SE ZACHOVALI, KDUŠTE BYLI INFLUENCEREM A ZESTELI, ŽE SI NĚKTERĚ DĚČ UVĚŠTĚLO, PROČTĚ SE POKUŠTELO NĚKTERĚM VĚŠTĚ?

*Obrázek: Ukázky pracovních listů z publikace Bezpečné chování na internetu pro kluky a pro holky.*

O problematice rizikových výzev je třeba informovat zejména rodiče dětí, kteří by měli znát rizika výzev i zabezpečení služeb internetu (sociálních sítí, videoportálů apod.) proti nevhodnému obsahu a rozpoznat případná poranění a vnější znaky doprovázející rizikové výzvy apod. Je důležité, aby rodiče s dětmi komunikovali a zajímali se o online svět dětí.



## 5 Online podvody

V online prostředí v posledních letech radikálně narůstá počet podvodů, které představují nejrozšířenější druh kybernetické kriminality. Můžeme říci, že podvody se postupně přesunuly z reálného světa právě do internetového prostředí a dynamicky se zde rozvíjejí – ještě před několika lety jsme například neznali podvody spojené s tzv. kryptoměnami, dnes jsou naprosto běžné. Policie ČR eviduje mnoho nejrůznějších typů online podvodů (tzv. scamu), jejichž společným jmenovatelem je úsilí internetových útočníků připravit nás o finanční prostředky či osobní/citlivé údaje. V této kapitole si přiblížíme nejčastější typy online podvodů spadajících pod § 209 TZ (TČ Podvod) či pod § 234 Neoprávněné opatření, padělání a pozměnění platebního prostředku.

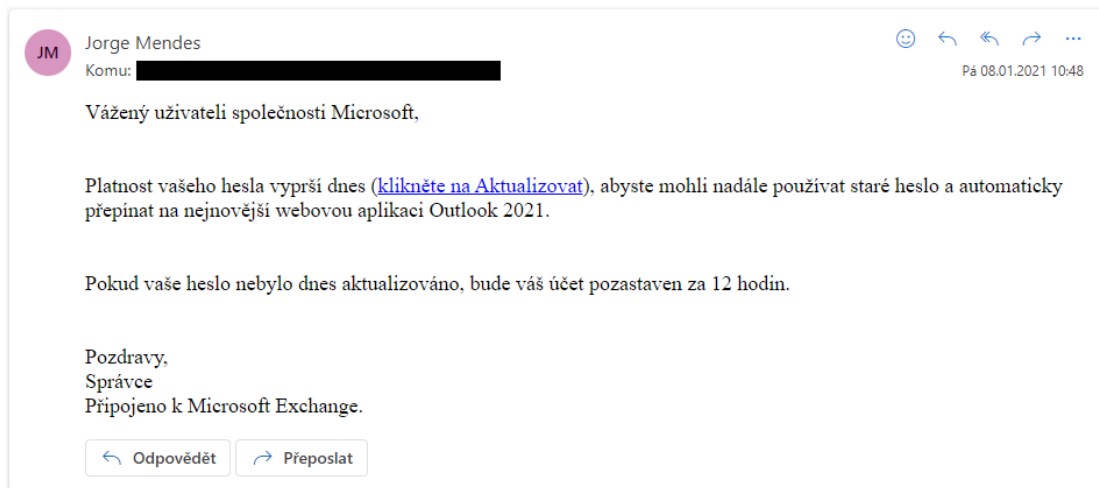
### 5.1 Phishing

**Phishing** je druh internetového podvodu, který je **zaměřen především na získání (krádež) osobních či jiných citlivých údajů**. Phishing se šíří zejména prostřednictvím e-mailové komunikace, v posledních však letech stále častěji proniká do prostředí sociálních sítí. Phishingové zprávy velmi často napodobují komunikaci nejrůznějších institucí, jako jsou např. banky, pojišťovny, pošta apod. Phishingové zprávy se často snaží vyvolat v uživateli pocit naléhavosti a nutnosti na zprávu reagovat.

Uživatelům je obvykle doručen důvěryhodně vypadající e-mail (často obsahující loga instituce, odkazy na reálné stránky instituce a informace, převzaté přímo z instituce – banky, pojišťovny, spořitelny), který oznamuje, že je z nějakého důvodu nutné přihlásit se na bankovní účet (pomocí jména a hesla). Uživatel,

který uvěří sdělení, klikne na odkaz uvedený v e-mailu. Poté dojde k připojení na falešné internetové stránky, které jsou často věrnou kopií stránek banky uživatele (stejný design, často stejný obsah, stejná loga, pouze drobné odlišnosti zejména v internetové adrese). Pokud se na stránky přihlásí, dojde ke krádeži údajů k účtu. V minulosti bylo phishing poměrně snadné odhalit, protože sdělení obsahovala pravopisné a gramatické chyby, v současnosti jsou však tyto zprávy díky použití umělé inteligence téměř bez formálních chyb a je nutné všimnout si jiných znaků.

Podobně se phishing šíří také v prostředí sociálních sítí – po kliknutí na odkaz jsou uživatelé přeměrováni na věrohodnou napodobeninu sociální sítě a vyzváni k přihlášení. Pokud se přihlásí, dojde k odcizení přihlašovacích údajů.



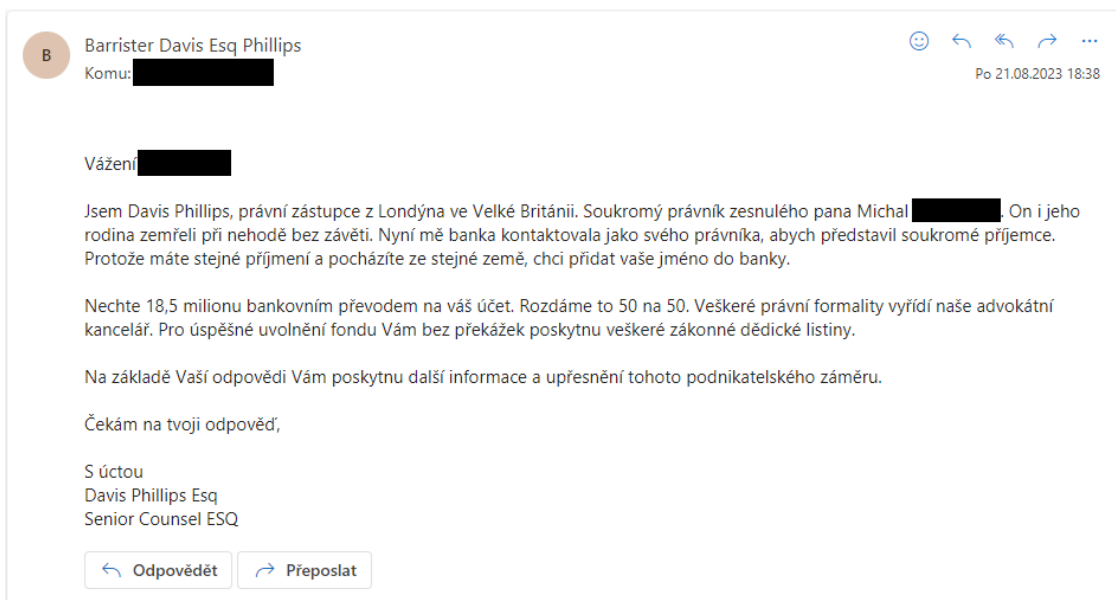
*Obrázek: Ukázka phishingového emailu*

## 5.2 Vishing

Vishing – hlasový phishing – je telefonní podvod, kdy pachatel obvolává své oběti, představí se např. jako zaměstnanec banky (nebo jiných společností) a sdělí, že účet oběti je napaden a on jediný může pomoci zachránit finanční prostředky. K záchraně účtu potřebuje bezpečnostní údaje k internetovému bankovníctví (ID a heslo, datum narození) nebo k platební kartě (číslo, platnost, jméno na kartě, PIN apod.). Následně se snaží oběť přesvědčit, aby předala bezpečnostní kódy z SMS nebo potvrdila operaci v aplikaci či zaslala bankovní klíč.

