Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

MPSV

Zajištění dostupného poradenství v otázkách bezpečnosti a příležitostí včetně internetového poradenství

Výstup KA 01 č. 7 a opatření SDG 2020 č. 4.3

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Zajištění dostupného poradenství v otázkách bezpečnosti a příležitostí včetně internetového poradenství

Výstup KA 01 č. 7 a opatření SDG 2020 č. 4.3

Název projektu:	Rozvoj systémové podpory digitální gramotnosti
Registrační číslo projektu:	CZ.03.1.54/0.0/0.0/16_020/0005634
Publikováno:	listopad 2020
Zpracovali:	Mgr. Tatiana Feketeová, Bc. Binh Le Thanh
Grafická úprava:	Anna Lhoťanová

Výstup KA 01 č. 7, Plnění opatření Strategie digitální gramotnosti ČR na období 2015 – 2020 č. 4.3: Zajištění dostupného poradenství v otázkách bezpečnosti a příležitostí včetně internetového poradenství.

Obsah

1. Úvod

Společnost, v níž budou příští generace žít, se zejména vlivem digitálních technologií zásadně změní a s touto proměnou musí dojít i ke změně prostředí, ve kterém se budou následující generace vzdělávat. Člověk vybavený pouze „klasickým vzděláním“, i kdyby bylo sebedokonalejší, nebude mít šanci se v digitálním světě plnohodnotně uplatnit.

Podíváme-li se na dnešní žáky, pak prakticky všichni využívají digitální technologie zcela běžně a vnímají je jako přirozenou součást svého života. Mimo školní výuku bývají v kontaktu prostřednictvím digitálních technologií spolu navzájem i s ostatním světem a také mají takřka nekonečný přísun informací. V tomto světě se orientují intuitivně, s pomocí přátel, občas rodiny, zřídka školy. Proto je nutné usilovat o propojení či synergii světa školního vzdělávání a vnějšího prostředí, o propojení učební zkušenosti žáků ve škole i mimo ni.

Využívání digitálních technologií má i významný sociální aspekt a zásadní vliv na rozvoj informační společnosti. Schopnost rozlišit přínosy a rizika využívání digitálních technologií jak v osobní, tak ve společenské rovině je jedním ze základních předpokladů pro život v informační společnosti. Nastavují se nové procesy a dříve či později je nutné nastavit nová pravidla, jež s využíváním digitálních technologií bezprostředně souvisejí např. etická pravidla a legislativa, autorská práva, obchod s osobními daty, prevence kyberkriminality, on-line bezpečí, kybernetické bezpečí atd.

Důvodem vzniku tohoto dokumentu je ukázat možná rizika spojená s používáním internetu, uvědomit si nedostatky virtuální komunikace a umět se bránit případnému virtuálnímu (reálnému) nátlaku. Mezi hlavní cílové skupiny patří nejenom děti a mládež, ale i jejich rodiče a prarodiče a také škola, tj. pedagogičtí pracovníci škol a školských zařízení, včetně volnočasových školských zařízení a institucí.

Cílem dokumentu je na základě provedené analýzy efektivních metod dostupného poradenství představit příklady a doporučení podporující rozvoj jednorázového i dlouhodobého poradenství pro otázky bezpečnosti a rizik spojených s používáním digitálních technologií a online příležitostí. Dále pak představit příklady a doporučení podpory příležitostí v otázkách bezpečnosti a rizik spojených s používáním digitálních technologií a online příležitostí včetně vytvoření konkrétní vzdělávací podpory pro cílovou skupinu rodiče, prarodiče a děti.

Dokument byl zpracován na základě analýzy existujících forem a způsobů efektivních metod dostupného poradenství pro otázky bezpečnosti a na základě dotazníkového šetření ohledně bezpečnosti na internetu, které analýzu podložilo. Cílovou skupinou průzkumu byly pedagogičtí pracovníci ve školách a školských zařízeních, včetně volnočasových školských zařízení (Středisko volného času, Dům dětí a mládeže, Školní družina nebo Školní klub).

Dokument bude obsahovat úvod, kontextualizaci a zacílení, metodologii identifikace dostupného poradenství v otázkách bezpečnosti a online příležitostí včetně internetového poradenství, kritéria identifikace, samotnou analýzu, návrhy řešení problematiky efektivních metod podporující rozvoj jednorázového i dlouhodobého poradenství pro otázky bezpečnosti a podpory příležitostí v otázkách bezpečnosti a rizik spojených s používáním digitálních technologií a online příležitostí a na závěr jednotlivé přílohy:

- Soubor nejčastěji kladených otázek a odpovědí souvisejících s bezpečností a riziky používání digitálních technologií a využíváním online příležitostí
- Metodika pro pracovníky organizací (školská zařízení, volnočasové instituce, knihovny, galerie, muzea aj.) poskytující poradenství rodičům, prarodičům a dětem v otázkách bezpečnosti a rizik spojených s používáním digitálních technologií a online příležitostí

- Mezigenerační vzdělávací program pro oblast bezpečnosti a rizik spojených s používáním digitálních technologií a online příležitostí, určený pro prezenční použití ve školách, volnočasových institucích apod.
- Metodika pro lektory mezigeneračního vzdělávacího programu pro oblast bezpečnosti a rizik spojených s používáním digitálních technologií a online příležitostí, určená pro prezenční použití ve školách, volnočasových institucích apod.

2. Kontextualizace a zacílení

Strategie digitálního vzdělávání v souladu s prioritami Strategie vzdělávací politiky České republiky do roku 2020 se zaměřuje na vytvoření vhodných podmínek a nastavení procesů, které povedou k cílům, metodám a formám vzdělávání odpovídajícím současnému stavu poznání, požadavkům společenského života i trhu práce, ovlivněným rozvojem digitálních technologií a informační společnosti vůbec. Posláním Strategie digitálního vzdělávání je iniciace změn jak v oblasti metod a forem vzdělávání, tak v oblasti cílů vzdělávání.

Strategie digitálního vzdělávání formuluje tři prioritní cíle, ke kterým budou směřovat první intervence:

- otevřít vzdělávání novým metodám a způsobům učení prostřednictvím digitálních technologií
- zlepšit kompetence žáků v oblasti práce s informacemi a digitálními technologiemi
- rozvíjet informatické myšlení žáků

Strategie seskupuje opatření do sedmi hlavních směrů intervence, které směřují k naplnění hlavní vize strategie.

Zásadním pro náš dokument je nediskriminační přístup k digitálním vzdělávacím zdrojům – frekventovanou připomínkou ke zdrojům na internetu je velké množství těchto zdrojů, jejich různorodá kvalita a z principu internetu i jejich neuspořádanost. Na internetu existuje množství vysoce kvalitních vzdělávacích zdrojů, ale problémem je příslušnou informaci o jejich existenci doručit k cílové skupině uživatelů, kterým by mohla být užitečná. V této oblasti již MŠMT v minulosti investovalo do vývoje Metodického portálu RVP.CZ, který do jisté míry již na bázi reputačního systému pracuje, dále nedávno zpřístupnilo Databázi výstupů projektů OP VK.

Cílem prosazení otevřených vzdělávacích zdrojů je zajistit uveřejnění digitálních obsahů nejrůznějšího charakteru, které byly podpořeny z veřejných prostředků, pod otevřenou licencí Creative Commons (příp. jinou), a tím k nim zjednodušit přístup a umožnit jejich sdílení všem aktérům ve vzdělávání.

Vytvoření recenzního systému pro hodnocení a doporučování kvality otevřených vzdělávacích zdrojů – cílem je vytvořit navštěvovaný systém tematicky anotovaných odkazů na otevřené digitální zdroje, který je členěn dle různých kategorií. Obsah i hodnocení daných zdrojů je tvořeno uživateli. Vytvořit funkční databázi (akreditovaných) vzdělávacích nabídek, ve kterém mohou zájemci o DVPP v přátelském uživatelském on-line rozhraní vyhledávat plánované termíny uskutečnění vzdělávacích programů dle různých kritérií a seznámit se s hodnocením dříve uskutečněných vzdělávacích programů.

Legislativní rámec (úroveň státu)

- I na úrovni státu se prevence rizikového chování – v našem případě kyberšikany či šikany – řídí v obecné rovině řadou strategických dokumentů, ze kterých pak vycházejí dokumenty dílčí. Mezi strategické dokumenty, které jsou s prevencí kyberšikany spojeny, patří zejména:
- Zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), ve znění pozdějších předpisů,
- Zákon č. 563/2004 Sb., o pedagogických pracovnících a o změně některých zákonů, ve znění pozdějších předpisů,
- Metodické doporučení k primární prevenci rizikového chování u dětí a mládeže č. j.: 21291/2010-28,
- Metodický pokyn ministryně školství, mládeže a tělovýchovy k prevenci a řešení šikany ve školách a školských zařízeních čj. MSMT-21149/2016,
- Strategie prevence kriminality 2016–2020 (definovaná ve víceletých cyklech Usnesením vlády ČR),
- Národní strategie primární prevence rizikového chování dětí a mládeže na období 2013–2018 (Ministerstvo školství ČR, 2013).

Legislativní rámec (úroveň školy):

Školy jsou povinny zajistit bezpečnost a ochranu zdraví svých žáků a zároveň vytvářet podmínky pro předcházení vzniku sociálně patologických jevů. Tato povinnost je dána školským zákonem (Zákon 561/2004 Sb., 2012), konkrétně § 29, který se zaměřuje na bezpečnost a ochranu a zdraví ve školách. Školami se rozumí školy a školská zařízení. Strategické dokumenty školy vztahující se k prevenci rizikového chování:

- Vnitřní řád školského zařízení, školní řád
- Školní preventivní strategie
- Preventivní program školy (dříve Minimální preventivní program)
- Krizové plány

Mezi dalšími dokumenty, které se dotýkají primární prevence na základní škole, patří:

- Program poradenských služeb ve škole – zahrnuje popis činností, rozdělení rolí a vymezení odpovědnosti školních poradenských pracovníků, vytvoření časového prostoru na poskytované služby, způsoby komunikace a spolupráce v rámci poradenského pracoviště se specializovanými poradenskými pracovišti ve školství (pedagogicko-psychologická poradna, speciálně-pedagogické centrum, středisko výchovné péče) a s relevantními organizacemi mimo školství.
- Plán dalšího vzdělávání pedagogů – zahrnuje školení pedagogů, především pracovníky pověřené řešením šikany (zejm. v prevenci šikanování, v oblasti komunikace, řešení konfliktů, účinné preventivní strategie v praxi školy, interakce mezi učitelem a žákem).

Preventivní a poradenské služby ve školách poskytují zaměstnanci školních poradenských pracovišť, která jsou definována vyhláškou Vyhláška č. 72/2005 Sb., o poskytování poradenských služeb ve školách a školských poradenských zařízeních, ve znění pozdějších předpisů. Poradenské služby ve škole jsou obvykle zajišťovány výchovným poradcem, školním metodikem prevence, případně školním psychologem/školním speciálním pedagogem a jejich konzultačním týmem složeným z vybraných pedagogů (Ciklová, 2014). Cílem školních poradenských pracovišť je především poradenská podpora žáků, rodičů i pedagogů.

3. Metodologie identifikace a analýza dostupného poradenství v otázkách bezpečnosti a online příležitostí včetně internetového poradenství

Online poradny

Server E-bezpečí

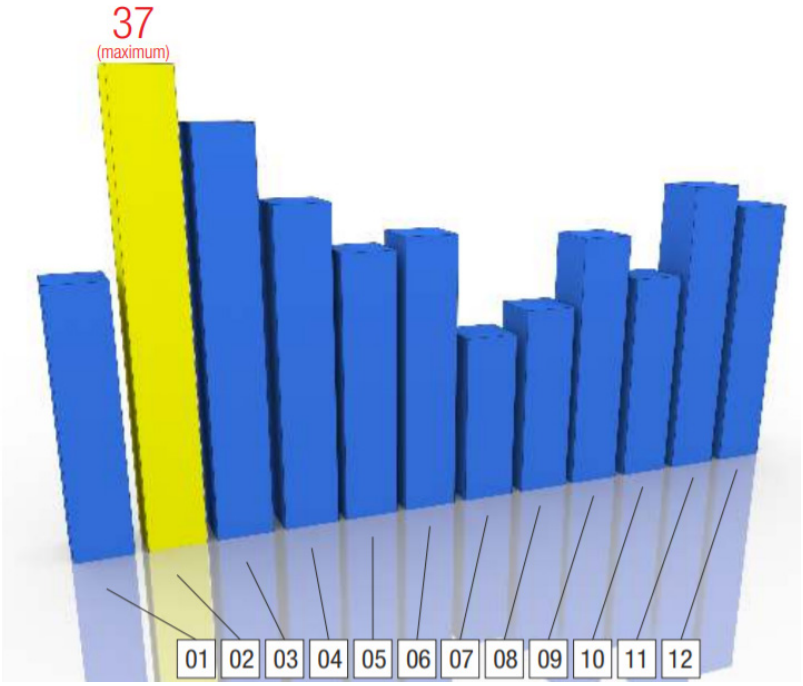
Důležitým prvkem fungování projektu E-Bezpečí je online poradna, která zahájila provoz v roce 2010. Poskytuje anonymní poradenství všem, kteří se nacházejí či se dostali do obtížných situací spojených se zneužíváním na internetu.

Poradna je provozována ve spolupráci s Policií České republiky, statutárním městem Olomouc, statutárním městem Ostrava a Pedagogickou fakultou Univerzity Palackého v Olomouci. Projekt také spolupracuje s Linkou bezpečí, bezpečnostními experty firem Seznam.cz, Google, Vodafone a dalšími poradenskými linkami a krizovými centry.

Online poradna v roce 2015 řešila 292 případů, k tomu 43 případů bylo předáno Policii České republiky. Dále se podílela na 31 blokacích závadného obsahu na internetu. Veškeré dotazy směřovaly skrz web www.napisnam.cz. V roce 2015 se nejčastěji řešilo podle cíle frekvence: pronásledování (stalking), únik intimních materiálů do prostředí internetu (sexting), útok na e-mailový či jiný účet, krádež hesla, kyberšikana a další formy agresivního chování, závadný obsah na sociálních sítích, vydírání a vyhrožování v prostředí internetu.

Dle výzkumné zprávy z roku 2015, poradna od vzniku působení v roce 2010 do roku 2015 řešila více než 1 500 případů spojených se zneužitím internetu a mobilních telefonů.

Počty případů řešených v roce 2015

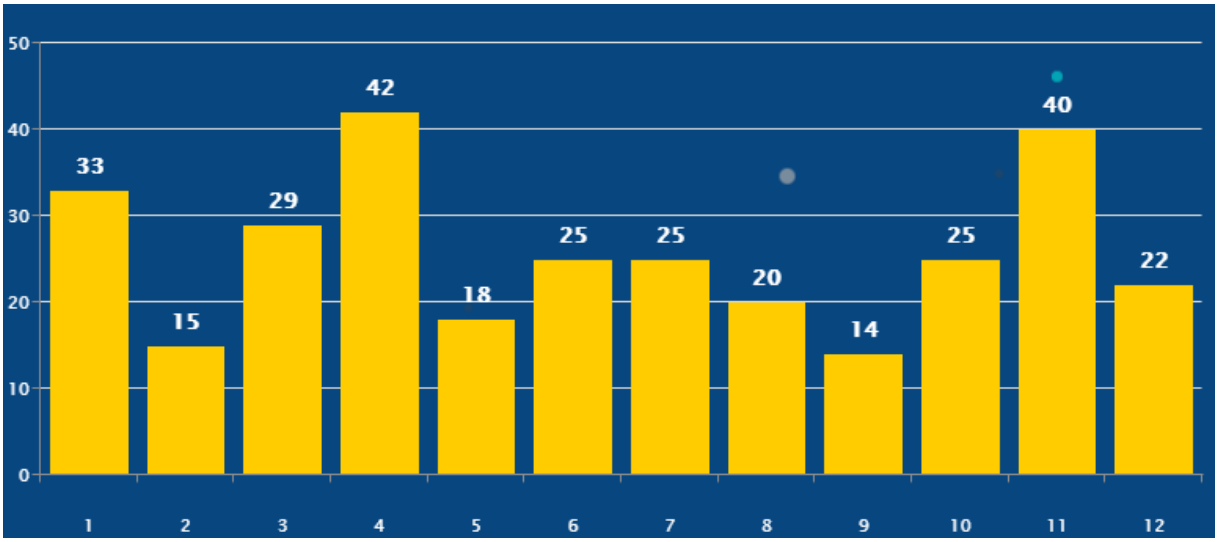


V roce 2017 zachytila již přes **300 případů spojených se zneužitím internetu, tj. internetové služby či mobilního telefonu**. Také výrazně vzrostlo množství případů úniku citlivého materiálu na internet spojených s následným vydíráním a vyhrožováním.

Počátek roku se nesl ve znamení případů **kyberšikany, stalkingu** (nezvládnutých rozchodů) či **zneužití citlivého materiálu (posílaní fotek, sexting apod.).** Stále více dětí hledalo pomoc v situaci, kdy poskytlo svůj intimní materiál osobě, které důvěřovalo. Často se tyto materiály objevily na internetu a staly se nástrojem pro vydírání. Klienti požadovali především **technickou podporu při odstranění poslaného materiál nebo diagnostiku příčin.** Rovněž žádali **o psychologickou podporu** – nejčastější otázky: co mám dělat, jak to říci rodičům, jak komunikovat s agresorem atd.

Nejvíce případů zaregistrovala poradna v dubnu roku 2017, kdy tým E-bezpečí řešil **44 případů** – většina z nich se týkala výzvy tzv. Modré velryby.

Tabulka případů v jednotlivých měsících v roce 2017

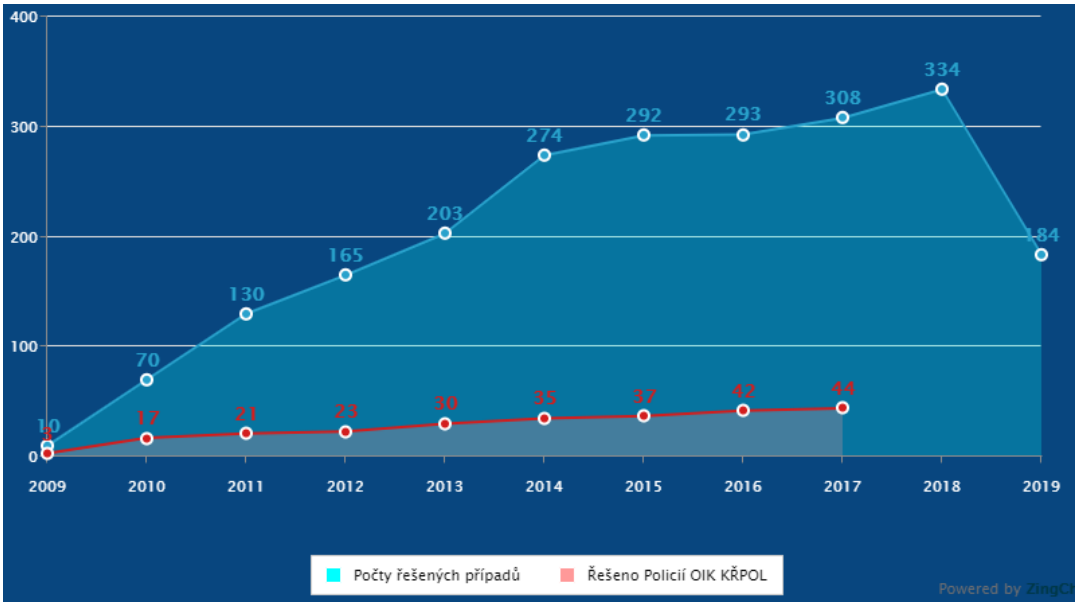


Postupem času se na poradnu začali obracet i učitelé. Oznamovali, že si jejich žáci kreslí na ruce obraz Modré velryby a nevěděli si rady. Děti také často sdílejí ve třídách informace, které slýchávají v televizích, internetu či v současnosti velmi rozšířené platformě Youtube. V těchto případech je velmi obtížné s tím něco dělat.

V poradně se mimo jiné objevovaly konkrétní případy online vydírání, které měly podobné scénáře – dospělého muže prostřednictvím Facebooku oslovila dívka a začali spolu komunikovat. Komunikace se stávala čím dál intimnější, postupně se přesunula do prostředí Skype, kde spolu dívka a muž provozovali videochat. Výsledkem pak byl únik intimních materiálů a následná platba jakéhosi výpalného za to, že videozáznam nebude zveřejněn. Obdobný případ byl zachycen i u dětí – na poradnu se obraceli rodiče s tím, že jejich dítě se stalo terčem podobného typu útoku.

Do poradny psali i klienti, kteří byli svému partnerovi či partnerce nevěrní a stali se terčem msty – jejich partneři začali šířit intimní materiály po internetu a poškozovali jim pověst. Tento čin je často spojen s nezvládnutým rozchodem – expartner či expartnerka si tímto způsobem vyřizují účty, zakládají jim falešné profily, objevil se i případ nabízení erotických služeb či zveřejňují kontaktní údaje a sdílejí intimní materiály.

Tabulka počtu případů v poradně od roku 2009 do 2019



Podle tabulky má v posledních letech počet případů zachycených poradnou E-bezpečí vzrůstající tendenci. Mění se také jejich obsah. V minulých letech převažovaly případy agrese, verbálních útoků, případně stalkingu, v současnosti však narůstá počet případů spojených s tzv. sextingem.