## 5.3 Scam419

K velmi rozšířeným typům podvodů patří také tzv. scam419. Scam419 je druhem **podvodu, který známe pod alternativním názvem „nigerijské dopisy“**. Číslovka 419 v názvu podvodu je číslo paragrafu nigerijského trestního zákoníku, který se zaměřuje právě na podvody. Základním principem tohoto podvodu je nabídka získání finančních prostředků ze zahraničí, které vznikly např. v rámci fiktivního dědického řízení. K tomu, abyste tyto finance mohli získat, musíte zaplatit „poplatky“ (v řádech desítek až stovek tisíců korun) za převod jmění ze země původu (obvykle z některé ze zemí Afriky) na účet v ČR. Samozřejmě jde o podvod a slibované finanční prostředky nikdy neobdržíte.



*Obrázek: Ukázka podvodného e-mailu v rámci Scam419*

## 5.4 Romance scam

Romance scam je jedním z klasických online podvodů a čas od času se s ním setkají uživatelé různých druhů online sezonek a seznamovacích diskusních skupin, na romance scam můžeme narazit také v rámci běžné e-mailové komunikace. Princip je prostý – cílem **pachatele je navázat s vyhlédnutou obětí v online prostředí romantický vztah a vylákávat z ní postupně co nejvíce financí, které pak putují do zahraničí. Pachatel si v rámci komunikace vymýšlí nové a nové historky, proč je nutné peníze odeslat, že na tom závisí jeho život apod. Romance scam bývá doprovázen příslibem rychlého zbohatnutí, protože je pachatel podle svých slov finančně zajištěn**

**a stejně tak zajistí vyhlédnutou oběť.** V posledních letech se pachatelé velmi často vydávali za **americké vojáky** či **lékaře pracující na zahraničí misi**, nově poradna E-Bezpečí zachytila případy, kdy pachatel předstírá, že je stavební inženýr, který žije v blízké zemi (např. Německu) a chce se seznámit, následně odstěhovat do ČR, postavit si zde dům apod.

### **Vybrané případy**

Osamělou ženu (57) z Olomoucka oslovil na Facebooku muž středních let (vdovec) Phillip Williams, který představil jako armádní lékař působící na misi v Jemenu. S ženou komunikoval česky s pomocí překladáče. Počáteční nezávazná konverzace poměrně rychle přerostla v komunikaci plnou citů.



*Obrázek: Profilová fotografie použita pachatelem*

Muž ženě vyznal lásku a plnou důvěru, napsal jí, že se k ní odstěhuje a že než přijede, odešle na její adresu balík se svými osobními dokumenty, elektronikou a všemi penězi (**2,5 mil. dolarů**). Žena s odesláním balíku na svou adresu souhlasila. Balík byl odeslán, ovšem nastal **PROBLÉM** – zadržela jej celní zpráva Turecka a požadovala vysoký poplatek za jeho vydání.

Muž ženu prosil o zaplacení celních poplatků, penále za pozdní platbu apod. Psal jí, že pokud mu nepomůže, bude jeho syn sirotkem, že se nikdy neuvidí, protože je v balíku celý jeho majetek.

Žena s mužem komunikovala **od 25. dubna do 14. června 2022**.

Celkem pachatel od ženy vylákal **14,61 mil. Kč**. Peníze žena postupně odcizila z účtu školy, kde působila jako účetní.



*Obrázek: Fotografie důvěřivé ženy u soudu*

Soud s důvěřivou ženou proběhl 9. 2. 2023, byla odsouzena k **trestu odnětí svobody na 4 roky a propadnutí majetku.**

## **Vybrané případy zachycené poradnou projektu E-Bezpečí**

### **Případ Jana 60 let (ČR, 2018)**

Paní Janu kontaktoval emailem neznámý šedesátiletý Američan, který jí nabídl odměnu za převod peněz a zlata, jež potřebuje odeslat z Ghany (kde zdědil velký majetek) do ČR. Za tento převod oslovené paní nabídl odměnu v řádech milionů, a navíc jí také nabídl partnerství a následný sňatek!

K tomu, aby bylo možné převod ze zahraničí uskutečnit, bylo ovšem nutné uhradit manipulační poplatky ve výši 11 000 eur. Paní Jana se nechala přemluvit, vzala si spotřebitelský úvěr a poplatky uhradila.

Američan se v komunikaci odmlčel.

Za krátký čas se ozval jeho „právní zástupce“, který paní napsal, že Američan omylem srazil v Ghaně 13letou dívku a sedí za to ve vězení. K propuštění z vězení potřebuje 7 000 eur na kauci, přičemž sliboval, že vše vrátí, jakmile se dostane na svobodu.

Paní Jana opět chtěla muži pomoci, a proto se rozhodla prodat svoje auto... Její syn kontaktuje poradnu E-Bezpečí...

## 5.5 CEO scam (BEC scam, Boss scam)

Boss scam (či CEO/BEC fraud, fake president) je druhem podvodu, ve kterém pachatelé předstírají, že jsou vaši nadřízení (např. ředitelé), a požadují, abyste převedli peníze z firemního účtu na účet jiný, např. na zafinancování konkrétního projektu, případně proplatili fiktivní fakturu či fiktivní platební příkaz. Podvod využívá především nepozornosti zaměstnanců, kteří jsou zvyklí se svým nadřízeným běžně e-mailem komunikovat a již si neověřují, od koho příkaz ve skutečnosti přišel.

Podvod začíná nenápadně, na firemní e-mail nám dorazí **zpráva, která se tváří, jako by ji odeslal váš nadřízený** – odesílatel se skutečně „jmenuje stejně“. Na první pohled se tedy může zdát, že opravdu pochází od vašeho nadřízeného.



<input type="checkbox"/>	ResearchGate	☆ Joel Billieux recommended this article –	Dnes 10:01
<input type="checkbox"/>	<b>Kamil Kopecký</b>	☆ <b>Platba</b>	 Dnes 9:45
<input type="checkbox"/>	Robert Plaga	☆ Pozvánka na raut	 Dnes 9:40
<input type="checkbox"/>	Václav Pisecký	☆ Opékání špekáčků s Policií ČR	Dnes 9:16

*Obrázek: Běžná e-mailová stránka se seznamem zpráv, pachatel využívá jméno Kamil Kopecký*

Ve zprávě je pak informace např. o tom, že dnes musíme urgentně uhradit nějakou částku na konkrétní bankovní účet – zpravidla v zahraničí. Ve skutečnosti však jde o podvodný e-mail, který těží z nepozornosti pracovníků (především u velkých firem).