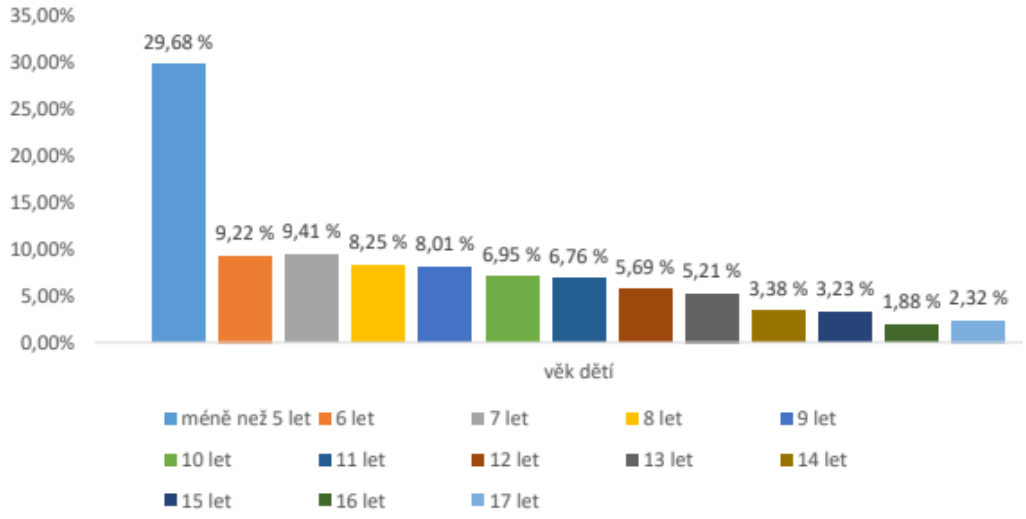
Výzkumy provedené serverem E-bezpečí

Rodič a rodičovství v digitální éře

Výzkum byl proveden v roce 2018 a zapojilo se celkem 1093 respondentů - rodičů. Z toho 86 % žen a 14 % mužů ve věku od 25 do 64 let. Průměrný věk respondentů činil 37,7 let. Dotazník vyplňovali participanti ze všech krajů ČR – nejvíce však z hlavního města Prahy, Moravskoslezského a Středočeského kraje. Necelou polovinu dotázaných tvořili rodiče, kteří mají 2 děti a poté respondenti s jedním dítětem, necelých 30 %.

Výzkum byl zaměřen na chování respondentů ve světě online technologií, digitální gramotnost a výchovu svých dětí s ohledem na prevenci rizikového chování v online světě.

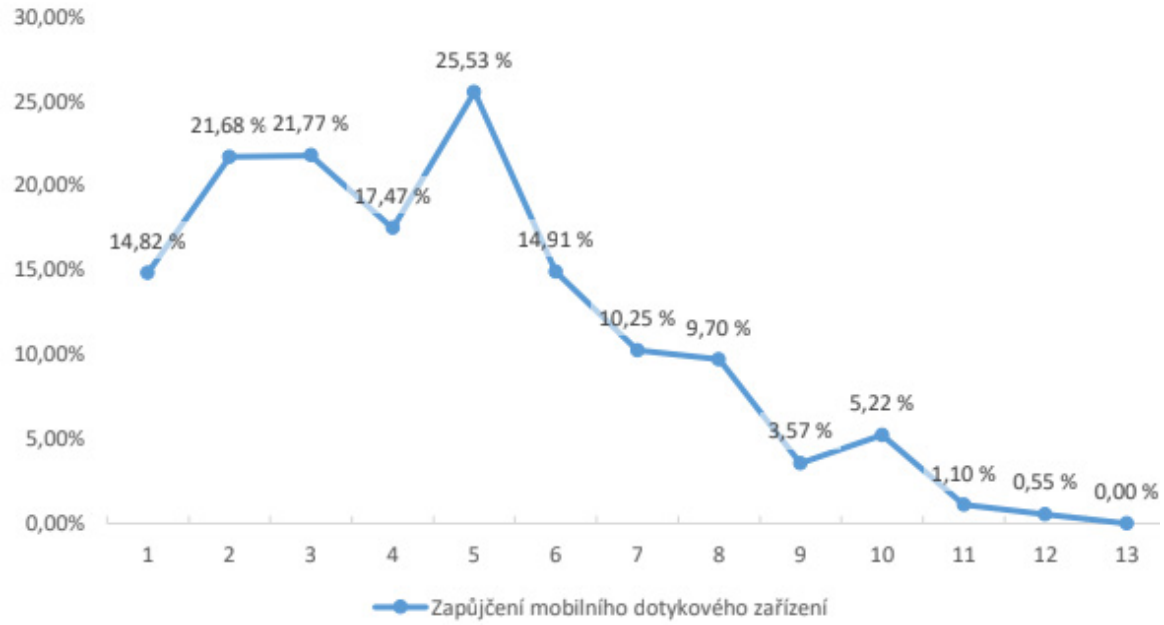
Tabulka s věkovou strukturou dětí respondentů



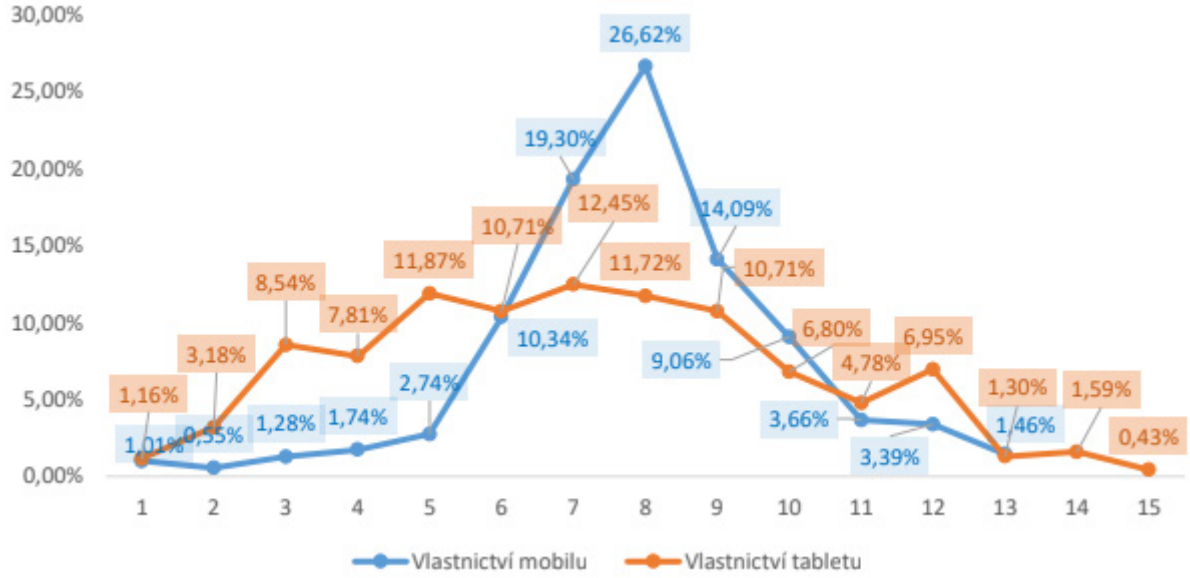
Rodiče patří mezi nejdůležitější prvky při výchově dětí. A jsou to z velké části oni, kdo jim jako první pořídí mobily či jim je zapůjčí. Výzkum se v tomto případě zaměřil na to, v kolika letech zažilo jejich dítě první kontakt s mobilním dotykovým zařízením (mobilem a tabletem).

Podle průzkumu se děti dostanou do kontaktu s těmito zařízeními již od prvního roku života. K výraznému poklesu dochází ve věku 6-7 let, kdy děti začínají získávat vlastní zařízení:

Graf zápůjčky mobilního zařízení



Nejvíce dětí pak dostává vlastní mobilní telefon v rozmezí 7-9 let. Souvisí to hlavně s přechodem na základní školu, kdy přístroj slouží jako komunikační nástroj. Zajímavostí je, že někteří rodiče pořídili dětem dříve tablet než mobil.



Důležitou částí výzkumu bylo to, zda rodič ví o chování svých dětí v online prostředí a také jestli je schopen zajistit v online prostředí bezpečí. Podle výsledků výzkumu se 73 % rodičů snaží svým dětem internet omezovat. Hlavní otázkou je jakým způsobem, protože drtivá většina rodičů nevyužívá žádný bezpečnostní systém – např. antivir či jiné softwarové nástroje.

Tabulka nejčastějších odpovědí

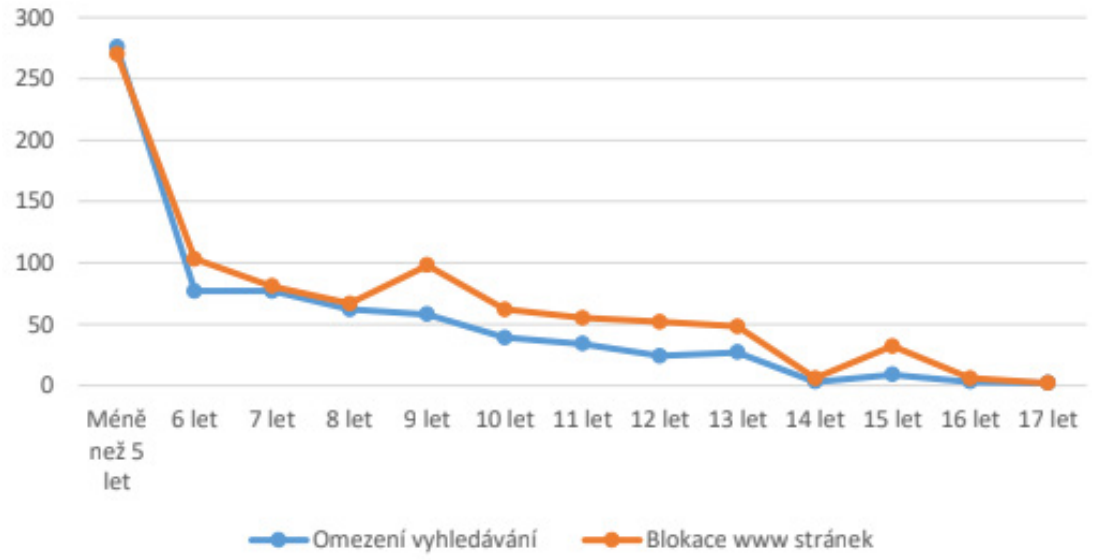
Způsob limitování času	Absolutní četnost (n)	Relativní četnost (%)
Ústní dohodou s dítětem (rodič provádí důslednou kontrolu).	753	68,89
Vypnutím techniky (dítě samo vypne techniku, respektuje dohodu).	493	45,11
Odebráním / poskytnutím techniky dítěti.	417	38,15
Ústní dohodou s dítětem (rodič neprovádí kontrolu).	303	27,71

Velmi důležité je, jestli rodiče ví, co jejich dítě/děti dělají v online prostředí. Průzkum ukázal, že 82 % z nich odpovědělo, že vědí, jaké informace na internetu jejich děti vyhledávají. Na druhou stranu, 13 % přiznalo, že nevědí. Další otázka byla zaměřena na znalost rodičů o obsahu vyhledávaných webových stránek. I v tomto případě přes 80% znalo druh informací, které jejich potomci vyhledávali. I proto 38 % z nich omezuje možnosti vyhledávání, naopak 63 % rodičů vůbec.

Nejčastější obsah, který rodiče dětem omezují

Typ obsahu	Absolutní četnost (n)	Relativní četnost (%)
Sexuálně laděný obsah	576	52,7
Násilný nebo odpudivý obsah	564	51,60
Nenávistný nebo urážlivý obsah	474	43,37
Sebepoškozování	464	42,45
Propagace terorismu	452	41,35

Graf omezování přístupu k obsahu



V online prostředí se vyskytují velká rizika a nebezpečí, jak již bylo zmíněno, a proto je nutné aktivní zapojení rodičů do procesu primární prevence. Mezi nejrozšířenější způsob prevence patří rozhovor rodiče s dítětem o nebezpečí internetu. Další metoda primární prevence, která bývá také často využívána, je dialog opačným směrem, kdy dítě musí učit rodiče o nebezpečí internetu.