*Obrázek: E-mailová adresa odesílatele neodpovídá, jde o podvod*

Ochranou je především **správně nastavený způsob předávání informací uvnitř firmy** (firemní komunikace), kdy jsou veškeré platební žádosti skutečně ověřeny. To však platí i mimo firemní sektor – vždy si ověřme, že v případě online plateb skutečně komunikujeme s oprávněnou osobou. Toto lze snadno provést třeba telefonicky.

## 5.6 Invoice scam

Invoice scam je druh podvodu, který v českém prostředí známe pod názvem „**podvodné faktury**“. Princip podvodu je jednoduchý, internetoví podvodníci rozesílají fiktivní faktury a využívají nepozornosti ekonomického personálu, který je ochoten fakturu proplatit. V některých případech pak podvodná faktura ve formě přílohy k e-mailu obsahuje virus (např. ransomware), který infikuje firemní počítač, či dokonce celou počítačovou síť.

>  
Vážená paní, vážený pane,  
děkujeme za projevenou důvěru v internetové obchody obchody24.cz.  
Tímto emailem potvrzujeme, že jsme v pořádku přijali vaši objednávku.

Číslo objednávky (variabilní symbol): Q4B1A400FD38103 Datum a čas  
objednávky: 10.01. 42:40 Kontaktní údaje:  
Alice Barešová  
+420 603 398 329

Vaše objednávka:  
-----  
EPSON Stylus C64, bílá: 1 x 1 903,00 Kč =1 903,00 Kč Doúprava PPL: 70  
Kč  
-----  
Celková cena nákupu vč. DPH: 1 973,00 Kč Způsob platby: Platba předem -  
platební karta  
Poznámka: Potvrzení platby a fakturu najdete v přiloženém souboru  
(ebill3431866.zip)  
-

Nyní prosím vyčkejte na našeho operátora, který se s vámi spojí  
maximálně do 1 pracovního dne a dohodne podrobnosti ohledně Vaší  
objednávky.

*Obrázek: Invoice scam ukázka*

## 5.7 Reverzní internetové podvody (R.I.P.)

Reverzní internetové podvody (R.I.P.) jsou zaměřeny na prodávající na inzertních portálech. Když prodejce zveřejní inzerát, ozve se mu kupující, který projeví vážný zájem o nabízené zboží. Zeptá se, zda by nevadilo **doručení Zásilkovnou, DPD, PPL, kurýrem** apod. Jakmile prodejce souhlasí, zájemce mu sdělí, že vše zařídí a pošle odkaz na platební bránu, kam složí peníze. Kupující zpravidla požaduje další údaje, např. osobní údaje a údaje k platební kartě, může také poslat odkaz na přepravní společnost, která kromě platby zajistí i přepravu zboží. Kupující je velice ochotný, prodávajícího přesně instruuje, co má dělat.



Obrázek: Ukázka konverzace prodávajícího a zájemce v rámci reverzního internetového podvodu (R.I.P)

## 5.8 Prevence a boj proti online podvodům

Součástí efektivní prevence online podvodů je nejen technická ochrana, ale také systematické zvyšování digitální gramotnosti uživatelů. Kromě tradičních vzdělávacích aktivit se v poslední době objevují nové nástroje zaměřené na praktickou osvětu. Jedním z nich je web **Prokoukni to!** ([www.panprokoukl.cz](http://www.panprokoukl.cz)), který nabízí přehledné návody, ukázky typických podvodných praktik a interaktivní materiály pomáhající uživatelům rozpoznávat rizikové situace v online prostředí. Tato iniciativa přispívá k tomu, aby se lidé dokázali lépe orientovat v kybernetických hrozbách a aktivně předcházeli útokům, které cílí na lidský faktor – nejčastěji zneužívaný prvek bezpečnosti. Pokud je osvěta kombinována s vhodnými bezpečnostními nástroji a odpovědným chováním uživatelů, významně se snižuje riziko úspěšných online podvodů.

Web **Prokoukni to!** nabízí i vlastního **AI chatbota** pojmenovaného **Pan Prokoukl**, který uživatelům pomáhá s orientací v podezřelých situacích. Umožňuje rychle vyhodnotit různé formy online podvodů, poradí, jak reagovat na neobvyklé zprávy, a nabídne praktické tipy, jak se chránit. Díky tomu mají lidé po ruce jednoduchý a srozumitelný nástroj, který jim dokáže pomoci, když si nejsou jistí.

Kromě samotné osvěty je ale důležité i to, aby lidé v běžném online životě dodržovali několik základních pravidel. Vyplatí se **dvakrát ověřit, s kým si píšeme, nedůvěřovat podezřelým zprávám a pravidelně si chránit účty silnými hesly nebo vícefaktorovým ověřením**. Pomáhá také **udržovat zařízení aktuální a vědět, kam se obrátit**, pokud něco nevypadá v pořádku.

Když se tyto jednoduché návyky spojí s lepší informovaností a dostupnými nástroji, výrazně se snižuje šance, že člověk naletí online podvodu.



Obrázek: Úvodní obrazovka webu **Prokoukni to!** ([www.panprokoukl.cz](http://www.panprokoukl.cz))

## 6 Děti, sociální média a sociální sítě

Jak již bylo naznačeno, děti jsou velmi aktivními uživateli nejrůznějších sociálních sítí, sociálních médií a velkého množství komunikačních nástrojů.



TikTok



Instagram



Snapchat



Discord



YouTube



BeReal



WhatsApp



Telegram



Messenger



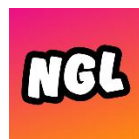
Tellonym



Facebook



Reddit



NGL

*Obrázek: Ikony a názvy online služeb a nástrojů často využívaných dětmi*



## **7 Rizika spojená s umělou inteligencí**

Velkým tématem současnosti je bezesporu umělá inteligence, především pak její generativní formy. Umělá inteligence přináší mnoho pozitiv a dokáže člověku efektivně pomoci v řadě profesí, zároveň však s sebou nese také rizika, na která se zaměříme právě v této kapitole. Detailněji se otázkám AI rizik věnuje publikace **„Umělá inteligence: Rizika a odpovědnost“**, která vznikla s podporou Ministerstva vnitra České republiky.

### **7.1 Nástroje generativní umělé inteligence dělají chyby**

Přestože jsou současné nástroje umělé inteligence natrénovány na velkých znalostních databázích, mohou se dopouštět nepřesností, či přímo chyb, jež mohou být způsobeny tím, že nástroj AI nepochopil vaše zadání (prompt) či nemá danou informaci k dispozici, protože je informace příliš specifická. Dále je třeba počítat s tím, že mnohé jazykové modely nepracují se zcela aktuálními informacemi – např. model GPT 5.1 obsahuje data k září 2024, a pokud bychom potřebovali novější informace, nástroj ve své verzi zdarma nám správnou odpověď nedá. V případě ChatGPT lze toto omezení překonat např. použitím vhodného rozšíření (pluginu), který umožní přistupovat k aktuálním informacím na internetu, případně vyzkoušením jiných nástrojů – např. Bing Chat či Google Bard, jež přístup k online informacím mají. Je tedy třeba připomenout, že informace, které nám AI generuje, je nutné vždy ověřovat.

## 7.2 Problém s autorskými právy

Jeden z problémů, který je s umělou inteligencí spojen, se týká autorského práva. Umělá inteligence je totiž natrénována na materiálech vytvořených lidmi, ty podléhají autorskému právu, a tedy i autorskoprávní ochraně. Přestože je výstup umělé inteligence odlišný od původních zdrojů (knih, článků, fotografií...), ve velké části případů jde vlastně jen o parafráze myšlenek konkrétního autora, platí povinnost tohoto autora také citovat. Řada modelů generativní AI však původní zdroje necituje a autory neuvádí. Co je potřeba připomenout: **Umělá inteligence není autorem díla – tím je vždy člověk**, dílo umělé inteligence nelze také do jisté míry autorsky chránit (záleží např. na míře kreativity, díky které dílo vzniklo). Při využití AI k tvorbě obsahu by tedy lidští autoři měli vždy uvést, že využili umělou inteligenci. Stejně tak je potřeba připomenout, že drtivá většina firem nabízejících nástroje generativní umělé inteligence má ve svých podmínkách uvedeno, že se **zříkají odpovědnosti za vytvořený obsah a odpovědnost mají vždy uživatelé**.

## 7.3 Podvádění ve škole

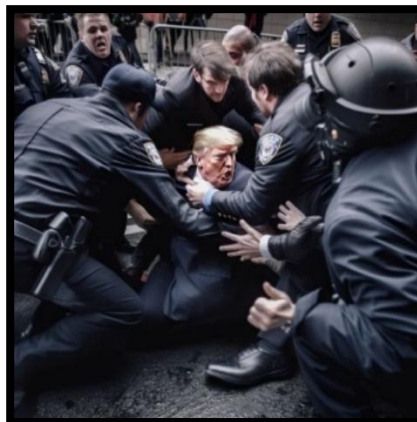
Každou moderní technologii je možné pozitivně využít, ale také zneužít. V případě umělé inteligence se nabízí možnost zneužití např. tak, že si žáci s její pomocí vypracují domácí úkoly (referáty, seminární práce, eseje, úvahy, ale také např. slovní úlohy apod.) a předloží je učiteli jako své vlastní. Ve vysokém školství pak hrozí např. zneužití AI při tvorbě kvalifikačních prací – student si může nechat pomocí AI vygenerovat teoretickou část své práce a vydávat ji za své dílo.

Podle výsledků aktuálního výzkumu **České školy a umělá inteligence** [13] mnoho českých učitelů v posledním roce zaznamenalo, že jejich žáci zneužili AI k podvádění. K nejčastějším formám pak patřilo: vygenerování eseje, referátu či jiného textového úkolu (24,71 %), překlady z/do cizích jazyků (16,37 %), vygenerovaná prezentace (11,08 %), vyřešení matematického příkladu (9,36 %). Učitelé v rámci tohoto výzkumu také souhlasili s tím, že umělá inteligence změní systém školství a učitelé budou muset změnit styl výuky tak, aby se s umělou inteligencí a jejím případným použitím počítalo.

#### **7.4 Tvorba škodlivého obsahu včetně dezinformací**

Veřejně dostupné nástroje generativní umělé inteligence dokáží velmi rychle vytvářet nepravdivý (často dezinformační) obsah, ať již v podobě textu, grafiky (fotografie) či videa. V praxi to znamená, že i laický uživatel dokáže přimět umělou inteligenci k tomu, aby během několika vteřin vytvořila článek (či fotografii), který je možné v podstatě okamžitě rozšířit internetem a vzbudit reakci čtenářů.

Před nedávnem obletěly svět fotografie papeže Františka v bílé péřové bundě a fotografie Donalda Trampa z jeho údajného zatčení policií, v obou případech však šlo o fotografie vygenerované generativní umělou inteligencí.



*Obrázek: Ukázky fotografií Donalda Trumpa vygenerovaných umělou inteligencí  
(Zdroj: CBS News)*



*Obrázek: Ukázky fotografií zesnulého papeže Františka vygenerovaných umělou  
inteligencí (Zdroj: CBS News)*

Kromě textu a fotografií dokáže umělá inteligence také velmi dobře napodobit – **naklonovat – lidský hlas**.<sup>[14]</sup> Několikaminutový záznam lidského hlasu konkrétního člověka stačí pouze nahrát do příslušné aplikace, která hlas podrobně zanalyzuje a naučí se jej také tvořit (syntetizovat). Poté můžete aplikaci napsat, co má daný hlas říkat, a během několika minut dostanete k dispozici výsledný zvukový záznam, který je často k nerozeznání od skutečného hlasu konkrétní osoby. S pomocí AI tedy bude snadné např. padělat nejrůznější projevy politiků či jiných veřejně známých osobností a klást jim do úst věty, které nikdy neřekli.

Umělá inteligence dokáže také produkovat podvodná videa, jež kombinují zvuk s mimikou obličeje konkrétního člověka – tzv. **deep fake videa**.<sup>[15]</sup> Příklady takto vytvořených videí jsme mohli vidět v rámci dezinformačních kampaní týkajících se rusko-ukrajinské války, kdy internetem začalo kolovat video,<sup>[16]</sup> na kterém ukrajinský prezident Zelenskyj vyzýval ukrajinské vojáky, aby se vzdali. Podobná videa se objevila také v případě slovenských parlamentních voleb v roce 2023.<sup>[17]</sup> Ve skutečnosti však šlo o uměle vytvořený záznam a příklad zneužití umělé inteligence pro tvorbu a šíření dezinformace.

## **7.5 Zneužití pro podvodnou činnost**

V březnu 2023 vydal Europol varování před rizikem zneužití ChatGPT a dalších obdobných nástrojů v rámci nejrůznějších druhů podvodů. <sup>[18, 19]</sup> Generativní umělou inteligenci lze totiž velmi jednoduše zneužít k online podvodné činnosti – ať už jde o podvody zaměřené na vylákávání osobních a dalších citlivých údajů (phishing), či podvody zaměřené na získání finančních prostředků (scam). Umělá

inteligence však dokáže naprogramovat také škodlivý kód (tzv. malware), který může napadnout náš počítač.[20]

## **7.6 Závislost na používání technologie**

Je otázkou, co se stane s fungováním lidské společnosti, pokud bude velkou část zajišťovat právě umělá inteligence, která se bude stávat stále autonomnější a která bude postupně stále více rozhodovat za člověka.

Mnoho zajímavých informací k tématu umělé inteligence naleznete na webových stránkách: <https://ai.e-bezpeci.cz>, <https://ai.e-bezpeci.cz/rizika/>.

## 8 Digitální stopa

Se všemi online riziky, o kterých jsme hovořili v předchozích kapitolách, úzce souvisí termín **digitální stopa**. Digitální stopa je souhrn všech informací, které o nás zůstávají v online prostředí v důsledku naší aktivity na internetu. Patří sem nejen příspěvky, fotografie, videa či komentáře, které sami zveřejníme na sociálních sítích, ale také data, která se o nás shromažďují automaticky – například vyhledávací historie, údaje o poloze, informace z mobilních aplikací a malé soubory zvané cookies, které zaznamenávají, jaké weby navštívujeme a co na nich děláme. Digitální stopu vytváříme vědomě i nevědomě a její rozsah se neustále zvětšuje.