Tabulka preventivních aktivit

Preventivní aktivita	Absolutní četnost (n)	Relativní četnost (%)
Rozhovor s dítětem o nebezpečích na internetu (rodič učí dítě).	836	76,49
Rozhovor s dítětem o nebezpečích na internetu (dítě učí rodiče a rodič na informace reahuje např. dítě řekne rodiči, co dělalo na internetu, jaké youtubery sledovalo atd.).	560	51,24
Prevenci v oblasti rizik na internetu jsme zatím neřešili.	164	15,00

Projekt „Kraje pro bezpečný internet“

Mobilní telefony, počítače a internet se staly v posledních letech naprostou samozřejmostí a součástí životů většiny z nás. Usnadňují nám život, můžeme díky nim bez problémů komunikovat s lidmi po celém světě, nakupovat z pohodlí obývacího pokoje, vzdělávat se, bavit se.

S novými technologiemi se musíme naučit zacházet, a to nejen po stránce manuální, ale především po stránce mentální. Je nutné se učit odolávat rozesílán hoaxů, zodpovědně zacházet se svými osobními údaji. Všechno často směřuje ke kyberšikaně či sextingu.

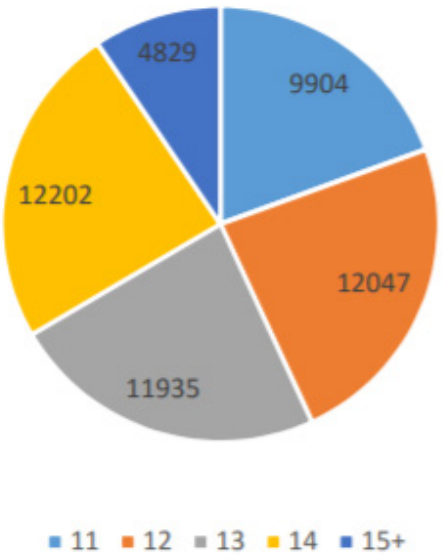
Projekt „Kraje pro bezpečný internet“ je podporovaný Asociací krajů České republiky, a byl schválen usnesením Rady Asociace krajů České republiky v roce 2013. V roce 2019 má projekt za úkol oslovit co nejširší a věkově různorodou veřejnost, především prostřednictvím aktualizovaných e-learningových lekcí, video spotů a vědomostních kvízů.

Výzkumy provedené Kraje pro bezpečný internet

Vnímání kyberkriminality mezi dětmi

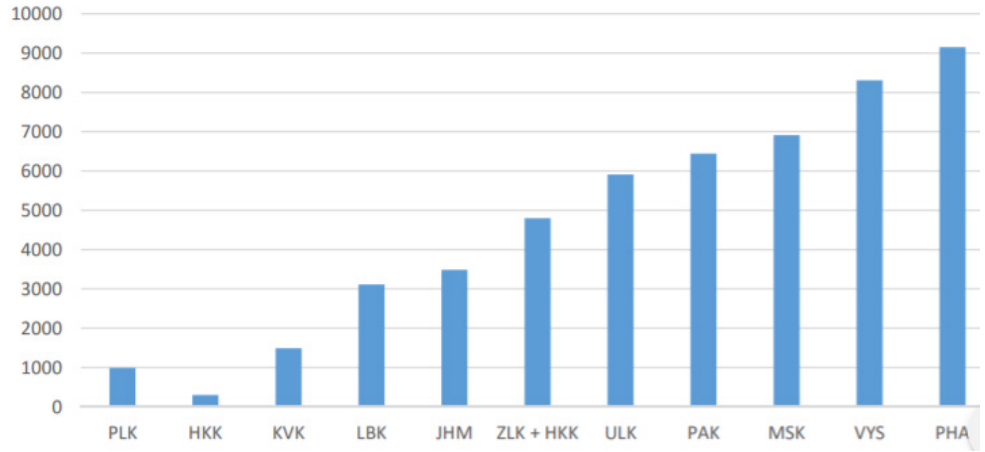
Cílem výzkumu je analyzovat znalosti a zkušenosti žáků s kyberkriminalitou a rizikovými jevy na internetu obecně. Cílovou skupinou výzkumu bylo tvořeno žáky druhého stupně základních škol, tedy žáky šesté až deváté třídy od 11 do 16 let. Do výzkumu se zapojili i žáci z víceletých gymnázií z jedenácti krajů. Celkem se zúčastnilo 50 917 respondentů. Průměrný věk respondentů by 12,80 let. Co se týče počtu dívek a chlapců, tak se dá konstatovat, že se od sebe tolik nelišil. Dívek se zúčastnilo 49,1 %, tedy 24 988 a chlapců se zúčastnilo v celkovém počtu 25 929, což odpovídá 50,9 %.

Graf věkového složení respondentů



Počet respondentů v jednotlivých krajích se velmi lišil. Bylo to dáno tím, že se školská zařízení do výzkumu zapojovala dobrovolně a rovněž podpora krajských koordinátorů byla rozdílná. Přes odlišné počty dotazovaných nejsou mezi jednotlivými kraji výraznější odchylky.

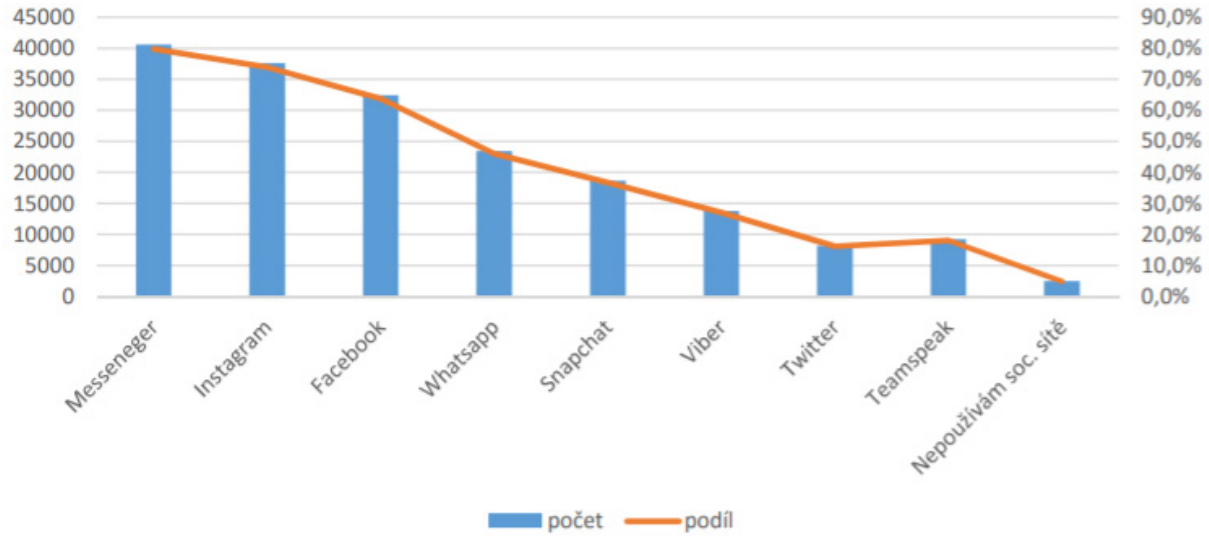
Graf počtů respondentů v krajích



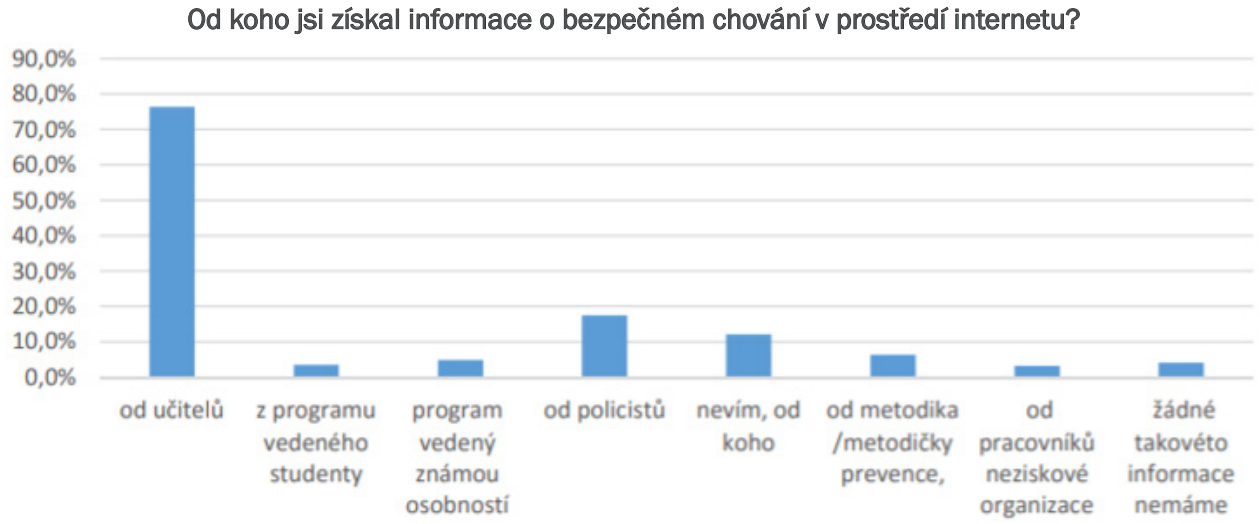
Hlavním tématem bylo **využívání sociálních sítí** žáky. Tyto výsledky napověděly pedagogům i preventivním pracovníkům, na které sociální sítě se zaměřit při výuce bezpečného využívání a na jakých sítích žáky nejlépe oslovit.

V jednotlivých krajích byly výsledky podobné, protože nejčastější odpovědí a nejužívanější sítí se stal facebookový nástroj Messeger. Užívá ho celkově 79,8 % žáků. Výjimkou je hlavní město Praha, kde nejpoužívanějším je sociální síť Instragram.