Existují dva základní typy digitální stopy:

**1. Aktivní digitální stopa** – vzniká vědomě, když sami zveřejníme příspěvek, fotografii nebo vyplníme formulář.

**2. Pasivní digitální stopa** – vzniká bez našeho aktivního přičinění, například při sledování webů, používání aplikací nebo při ukládání dat poskytovateli internetových služeb.

Digitální stopa je dlouhodobá a obtížně odstranitelná – informace jednou zveřejněné na internetu mohou být kopírovány, archivovány a šířeny i bez našeho vědomí. Proto lze také zjednodušeně říci, že **to, co jednou na internet nahrajeme, už z něj nejde zcela smazat.**

## **Jaká rizika digitální stopa přináší?**

Digitální stopa není jen souhrn neutrálních informací – může se stát zdrojem rizik, která ovlivní soukromí, bezpečnost i budoucnost jedince.

### **1. Ztráta soukromí**

Sdílení příliš osobních údajů může vést k narušení soukromí. Fotografie, adresy, telefonní čísla či informace o zdravotním stavu se mohou dostat k lidem, kterým nebyly určeny.

### **2. Zneužití osobních údajů**

Údaje z digitální stopy mohou být použity k podvodům, krádežím identity nebo jiným nezákonným aktivitám. Útočníci mohou tyto informace využít k manipulaci či vydírání.

### **3. OSINT – otevřené zpravodajství**

Digitální stopa je často využívána v rámci tzv. **OSINT** (Open Source Intelligence). Jedná se o metodu sběru a analýzy informací z volně dostupných zdrojů, kterou používají bezpečnostní složky, novináři, ale i hackeři či podvodníci. Z veřejně dostupných dat lze sestavit překvapivě přesný obraz jednotlivce – zjistit jeho zvyklosti, pohyb, kontakty, pracovní historii, či dokonce finanční situaci. To zvyšuje riziko cílených útoků, sociálního inženýrství nebo vydírání.

#### **4. Kyberšikana a reputační rizika**

Nevhodný obsah, který byl zveřejněn v dětství či dospívání, se může objevit i po letech a být zneužit například ke kyberšikaně. Staré příspěvky mohou ovlivnit vztahy, školní prostředí nebo profesní život.

#### **5. Cílená reklama, profilování a sledování**

Digitální stopa umožňuje detailně mapovat náš pohyb na internetu – co vyhledáváme, které stránky navštívíme, kde se nacházíme. Tyto informace se používají k profilování uživatelů a k personalizaci obsahu, který vidíme.

Na základě našich dat jsou upravovány reklamy, které se nám zobrazují.

Dochází i k personalizaci zpráv a výsledků vyhledávání, což může ovlivnit naše názory a rozhodování.

Tento proces vede k vytváření tzv. informačních bublin, kdy uživatel vidí pouze informace, které odpovídají jeho předchozím preferencím a chování.

#### **6. Dopad na budoucí pracovní (a jiné) příležitosti**

Zaměstnavatelé, školy nebo jiné instituce mohou vyhledávat informace o kandidátech. Nevhodný obsah na sociálních sítích může negativně ovlivnit přijímací řízení či pracovní pohovor.



*Obrázek: Ukázky nevhodných fotografií sdílených na sociálních sítích s možným dopadem na budoucí profesní dráhu*

## 9 Sharenting

Sharenting je fenomén, který velmi úzce souvisí s bezpečností dětí v online prostředí a na němž se aktivně podílejí především rodiče. Jedná se o spojení slov *share* (sdílet) a *parenting* (rodičovství) a označuje situace, kdy **rodiče (ale také prarodiče) sdílejí na internetu fotografie, videa a další osobní informace o svých dětech**. Tento trend je přítomen nejen v České republice, ale i v zahraničí a vyvolává řadu otázek týkajících se ochrany soukromí, práv dítěte, ale také motivace rodičů a potenciálních rizik.

Výzkum realizovaný v roce 2022 Univerzitou Palackého v Olomouci ve spolupráci se společností Microsoft[21] ukázal, že sharenting je v českém prostředí velmi rozšířený. Do výzkumného šetření se zapojilo 2 481 rodičů a výsledky jsou alarmující: 69 % z nich přiznalo, že sdílí citlivé údaje o svých dětech. Z tohoto počtu dokonce **6,7 % rodičů zveřejňuje vysoce rizikové fotografie**, na kterých je tvář dítěte jasně identifikovatelná. Tyto údaje potvrzují, že velká část rodičů sdílí obsah, aniž by si uvědomovala možné důsledky.

Podobné výsledky přinášejí i zahraniční studie.[22] V USA sdílí obsah o svých dětech až 75 % rodičů, v Austrálii se tento podíl blíží 90 %. V evropském kontextu se hodnoty pohybují mezi 70 a 80 %. Italští výzkumníci upozorňují na to, že většina rodičů si není vědoma rizik spojených s nadměrným sdílením a podceňuje právní aspekty. Studie z Říma dokonce ukazuje, že 31 % rodičů začne sharenting praktikovat už během prvních šesti měsíců po narození dítěte.

K **nejrizikovějším typům fotografií patří ty, na nichž je dítě částečně, či dokonce zcela obnaženo** (např. ve věku novorozence či batolete – třeba při koupání, pasení koníčeků atd.). Tyto fotografie velmi často unikají mimo kontrolu rodičů, kteří je na sociální sítě nasdíleli. Rizikové jsou však ale také snímky, které nemusejí být vyloženě sexuálně explicitní, ale zachycují dítě v nějaké nepříjemné či dehonestující situaci – třeba při „vykonávání potřeby“ (dítě sedí na nočníku), pláče, krmení (dítě je upatlané od jídla) či při nemoci (zarděnky, neštovice). Rodiče tyto materiály považují za roztomilé, nicméně dětem mohou v pozdějším věku způsobit problémy. Poradna E-Bezpečí eviduje hned několik případů, kdy dítě dostalo na základní škole přezdívku „*pokakánek*“ právě podle fotografie, kterou spolužáci objevili na profilu jeho rodiče.



*Obrázek: Příklady závadových fotografií sdílených v rámci sharentingu  
(Zdroj: E-Bezpečí)*

## Doporučení pro rodiče

Při sdílení jakékoli informace o svém dítěti – ať už jde o fotografie, videa, nebo třeba informace o jeho zdravotním stavu – je **nutné promyslet, zda tyto materiály nemohou být zneužity**, a to nejenom dnes, ale také v budoucnu. Zároveň je nutné si uvědomit, že při sdílení materiálu třeba prostřednictvím sociálních sítí velmi rychle ztrácíme nad jeho šířením kontrolu, protože jej může stáhnout kdokoli, kdo má k našemu profilu přístup.

Na prvním místě je tedy nutné **zvážit, zda to, co o svém dítěti sdílíme**, jej (ne)může v budoucnu nějak negativně ovlivnit (např. aby nestalo terčem posměchu, či dokonce šikany/kyberšikany od svých spolužáků, kteří jeho foto odhalí a rozšíří). Samozřejmostí by mělo být také získání souhlasu dítěte – i malé dítě by mělo souhlasit s tím, že jeho fotografii či video ukážeme jiným lidem.

Pokud sdílíme hromadná foto, třeba z oslav narozenin, kde je více dětí, **zkontrolujme, zda s tímto sdílením souhlasí i rodiče ostatních dětí, jež jsou na fotografii zachyceny**. Ne každý chce sdílet foto svých dětí na internetu.