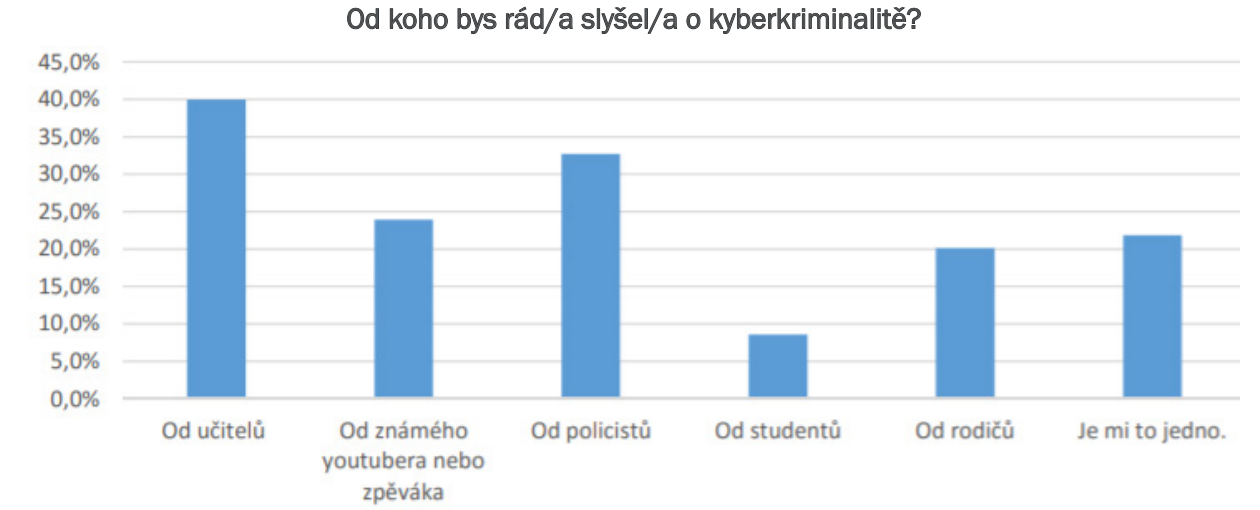
Graf užívání sociálních sítí



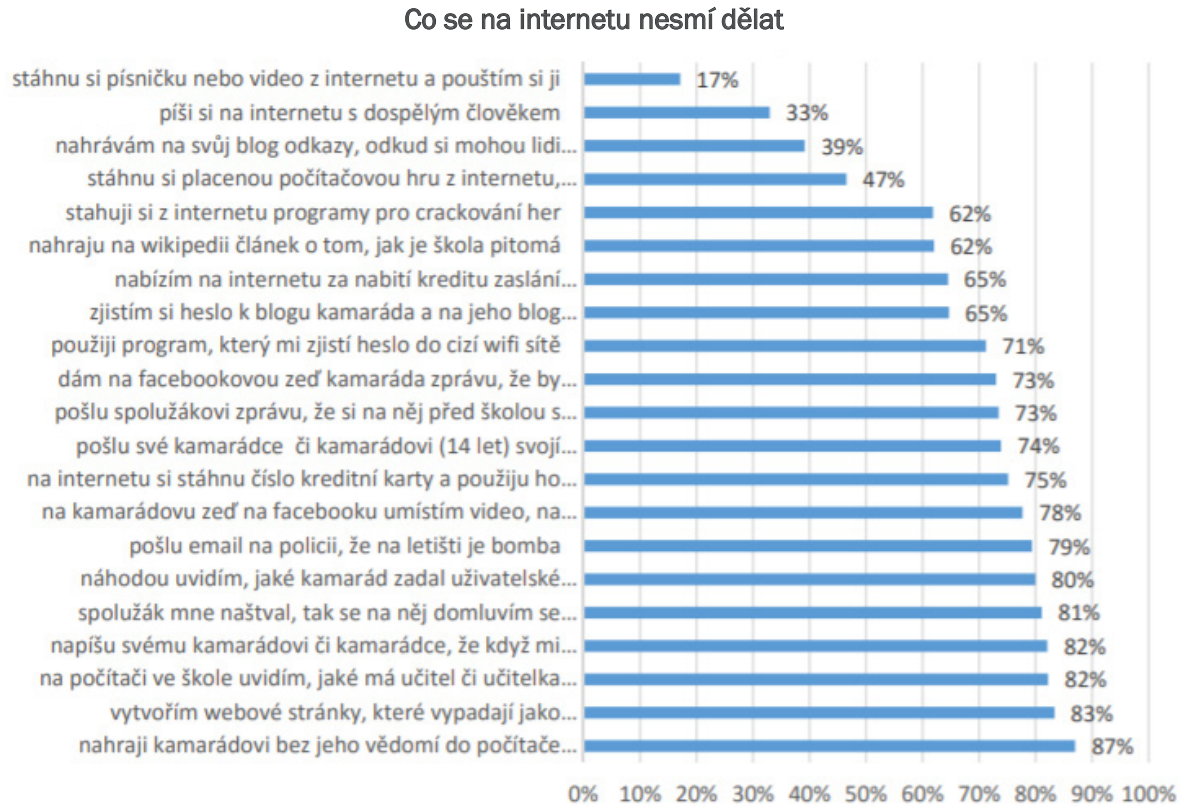
Zásadním tématem výzkumu byla znalost kyberkriminiality. Cílem otázky bylo zjistit, kdo prevenci v jednotlivých školských zařízeních provádí. Žáci informace nejčastěji získávají od učitelů ve školách (přes 76 %), na druhém místě jsou pak policisté a poté rodiče.



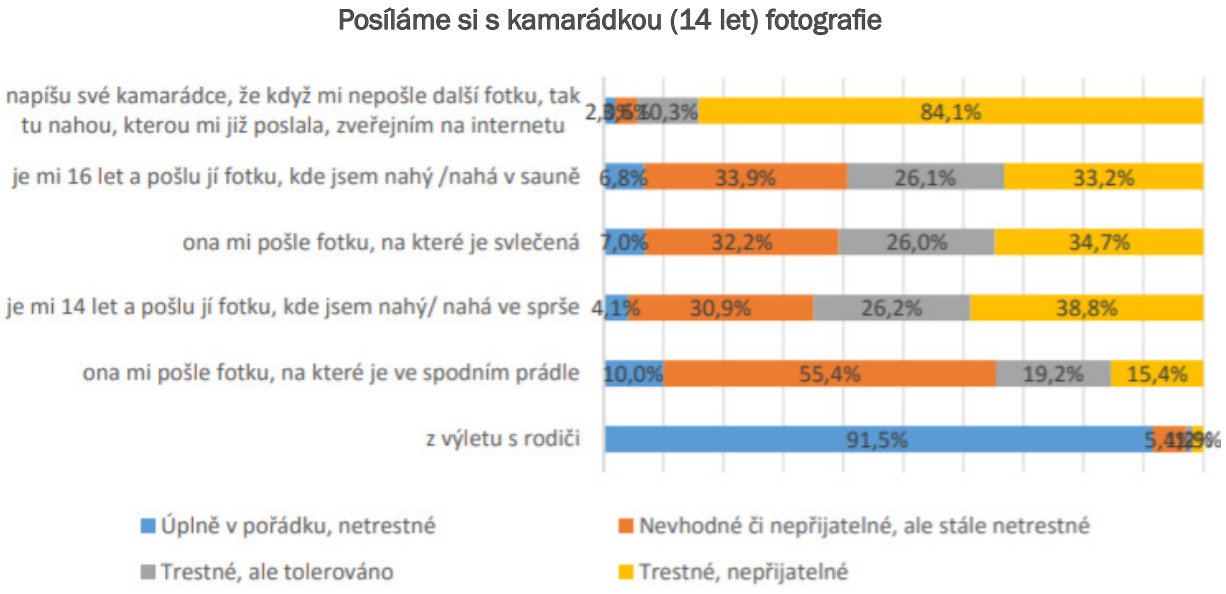
V souvislosti na první otázku byli žáci dotazováni, **od koho by rádi slyšeli informace o kyberšikaně a bezpečném chování na internetu.** Výsledek ukázal, že žáci preferují jako zdroj informací opět **učitele, celkově 40 %**, následují **policisté, celkově 32,7 %**, poté **od nějakého známého youtubera či zpěváka, celkově 23,9 %.**

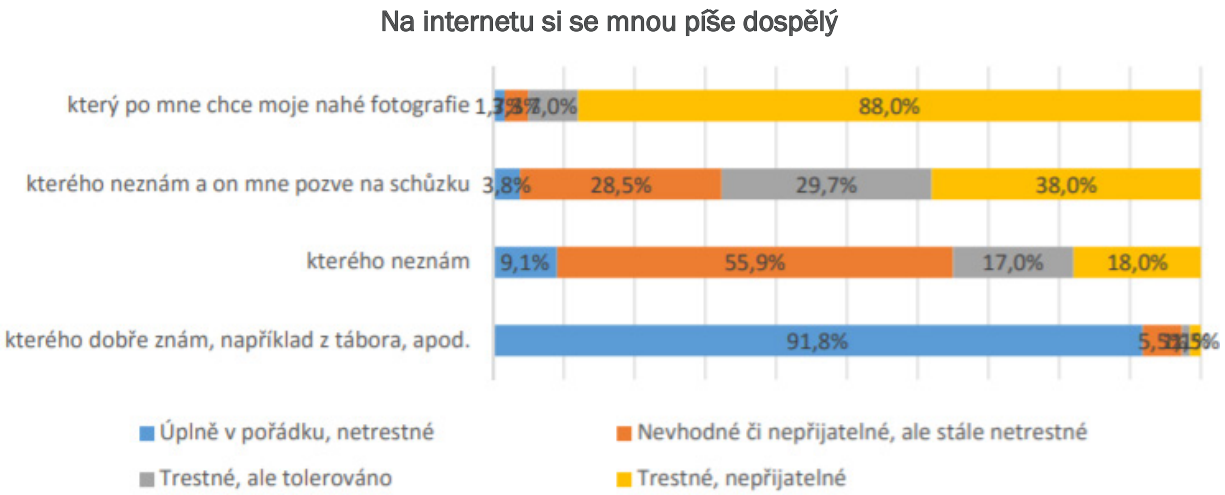


Co se týče znalostí kyberkriminality, vybírali žáci z možností, jaké jednání je protizákonné. Konkrétně, co se nesmí na internetu dělat. Výsledky mezi kraji se výrazně nelišily. Nejvíce žáků (80 %)označilo jako kyberkriminalitu možnost „**nahraji kamarádovi bez jeho vědomí do počítače program, abych se mohl dívat, co na počítači dělá**“. Následovala odpověď phishing, ten žáci označili jako trestný v 83 %, vyhrožování přes internet 82 %, neoprávněný přístup k počítačovému systému 82 % odpovědí.



Dalším typem otázek byl výběrový. Konkrétně, museli rozpoznat co je závažné a co ne. Cílem bylo zjistit, kde mají žáci nastavenou hranici, jaké jednání je podle jejich názoru ještě v kyberprostoru přijatelné a co už ne. Měli výběr z čtyřbodové škály: **1 – „úplně v pořádku, netrestné," 2 – „nevhodné či nepřijatelné, ale stále netrestné," 3 – „trestné, ale tolerováno" až po 4 – „trestné, nepřijatelné"**.





Z dotazníkového šetření vyplynulo, že v současné době jsou žáci na sociálních sítích stále aktivnější. Pouze **4,8 % žáků uvedlo, že neužívá žádné sociální sítě**. Nejvíce užívanou sociální sítí je Messenger, **kde má svůj účet 79,8 % žáků, následovaný Instagramem u 73,8 % žáků**. **Facebook je až na třetím místě, svůj účet na něm má 63,7 % žáků**. Informace o bezpečném chování v prostředí internetu získávají žáci nejčastěji **od učitelů (76,4%), dále od policistů (17,5 %) a v 12,2 % nejsou schopni žáci určit, od koho informace mají**. Žáci preferují informace o bezpečném chování na internetu podané od učitelů (40 %), následované preferencí informací od policistů (32,7 %) a od známé osobnosti (23,9 %). Výsledky provedeného výzkumu ukázaly, že **žáci mají stále nedostatečné znalosti takřka ve všech oblastech týkajících se rizikového chování na internetu a kyberkriminality**.

Linka bezpečí

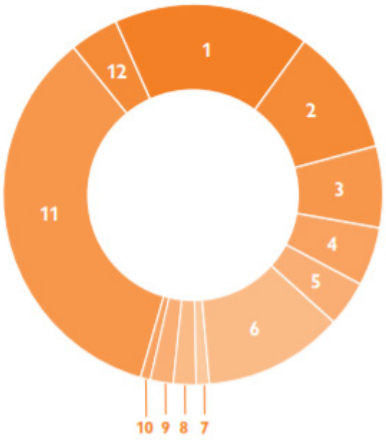
V roce 2017 Linka bezpečí přijala celkem 151 421 hovorů – což je více než 400 hovorů denně. Nejvíce volali děti mezi 13 a 16 lety, přičemž dívky mají častěji než chlapci k řešení konkrétní téma. Nejčastěji řešené otázky se v roce 2017 nezměnily, pětina dětí se svěřila s problémy sexuálního zrání, dále pak s osobními problémy. K předání konkrétního odkazu na další instituci došlo při dovolání na centrálu 5297 a dále minimálně v 1506 tematických hovorech s dětmi. Podle posledních průzkumů zaznamenala Linka bezpečí v roce 2018 2182 telefonátů, e-mailů či chatů, což bylo o 100 více než o rok dříve.