**Nesdílejme žádné příliš osobní fotografie** – odolejme nutkání nahrát na internet **např. dítě na nočníku, upatlané od jídla, počurané či pokakané** apod. To, co může připadat roztomilé nám, nemusí připadat roztomilé ostatním a dítěti to může způsobit v budoucnu řadu problémů.

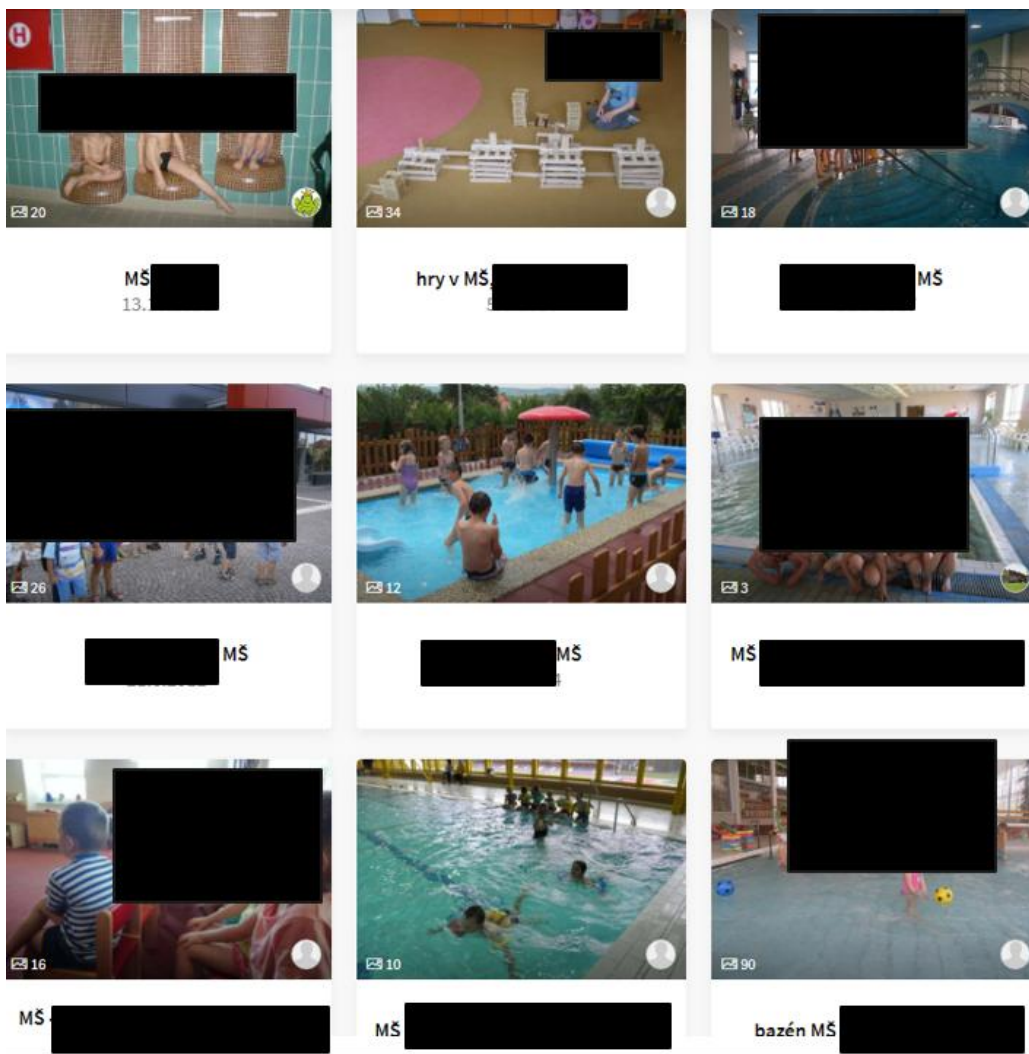
Upozorněme na tyto problémy i prarodiče, protože i oni aktivně sdílejí a šíří fotografie či videa svých vnoučků.

V této souvislosti stojí za zmínku preventivní projekt „**Nebudujte svému dítěti digitální stopu**“ (**Nebudujte svému dítěti digitální stopu**), který se zaměřuje na osvětu rodičů v oblasti bezpečného sdílení informací o dětech. Projekt upozorňuje na to, že veškerý obsah zveřejněný online vytváří dítěti dlouhodobou digitální stopu, jež může ovlivnit jeho pověst, budoucí vztahy i profesní život. Cílem projektu je pomoci rodičům lépe porozumět rizikům spojeným se sdílením fotografií a osobních údajů, nabídnout praktické rady, jak sdílet bezpečně nebo kdy raději nesdílet vůbec, a zároveň podpořit respektující přístup k právu dítěte na soukromí už od nejtělejšího věku.

Sharenting je spojován zejména s nevhodným sdílením citlivých údajů dětí jejich rodiči. Problematické je samozřejmě i **sdílení citlivých údajů dětí institucemi, které je mají v „dočasné“ péči a přebírají za ně zodpovědnost.**

Instituce, které mají děti v dočasné péči, mohou ohrozit jejich soukromí různými způsoby. Často se to děje na **webových stránkách či sociálních sítích škol, a to včetně škol mateřských, na stránkách a sociálních sítích dětských domovů a neziskových organizací, kde jsou zveřejňovány fotografie z výletů, školních akcí, z bazénů, táborů nebo vánočních besídek, někdy dokonce s uvedením jmen dětí.** Velmi problematické je také využívání osobních příběhů dětí v charitativních a fundraisingových kampaních – například popisy důvodů, proč byly odebrány z rodiny, nebo sdílení detailů o jejich zdravotním stavu, aby se získala podpora veřejnosti. Rizikové je rovněž zveřejňování fotografií v obecních či školních zpravodajích, kde nebývá zajištěna anonymita dětí. V médiích se pak objevují reportáže či rozhovory z prostředí dětských domovů,

kde jsou děti ukazovány i s jejich osobními příběhy, což může vést k jejich stigmatizaci. A v neposlední řadě hrozí i neúmyslné zveřejnění interních dokumentů, například seznamů, hodnocení nebo zpráv o chování a zdravotním stavu. Všechny tyto způsoby sdílení představují vážné riziko, protože děti samy si nemohou rozhodnout, co chtějí zveřejnit, a instituce, které za ně dočasně nesou zodpovědnost, mají povinnost jejich identitu a soukromí chránit.