Online služby Linky bezpečí: chat a e-mailová poradna 2017

Linku bezpečí mohou děti kontaktovat nejen po telefonu, ale i přes on-line komunikační kanály – chat a e-mail. Ze statistik Linky bezpečí je patrné, že tyto dva způsoby komunikace jsou pro děti také velmi důležité, protože pro mnohé z nich je písemná forma pro otevření závažného či intimního tématu přijatelnější.

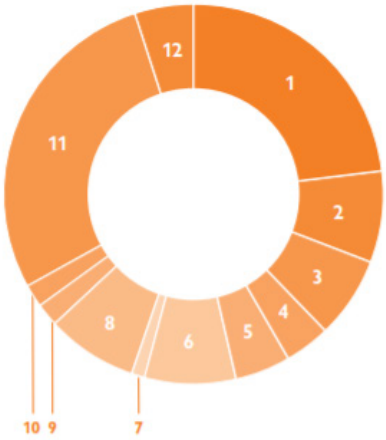
Prostřednictvím chatu Linky bezpečí bylo zaznamenáno v roce 2017 nejvíc dotazů za dobu jeho provozu − 2017, což znamená nárůst o více než 820 příspěvků ve srovnání s rokem 2016. Nejčastěji se děti svěřovaly s psychickými problémy nebo sebevražednými myšlenkami. Dalším klíčovým tématem byly zkušenosti dětí se sebepoškozováním. Sebevražedné myšlenky a sebepoškozování byly v mnoha případech důsledkem dalších trápení – problémů v rodině, týrání či zneužívání. V e-mailové poradně v roce 2017 také přijali rekordní počet dotazů – 2827. Důvodem může být přetrvávající příklon dětí ke komunikaci přes internet, lepší propagace této služby prostřednictvím facebookového profilu Linky

bezpečí či projektu Linka bezpečí ve vaší třídě. K nejčastěji řešeným tematickým okruhům patřily i zde psychické obtíže. Závěrem lze říci, že komunikace o závažných tématech se mnohým dětem jeví snazší právě prostřednictvím on-line kanálů. Při psaní nemusí skrývat pláč, který tato témata často provází.



zastoupení témat na chatu (2017)

1 rodinné vztahy **17 %**
2 CAN **11 %**
3 partnerství a láska **7 %**
4 vrstevnické vztahy **5 %**
5 škola **4 %**
6 osobní témata **12 %**
7 závislosti **1 %**
8 jiná témata **2 %**
9 sexuální vyzrávání **2 %**
10 internet **1 %**
11 psychické obtíže **35 %**
12 šikana **4 %**

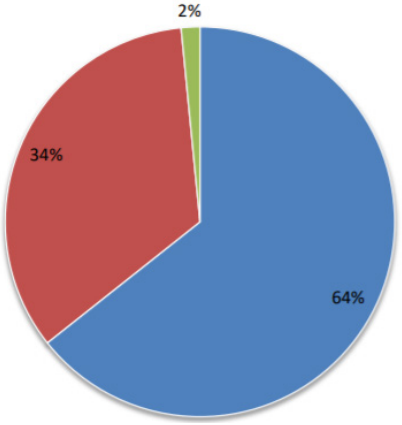


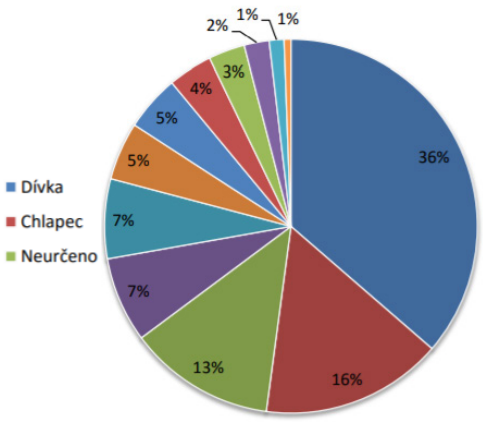
zastoupení témat v e-mailové poradně (2017)

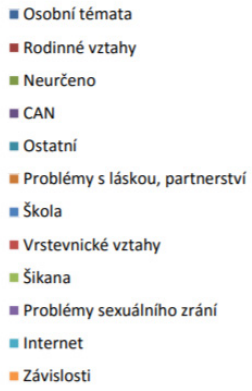
1 rodinné vztahy **24 %**
2 CAN **8 %**
3 partnerství a láska **7 %**
4 vrstevnické vztahy **4 %**
5 škola **5 %**
6 osobní témata **8 %**
7 závislosti **1 %**
8 jiná témata **8 %**
9 sexuální vyzrávání **2 %**
10 internet **2 %**
11 psychické obtíže **29 %**
12 šikana **5 %**

Online služby Linky bezpečí: chat a e-mailová poradna 2015

V roce 2015 přijala Linka bezpečí stabilně kolem 900 chatů ročně. Co se týče zastoupení pohlaví, ozvalo se 64 % dívek a 34 % chlapců. Zbylá 2 % se nedala určit. Děti se také nejčastěji na chatu svěřovaly s osobními problémy, které souvisely se šikanou nebo zneužíváním.







Děti rovněž využívaly e-mailovou komunikaci s pracovníky Linky bezpečí. V roce 2015 zaznamenala Linka rekordní počet dotazů. Důvodem byl nárůst internetových možností a větší příklon dětí ke komunikaci přes internet.

Podle ředitelky Linky bezpečí Kateřiny Liškové dostávají konzultanti zhruba 430 kontaktů, jelikož některé děti jim volají opakovaně, jiné zase píší e-maily či s odborníky chatují. Podle statistik převažují dívky, které jsou obecně sdílnější a nejčastější věková hranice je mezi 12 a 17 lety. Linka bezpečí se v poslední době velmi často setkává s kyberšikanou. Snaží se jim poradit možnosti např. obrátit se na Policii ČR, agresory zablokovat a snažit se omezit kontakt na minimum.

Dětské krizové centrum

Dětské krizové centrum (DKC) působí v oblasti šikany již 25 let. Řeší nejzávažnější případy fyzického, psychického a sexuálního násilí na dětech. Patří mezi nejznámější specializované zařízení, které má celorepublikovou působnost. Od vzniku, v roce 1992, využilo ambulantních služeb DKC 6 200 klientů, prostřednictvím Linky důvěry DKC přijalo 56 000 kontaktů.

Linka důvěry DKC

Od roku 2017 centrum spustilo nové číslo Linky důvěry – Rizika kyberprostoru! Podle zdroje EU Kids Online hledá 40 % dětí na internetu nové kamarády, přičemž celkem 58 % českých dětí považuje seznamování a komunikaci s lidmi na internetu za riskantní a 76 % dotázaných si myslí, že osobní schůzka s neznámými lidmi z internetu je nebezpečná. Přesto podle výzkumu na ni šlo 55 % z nich.

V rámci nové formy ohrožení rozšířilo centrum svoji působnost a reaguje na ohrožení dětí v kyberprostoru. Cílem linky důvěry DKC je poskytnout poradenství a krizovou intervenci všem dětem, které se setkaly nebo jsou ohroženy v kyberprostoru. Patří sem také ochrana práv dětí, informace o možnostech řešení kyberšikany atd.

Statistiky Dětského krizového centra v roce 2017

DKC v roce 207 poskytlo své služby 366 ohroženým dětem. Věnuje se nejen dětem, ale i dospělým. Celkový počet uživatelů, kteří využili služby DKC, dosáhl v roce 2017 čísla 820.

Podle statistik nejvíce klientů bylo z Prahy (55 %), dále pak ze Středočeského kraje (34 %).

Praha	55 %
Středočeský kraj	34 %
Ostatní kraje	11 %
Celkem	**100 %**

Samotná Linka důvěry DKC v roce 2017 přijala 3 598 kontaktů.

Vstupní problematika	Počet ohrožených dětí	%	Počet uživatelů	%	Počet uživatelů	%
Fyzické týrání	32	*9*	*75*	*9*	*2 034*	*19*
Psychické týrání	7	2	14	2	426	4
Sexuální zneužívání	135	37	279	34	4 552	42
Ohrožující prostředí	59	16	123	15	1 995	19
Vyhrocený spor o dítě	20	5	26	3	157	1
Jiná problematika	113	31	304	37	1630	15
Celkem	**372**	**100**	**746**	**100**	**6 638**	**100**

Kybergrooming - jedná se o sexuální zneužívání dětí spojená s jejich pohybem na internetu, hlavně na sociálních sítích. Mezi závažné rizikové faktory patří volné dostupné pornografické stránky, a to i pro nezletilé děti, které se dokáží volně pohybovat v kyberprostoru, a to i bez jakékoliv kontroly. Dostávají se tedy například k pornografickému materiálu ještě dříve, než odpovídá jejich psychologickému vývoji. Výsledkem je neadekvátní chování dětí, při němž opakují, co viděly, v rámci sexuálního experimentování s výrazně mladšími dětmi z rodiny (mladší sourozenci, sestřenice, bratranci atd.) či mimo své rodiny (děti ze školy, sousedství atd.).

Nejvíce případů musela linka řešit v oblasti rodinné problematiky, dále pak sexuální problematiky, šikany a kyberprostoru.

Převažující problematika v kontaktech přijatých LD DKC v roce 2017	
Syndrom CAN	831
Rodinná problematika	839
Vrstevnická problematika	94
Osobní a existenciální problematika	1 792
Partnerská a manželská problematika	200
Sociálně právní problematika	429
Zdravotní problematika	142
Sexuální problematika	183
Závislosti	59
Sociální patologie	54
Šikana, kyberprostor	118
Jiná traumatizující událost	79

Europ Assitance Česká a Slovenská republika

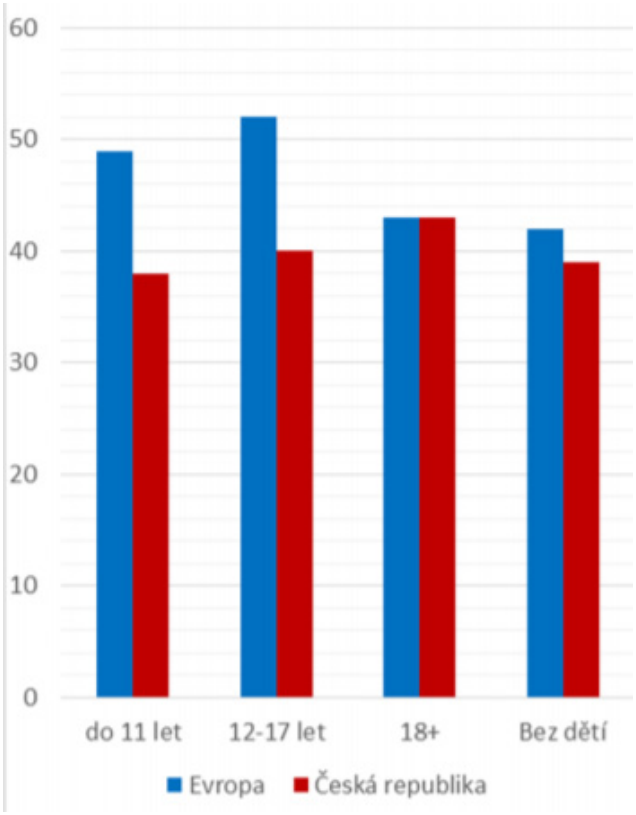
V roce 2018 vydala společnost Europ Assitance výzkum, který se zabýval, jak moc se Češi bojí o své děti v oblasti internetu. Průzkumu se zúčastnilo 7200 respondentů z celkem devíti zemí.