Obrázek: Příklady sdílení citlivých údajů dětí mateřskými školami ve veřejně dostupné online fotogalerii (Zdroj: E-Bezpečí)



## 10 Zásady efektivní prevence

Aby byla prevence rizikového chování na internetu co nejefektivnější, je nutné dodržovat několik zásad:

- A. **Smyslem efektivní prevence je zajistit, aby k rizikovému chování nedocházelo, případně aby byl jeho dopad minimalizován.** Proto je nutné **realizovat preventivní aktivity co nejdříve** – tj. v nízkém věku dítěte. Prevence však musí být vždy **úměrná věku dětí** (či jiným cílovým skupinám), tomu musí odpovídat forma a volba témat. U menších dětí (1. stupeň ZŠ či MŠ) je vhodné zaměřit se na obecnější témata, která jsou spojena se základními bezpečnostními návyky (hesla, dvojfázové zabezpečení, ochrana osobních údajů, na co si dávat pozor při komunikaci s jinými lidmi na internetu apod.), u větších dětí by měla být specifitější – orientovaná na zcela konkrétní problémy (kyberšikana, sexting, kybergrooming, rizika spojená se sociálními sítěmi apod.).
- B. Efektivní prevence by měla být **dlouhodobá** a **kontinuální**, krátkodobé aktivity bývají méně efektivní než dlouhodobé programy.
- C. Efektivní prevence se orientuje na **rozvoj znalostí, dovedností a postojů** cílové skupiny. Preventivní programy by měly usilovat o co **největší zapojení cílové skupiny** – vhodné jsou diskuse, kladení otázek, sdílení vlastních zkušeností, návrhy řešení konkrétních rizikových situací apod. Velmi důležité je také zaměřit se na aktivní ovlivňování postojů žáků

(případně změny chování) a uvědomit si, že řešit agresivní útok agresivní reakcí není efektivní cesta řešení problému.

- D. Efektivní prevence využívá principů tzv. **učení založeného na problémech / problémových situacích** (Problem-Based Learning, PBL). Tato metoda umožňuje žákům rozvíjet klíčové dovednosti, jako jsou kritické myšlení, řešení problémů a schopnost spolupráce, tím, že je vystaví reálným nebo hypotetickým problémům a vyzývá je k jejich řešení. V praxi to znamená co nejvíce pracovat aktivně s kazuistikami.
- E. V rámci preventivních aktivit **žáky nikdy nestrašíme** – strašení je málo efektivní a často i kontraproduktivní. V rámci vzdělávacích aktivit žákům předkládáme co nejvíce **objektivních informací** a orientujeme se na **posilování pozitivních vzorců chování**. Celkové vyznění preventivní akce by mělo být vždy nastaveno pozitivně. Preventivní akce by měli realizovat vyškolení **odborníci**, kteří mají hlubokou znalost jednotlivých témat a jsou vybaveni pedagogickými/didaktickými kompetencemi.
- F. Prevence by měla probíhat v **bezpečném prostředí**. Osoby, které jsou do prevence zapojeny, by měly cítit, že mohou vyjadřovat své názory a pocity bez strachu z odmítnutí, dehonestace či trestu. Prevence by neměla probíhat tam, kde dosud nejsou dořešeny („zaléčeny“) existující rizikové formy chování. Prevence funguje jiným způsobem než intervence.

- G. Pokud k prevenci využijeme audiovizuální materiály (filmy, seriály apod.), je velmi důležité doprovodit je komentářem, rozbořem, následnou diskusí.  
**Audiovizuální materiály určené pro prevenci by měly být doplněny metodikou.**

## 11 Důležité odkazy a další materiály

### Portály orientované na online bezpečnost

E-Bezpečí ([www.e-bezpeci.cz](http://www.e-bezpeci.cz))

Kybergrooming ([www.kybergrooming.cz](http://www.kybergrooming.cz))

Sexting ([www.sexting.cz](http://www.sexting.cz))

Safer Internet Centrum ČR ([www.bezpecnyinternet.cz/cs/](http://www.bezpecnyinternet.cz/cs/))

NÚKIB ([www.nukib.gov.cz](http://www.nukib.gov.cz))

Internetem bezpečně ([www.internetembezpecne.cz](http://www.internetembezpecne.cz))

Bezpečně v síti ([www.bezpecnevsiti.cz](http://www.bezpecnevsiti.cz))

Policie ([www.policie.gov.cz](http://www.policie.gov.cz))

Prokoukni to! ([www.panprokoukl.cz](http://www.panprokoukl.cz))

### Metodické příručky s aktivitami pro žáky

[Bezpečné chování na internetu pro kluky a pro holky](#)

### Metodická doporučení a metodické pokyny MŠMT

[Stránka MŠMT](#) obsahuje metodická doporučení a metodické pokyny v oblasti primární prevence rizikového chování, včetně prevence rizikového chování vybraných online rizik jako např. metodická doporučení **Kyberšikana a další formy kybernetické agrese, Rizikové sexuální chování** apod.

### **Edukační hra: *Samova dobrodružství: Trable ve škole***

Hra zábavnou a srozumitelnou formou učí děti základům online bezpečnosti. Zaměřuje se na témata, jako jsou **bezpečné heslo, biometrické zabezpečení, dvoufázové ověření (2FA), antivirová ochrana, malware, phishing, digitální stopa, rizika sdílení nebo vliv sociálních sítí**. Hráči postupně odemykají nové úrovně, řeší interaktivní úkoly a učí se správně reagovat v digitálním světě.

Odkaz na hru naleznete [ZDE](#).

### **Preventivní materiál: *Umělá inteligence: Rizika a odpovědnost***

Publikace je metodickým průvodcem světa umělé inteligence, který se věnuje jejímu praktickému využití, ale také etickým a právním aspektům. Zvláštní pozornost věnuje generativní umělé inteligenci, která umožňuje vytvářet texty, obrázky, hudbu nebo videa, ale zároveň může být zneužita k šíření dezinformací, manipulaci či podvodům. Zkoumá, jaké dopady může mít AI na autorská práva, soukromí a bezpečnost, a upozorňuje na rizika spojená s jejím nekontrolovaným využíváním.

Odkaz na preventivní materiál naleznete [ZDE](#).

### **Preventivní projekt: *Nebudujte svému dítěti digitální stopu***

Projekt si klade za úkol zvýšit povědomí rodičů, především budoucích maminek, které často jako první sdílejí o dítěti různé osobní informace na internetu. Patří mezi ně například snímky z koupání, z domácího prostředí, z dovolených či fotografie zachycující běžné momenty každodenního života. Takový obsah však

pomůže dítě snadno identifikovat a v některých případech i umožnit jeho sledování. Je proto důležité, aby rodiče pečlivě zvažovali, co a kde zveřejňují, a díky tomu co nejvíce omezili rizika spojená s digitální stopou svých dětí. Současně by měli brát v úvahu i to, že děti mají právo vytvářet si svou vlastní digitální identitu až ve chvíli, kdy jsou na to připraveny. Čím méně informací o dítěti rodiče předčasně zveřejní, tím mu do budoucna ponechají větší prostor, aby o svém soukromí rozhodovalo samo.

Odkaz na preventivní materiál naleznete [ZDE](#).