Z výsledků se dá vyčíst, že se čeští rodiče příliš nestarají o to, jaké nebezpečí čeká jejich děti na internetu. Jen dva z pěti rodičů nezletilých dětí má vážné obavy, že by mohlo na internetu dojít k trestnému činu. Evropský průměr je přitom o 10 % vyšší. Z tzv. sexuálních predátorů má pak strach 35 % českých rodičů, v Evropě je to celá polovina.

Výzkum ukázal, že mladí Češi chápou internet jako bezpečné prostředí a nevnímají rizika, s tím spojená, které mohou zasáhnout i jejich příbuzné. V evropském srovnání jsou Češi společně s Rakušany na spodních příčkách. Třetina Evropanů ve věku 25 – 44 uvedla, že se vážně obává o bezpečnost svých blízkých na internetu. V České republice to bylo méně než 16 %.

Konkrétně se k tomu přiznal každý pátý rodič dítěte ve věku do 11 let. V Evropě jich přitom průměrně bylo 36 %. Rodiče s dospívajícími dětmi (12 – 17 let) se o jejich bezpečnost na internetu obává 21 %, v Evropě 38 %. Dvě pětiny (38 %) českých rodičů s dětmi do 11 let se obává, že na internetu může dojít k trestnému činu.

Obavy z trestné činnosti online - velké obavy podle dětí v rodině



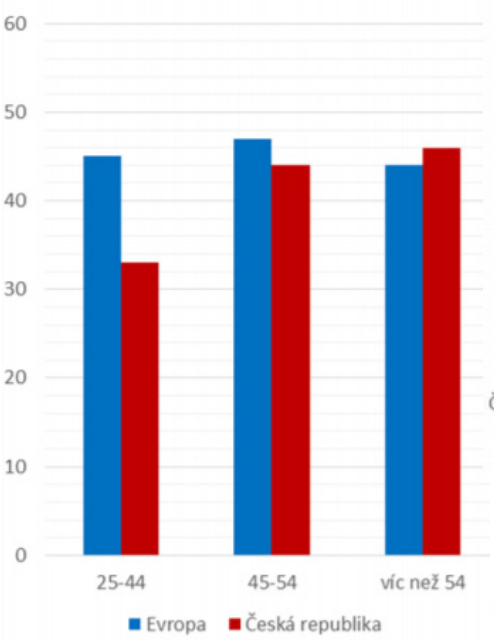
Z obecného pohledu lze konstatovat, že mladí lidé získávají zkušenosti s internetem už během dospívání a v životě dítěte je považováno za běžnou součást jejich života. To může způsobit, že je pro ně kyberprostor bezpečným místem. Starší generace je vůči internetu obezřetnější a mají k jeho využívání větší respekt.

Jedním z hlavních důvodů podceňování internetu je nedostatek informací. Z dřívějších výsledků vyplynulo, že Češi se v hrozbách internetu příliš neorientují. Pro děti je důležité, aby jim rodiče předávali relevantní informace a správně bezpečné zásady chování na internetu.

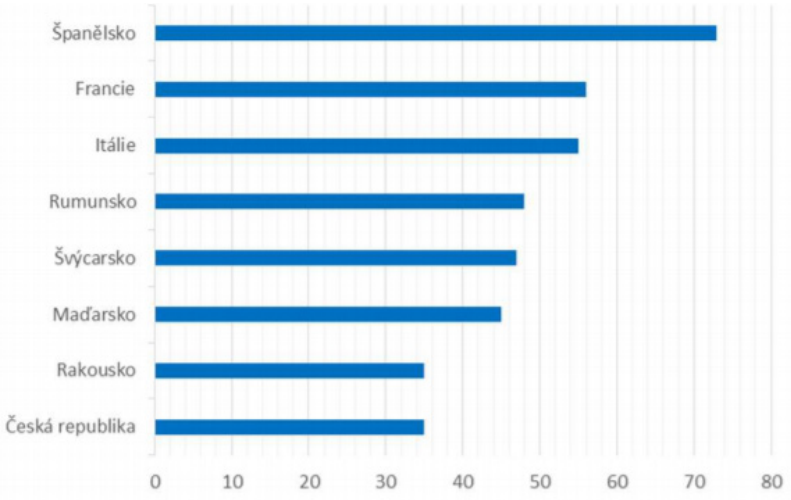
Průzkum Euro Assistance se také zaměřil na otázku, jak moc se rodiče bojí sexuálních predátorů, na které mohou jejich děti v kyberprostoru narazit. Vážné obavy mělo 35 % českých rodičů. V Evropě to byla skoro polovina, 49 %. Nejcitlivější v tomto ohledu byli Španělé, kde se doznalo 73 % rodičů, následovanými Francouzi (56 %) a Italové (55 %). Naopak podobně ve výsledku dopadli Češi společně s rodiči z Rakouska (35 %).

Rodiče z České republiky podobně mírně hodnotili také riziko online šikany, přitom v jiných evropských státech toto téma patřilo mezi nejvýraznější hrozby.

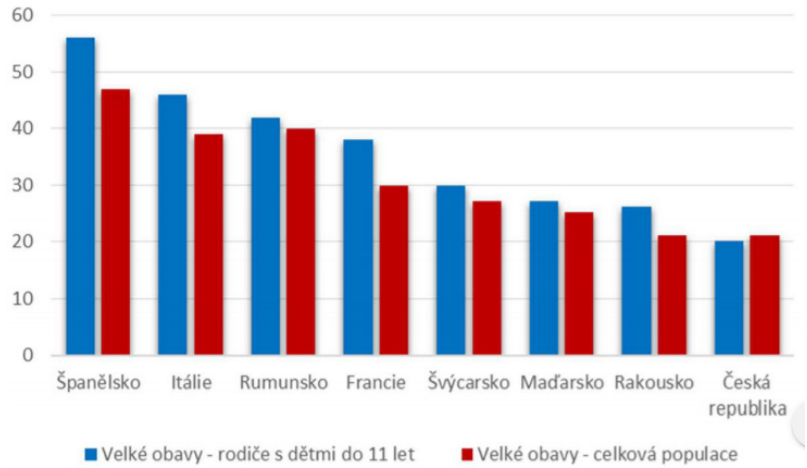
Obavy z trestné činnosti online
- velké obavy podle věku



Podíl rodičů s velkými obavami ze sexiálních predátorů



Pořadí států podle toho, kde rodiče nejvíce vnímají rizika, která hrozí online jejich rodině

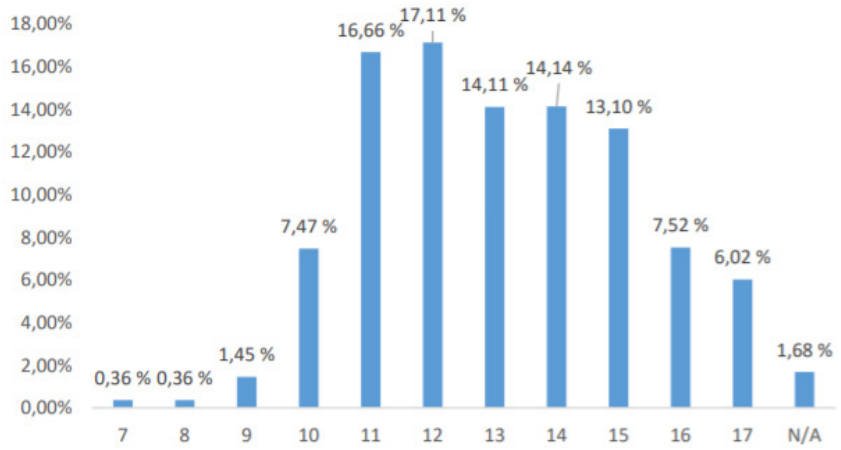


O2 Chytrá škola

Společný výzkum společnosti O2 a Univerzity Palackého v Olomouci – České děti v kybersvětě

Výzkum se převážně věnuje aktivitám dětí v online světě, hlavě s jakými riziky a hrozbami se setkávají. Taktéž se zaměřuje na problematiku používání mobilního telefonu dětmi ve školách např. o přestávkách.

Zapojilo se 27 177 respondentů ve věku 7 až 17 let ze všech krajů České republiky, z toho 49,83 % tvořili chlapci. Průměrný věk byl 13,04 let. Nejvíce dotazovaných pocházelo z Moravskoslezského, Olomouckého a Středočeského kraje. a Středočeského kraje.



Prvním otázka se týkala nejčastěji navštěvovaných webových stránek. V této fázi byli respondenti rozděleni do dvou skupin – děti mladší 13 let a respondenti nad 13 let. Důvodem rozdělení bylo, že většina online služeb má hranici 13 let, od kdy je možné službu využívat. Potvrdil se předpoklad, že děti mladší 13 let ji budou porušovat.

Tabulka A: Které internetové stránky/služby na internetu využívají děti mladší 13 let

Internetová stránka/služba	Absolutní četnost (n)	Relativní četnost (%)
Sociální sítě.	6 106	51,75
Servery pro sdílení videosouborů (např. YouTube, Vimeo, Stream apod.)	4 850	41,10
Online encykopedie (např. Wikipedia, CoJeCo apod.)	3 578	30,32
Stránky s herní tématikou (on-line hry, návody na hraní her apod.)	3 483	29,52
Úložiště souborů (např. Hellspy, Ulož.to apod.).	2 479	21,01
Eshopy, bazary, aukční servery.	1 789	15,16
Servery pro streamování obsahu (např. Twitch apod.)	1 307	11,08
Vzdělávací stránky (Khanova akademie, MOOC kurzy apod.).	901	7,64
Online videochat (např. Omegle, Ome.tv apod.).	890	7,54

Internetová stránka/služba	Absolutní četnost (n)	Relativní četnost (%)
Zpravodajské portály (např. Idnes.cz, Ihned.cz, Lidovky.cz apod.).	867	7,35
Stránky s pornografií	335	2,84