### **Další informace**

Prevence kriminality ([www.prevencekriminality.cz](http://www.prevencekriminality.cz))

## 12 Reference

- [1] MINISTERSTVO ŠKOLSTVÍ, mládeže a tělovýchovy. *Co dělat, když - intervence pedagoga. Příloha č. 7 - Kyberšikana*. 2009.
- [2] KOPECKÝ, Kamil. Měly by školy řešit kyberšikanu, ke které dochází i mimo výuku? Existuje řada situací, kdy ano. *E-Bezpečí* [online]. 2022, **7**(1), 20–22 [vid. 2023-10-21]. ISSN 2571-1679. Dostupné z: <https://e-bezpeci.cz/journal/articles/2615.html>
- [3] *Listina základních práv a svobod* [online]. [vid. 2023-10-21]. Dostupné z: <https://www.psp.cz/docs/laws/listina.html>
- [4] *Kam až sahá svoboda slova? ‚Hrana je zákon a jeho výklad,‘ vysvětluje odborník Bartoň | iROZHLAS - spolehlivé zprávy* [online]. [vid. 2023-10-21]. Dostupné z: [https://www.irozhlas.cz/zpravy-domov/svoboda-slova-hranice-projev-socialni-site-realita\\_2204190700\\_pik](https://www.irozhlas.cz/zpravy-domov/svoboda-slova-hranice-projev-socialni-site-realita_2204190700_pik)
- [5] SZOTKOWSKI, René, Kamil KOPECKÝ a Pavla DOBEŠOVÁ. *Sexting u českých dětí* [online]. B.m.: Univerzita Palackého v Olomouci, 2020 [vid. 2021-10-12]. Dostupné z: doi:10.5507/pdf.20.24457932
- [6] KOPECKÝ, Kamil. Stručný úvod do problematiky online vydírání českých dětí se zaměřením na tzv. sextortion. *Pediatric pro praxi*. 2014, **15**(6), 352–354. ISSN 1803-5264.
- [7] KOPECKÝ, Kamil a Martin KOŽÍŠEK. *Podvodys webkamerami - webcam trolling* [online]. 2013 [vid. 2015-04-10]. Dostupné

z: <http://www.slideshare.net/kopecky/podvody-s-webkamerami-webcam-trolling>

- [8] KOPECKÝ, K. Misuse of web cameras to manipulate children within the so-called webcam trolling. *Telematics and Informatics* [online]. 2015, **33**(1). ISSN 07365853. Dostupné z: doi:10.1016/j.tele.2015.06.005
- [9] KOPECKÝ, Kamil a René SZOTKOWSKI. *Sexting a rizikové seznamování českých dětí v kyberprostoru*. 2017.
- [10] KOPECKÝ, Kamil, Pavla STRÍLKOVÁ, René SZOTKOWSKI a José-María ROMERO-RODRÍGUEZ. Rizikové výzvy v on-line prostředí. *Pediatric pro praxi* [online]. 2020, **21**(2), 85–89 [vid. 2021-10-04]. ISSN 12130494. Dostupné z: doi:10.36290/PED.2020.016
- [11] KOPECKÝ, Kamil. Co jsou tzv. nebezpečné výzvy (challenges)? *E-Bezpečí* [online]. 2022 [vid. 2023-05-25]. Dostupné z: <https://www.e-bezpeci.cz/index.php/kontakt/71-trivium/1433-co-jsou-nebezpecne-vyzvy>
- [12] KOPECKÝ, Kamil, René SZOTKOWSKI a Lukáš KUBALA. *Bezpečné chování na internetu pro kluky a pro holky (náměty na výukové aktivity)* [online]. Olomouc: Univerzita Palackého v Olomouci, 2022 [vid. 2023-07-28]. ISBN 978-80-244-6197-7. Dostupné z: <https://e-bezpeci.cz/index.php/ke-stazeni/tiskoviny/159-bezpecne-chovani-na-internetu-pro-kluky-a-pro-holky-2022/file>

- [13] KOPECKÝ, Kamil, René SZOTKOWSKI, Dominik VORÁČ, Veronika KREJČÍ a Pavla DOBEŠOVÁ. *České školy a umělá inteligence* [online]. 2023 [vid. 2023-09-25]. Dostupné z: <https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/163-ceske-skoly-a-umela-inteligence-2023/file>
- [14] KOPECKÝ, Kamil. Klonování lidského hlasu s pomocí AI otevírá prostor pro nové druhy dezinformací. Naklonovat hlas kohokoli se stalo extrémně snadné. *E-Bezpečí* [online]. 2023 [vid. 2023-09-25]. Dostupné z: <https://e-bezpeci.cz/index.php/clanky-komentare/3555-klonovani-lidskeho-hlasu-s-pomoci-ai-otevira-prostor-pro-nove-druhy-dezinformaci-naklonovat-hlas-kohokoli-se-stalo-extremne-snadne>
- [15] KOPECKÝ, Kamil. Deep fake – stručný úvod do problematiky. *E-Bezpečí* [online]. 2019 [vid. 2023-09-25]. Dostupné z: <https://www.e-bezpeci.cz/index.php/70-projekt-fake-news/1417-deep-fake-strucny-uvod-do-problematiky>
- [16] FIŠER, Miloslav. „Ukrajinci, vzdejte se!“ říká Zelenskyj na deepfake videu. *Novinky.cz* [online]. 2022 [vid. 2023-09-25]. Dostupné z: [https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-ukrajinci-vzdejte-se-hackeri-siri-na-webech-deepfake-video-se-zelenskym-40390683#dop\\_ab\\_variant=0&dop\\_source\\_zone\\_name=novinky.szhn.p.box&source=hp&seq\\_no=6&utm\\_campaign=abtest183\\_vzhled\\_vy](https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-ukrajinci-vzdejte-se-hackeri-siri-na-webech-deepfake-video-se-zelenskym-40390683#dop_ab_variant=0&dop_source_zone_name=novinky.szhn.p.box&source=hp&seq_no=6&utm_campaign=abtest183_vzhled_vy)

h\_pole\_na\_tel\_varBB&utm\_medium=zboxiku&utm\_source=www.seznam.cz

- [17] PALATA, Luboš. Den před volbami: Na Slováky útočí falešná videa, varuje před nimi i policie. *Deník.cz* [online]. 2023 [vid. 2023-10-06]. Dostupné z: <https://www.denik.cz/staty-eu/volby-na-slovensku-falesna-video-umela-intelligence.html>
- [18] EUROPOL. *ChatGPT - The impact of Large Language Models on Law Enforcement, a Tech Watch Flash Report from the Europol Innovation Lab* [online]. 2023. Dostupné z: <https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf>
- [19] EUROPOL. The criminal use of ChatGPT – a cautionary tale about large language models. *Europol* [online]. 2023 [vid. 2023-09-25]. Dostupné z: <https://www.europol.europa.eu/media-press/newsroom/news/criminal-use-of-chatgpt-cautionary-tale-about-large-language-models>
- [20] KOPECKÝ, Kamil. ChatGPT umožňuje běžným uživatelům vytvářet nejrůznější druhy škodlivých kódů, lze očekávat nárůst internetových podvodů všeho druhu. *E-Bezpečí* [online]. 2023, **8**(1), 34–39 [vid. 2023-

10-06]. ISSN 2571-1679. Dostupné z: <https://e-bezpeci.cz/journal/articles/3193.html>

- [21] KOPECKÝ, K, R SZOTKOWSKI, H MIČKOVÁ a A NOVÁKOVÁ. *Sharenting u českých rodičů (výzkumná zpráva)* [online]. 2022 [vid. 2022-07-01]. Dostupné z: <https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/158-sharenting-u-ceskych-rodicu-2022/file>
- [22] KOPECKÝ, Kamil, René SZOTKOWSKI, Helena MIČKOVÁ a Veronika KREJČÍ. Sharenting u českých rodičů a jeho rizika. *Pediatric pro Praxi* [online]. 2023, **24**(1), 8–12. ISSN 18035264. Dostupné z: [doi:10.36290/ped.2023.011](https://doi.org/10.36290/ped.2023.011)



Pedagogická  
fakulta

Univerzita Palackého  
v Olomouci



PREVENCE  
SE MUSÍ VYPŁATIT



MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY

[www.e-bezpeci.cz](http://www.e-bezpeci.cz)