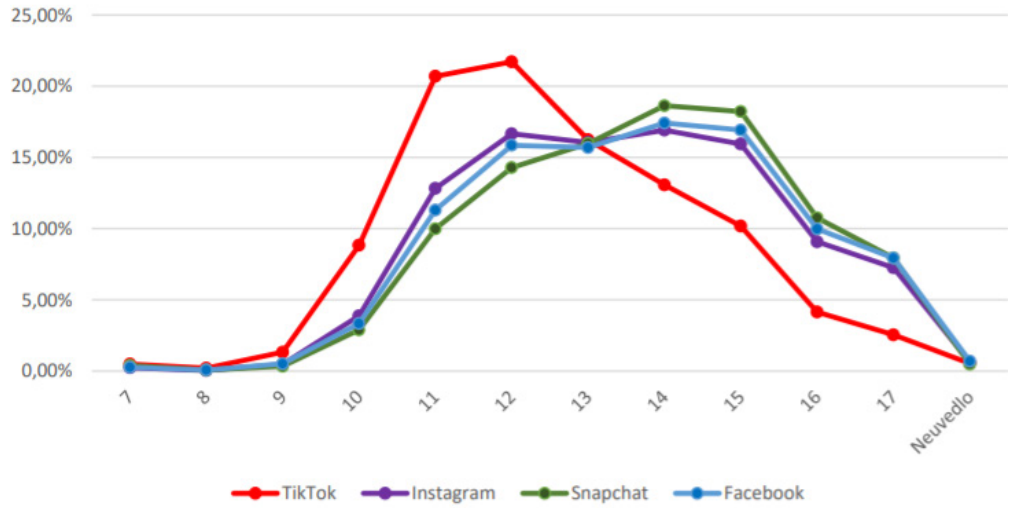
Tabulka B: Které internetové stránky/služby na internetu využívají děti nad 13 let

Internetová stránka/služba	Absolutní četnost (n)	Relativní četnost (%)
Sociální sítě.	11 282	75,61
Servery pro sdílení videosouborů (např. YouTube, Vimeo, Stream apod.)	8 343	55,91
Online encykopedie (např. Wikipedia, CoJeCo apod.)	5 853	39,23
Eshopy, bazary, aukční servery.	4 265	28,58
Úložiště souborů (např. Hellspy, Ulož.to apod.).	4 192	28,09
Stránky s herní tématikou (online hry, návody na hraní her apod.).	3 894	26,10
Servery pro streamování obsahu (např. Twitch apod.).	2 970	19,90
Stránky s pornografií	2 698	18,08
Zpravodajské portály (např. Idnes.cz, Ihned.cz, Lidovky.cz apod.).	2 581	17,30
Vzdělávací stránky (Khanova akademie, MOOC kurzy apod.).	1 037	6,95
Online videochat (např. Omegle, Ome.tv apod.).	823	5,52
Stránky na darknetu.	608	4,07
Stránky s násilným obsahem.	560	3,75
Jiné	29	0,19
Neuvedlo	401	2,69

Dle statistik lze vyčíst, že k rizikům patří využívání sociálních sítí malými dětmi – 23 % dětí z celého výzkumu (51,75 % je mladších 13 let) využívá sociální služby, i přesto, že nesplňují věkový limit. Výzkum také zachytil negativní čísla v podobě využívání online videochatů (aplikace Omegle) u dětí mladších 13 let.

Na otázku, jaké další online nástroj děti aktivně používají, jednoznačně dominoval kanál YouTube. Bylo prokázáno, že tuto platformu sleduje drtivá většina respondentů českých dětí (59,51 %), následuje Facebook, Messenger, Instagram a pak tradiční nástroje jako je e-mail a posílání SMS. Nově se však objevila plat- forma TikTok, v současné době hojně využívá 28,48 % českých dětí.

Zajímavé je sledovat i věkové složení respondentů a jejich využívání různých aplikací. Facebook a Instagram používají spíše respondenti ve věku 12 – 14 let, zatímco hudební platformu TikTok děti 10 – 11 let. Je to dáno tím, že skrze TikTok mohou děti sdílet krátká hudební videa a převážně cílí na mladší publikum.



Průzkum se také dotýkal otázky, které vyhledavače děti nejvíce používají. K žádnému překvapení nedošlo a k prohlížeči od společnosti Google se přihlásila drtivá většina dětí, tedy 84,04 %. Na druhé místě se umístil český vyhledávač Seznam.cz, který za Google hodně zaostal (10 %).

Výzkum se zaměřil i na hojně diskutovanou otázku ohledně spojení dětí a mobilních telefonů. Více než polovina děti potvrdila, že ve svém mobilním telefonu má volný přístup na internet a jsou na Wi-Fi sítě nezávislá. Nejvyužívanější platformou na mobilech je Facebook, Messenger či WhatsApp, potvrdilo to 66 % dětí.

Nejčastější aktivity dětí s mobilním telefonem

Internetová stránka/služba	Absolutní četnost (n)	Relativní četnost (%)
Telefonování.	19 701	72,49
Psaní a odesílání zpráv přes online služby (Facebook, Messenger, WhatsApp apod.).	18 044	66,39
Sledování videí na YouTube.	17 778	65,42
Psaní a odesílání SMS/MMS zpráv.	14 735	54,22
Fotografování.	14 039	51,66
Hraní her.	13 457	49,52
Poslech hudby či mluveného slova (např. Spotify, Apple Music apod.	12 801	47,10
Vyhledávání informací (např. na Google).	10 400	38,27
Sledování oblíbených youtuberů.	9 091	33,45

Průzkum se také zaměřil na využívání mobilních telefonů ve školách se zaměřením na regulace jejich používání.

Přestávky	Vyučovací hodiny	Relativní četnost (%)
povoleno	zakázáno	53,30
zakázáno	zakázáno	41,20
povoleno	povoleno	2,48
zakázáno	povoleno	1,09
neuvedlo	neuvedlo	1,92

Nadpoloviční většina má o přestávkách povoleno využívat mobilní telefony, ale ne během vyučování. Stále však platí, že pedagog může povolit mobily během vyučování jako užitečný nástroj pro vyhledávání informací. Odborníci z výzkumu se také zaměřili na počínání žáků během přestávek. Výsledky ukázaly, že v drtivé většině, tedy 85,24 %, si děti povídají.

I když mají některé školy zakázané používání mobilních telefonů o přestávkách, část dětí ho nedodržuje např. hrají o přestávkách hry, jsou na sociálních sítích nebo chatují.

V souvislosti s regulací mobilních telefonů na školách se často diskutuje o možnosti zneužití, například k nahrávání a focení spolužáků bez svolení dotyčných. 35,71 % dětí potvrdilo, že je někdo jiný ve škole vyfotil bez jejich souhlasu, 22,5 % dětí pro změnu uvedlo, že je někdo jiný natáčel, a to také bez jejich souhlasu.

Výzkumníci také uvedli, že i děti v útlém věku jsou konzumenty různých videí/videoobsahu. Bylo vhodné zjistit, jakým typům videí respondenti dávají přednost. Otázky ohledně videí bylo rozděleno do několika kategorií: například Vtipná videa, Výzvy, Let´s play videa, Vlogy, Fashion vlogy, Food videa atd. Průzkum se zaměřil pouze na dominantní služby poskytující videa, vynechány byly například hudební klipy

	Facebook		Instagram		YouTube		TikTok		Twitch		Jinde	
	Četnost	(%)	Četnost	(%)	Četnost	(%)	Četnost	(%)	Četnost	(%)	Četnost	(%)
Vtipná videa (žertíky, pranky).	5974	21,98	10438	38,41	21123	77,72	4851	17,85	1544	5,68	862	3,17
Výzvy (challenge).	1946	7,16	4749	17,47	18210	67,01	2797	10,29	930	3,42	633	2,33
Let's play videa (hraní her)	980	3,61	1467	5,40	16641	61,23	658	2,42	4019	14,79	834	3,07
Vlogy (videodeníčky).	893	3,29	3898	14,34	15579	57,32	866	3,19	570	2,10	590	2,17
Fashion Haul videa (videa o módě).	1054	3,88	3848	14,16	9274	34,12	892	3,28	288	1,06	816	3,00
Unboxing videa (rozbalování věcí).	1012	3,72	3632	13,36	15915	58,56	932	3,43	1006	3,70	540	1,99
Food videa (videa o jídle).	2531	9,31	7000	25,76	12183	44,83	1307	4,81	674	2,48	807	2,97
Reakční videa (kritické hodnocení videí jiných youtuberů).	990	3,64	2448	9,01	16076	59,15	1053	3,87	1114	4,10	495	1,82
Pornografická / erotická videa.	574	2,11	789	2,90	1173	4,32	499	1,84	406	1,49	4391	16,16
Videa zobrazující násilí (fyzické i psychické, týrání, projevy nenávisti apod.).	918	3,38	863	3,18	2384	8,77	417	1,53	309	1,14	1468	5,40
Videa zobrazující osoby s poruchami příjmu potravy (mentální anorexie, morbidní obezita).	722	2,66	1114	4,10	3208	11,80	488	1,80	232	0,85	1004	3,69
Videa zobrazující sebepoškozování.	811	2,98	1334	4,91	2356	8,67	527	1,94	352	1,30	1139	4,19
Videa zobrazující šokující a odpudivý obsah (jatka, zabíjení zvířat).	959	3,53	1073	3,95	2344	8,62	418	1,54	252	0,93	1251	4,60
Videa zobrazující vandalismus (ničení majetku).	1086	4,00	1363	5,02	4604	16,94	504	1,85	315	1,16	919	3,38
Videa zaměřená na propagaci terorismu.	749	2,76	618	2,27	1650	6,07	377	1,39	254	0,93	1237	4,55
Videa zaměřená na vzdělávání (třeba Khanova škola).	908	3,34	1219	4,49	5990	22,04	375	1,38	257	0,95	1568	5,77
Videa zaměřená na parkour / freerunning.	1568	5,77	3483	12,82	11988	44,11	1537	5,66	540	1,99	782	2,88
N		**27177**		**27177**		**27177**		**27177**		**27177**		**27177**

Výzkum se rovněž ohlédl za nejpalčivějším tématem internetu, tedy kyberšikanou. Cílem bylo zmapovat nejčastější formy agrese, se kterými se děti v kyberprostoru setkávají. Podle statistik zažilo v roce 2018 kybernetickou agresi 41,29 % dotázaných, což představuje celkem 11 221 incidentů.

Vybrané formy agrese, se kterými se děti setkaly

Riziková forma	Absolutní četnost (n)	Relativní četnost (%)	Výzkum NIK 2014	Rozdíl
Některou z forem kybernetické agrese v posledním roce zažilo:	11 221	41,29	45,81	-4,52
Někdo ti slovně ublížil prostřednictvím internetu či mobilního telefonu (ponižoval tě, urážel, zesměšňoval nebo tě jinak slovně ztrapňoval).	7 383	27,17	34,33	-7,16
Někdo prostřednictvím internetu či mobilního telefonu šířil fotografii, která tě měla ponížit, zesměšnit nebo jinak ztrapnit.	3 330	12,25	13,70	-1,45
Někdo prostřednictvím internetu či mobilního telefonu šířil tvoji intimní fotografii.	919	3,38	-	-
Někdo prostřednictvím internetu či mobilního telefonu šířil videonahrávku, která tě měla ponížit, zesměšnit nebo jinak ztrapnit.	1 768	6,51	6,54	-0,03
Někdo prostřednictvím internetu či mobilního telefonu šířil zvukovou nahrávku, která tě měla ponížit, zesměšnit nebo jinak ztrapnit.	1 038	3,82	3,89	-0,07
Někdo ti vyhrožoval nebo tě zastrašoval pomoci služeb internetu nebo mobilního telefonu.	2 649	9,75	17,84	-8,09
Někdo tě pomocí služeb internetu nebo mobilního telefonu vydíral (pokud něco neuděláš, tak něco provede třeba tobe nebo někomu v tvém okolí apod.).	1 580	5,81	7,91	-2,1
Někdo se bez tvého svolení dostal do tvého on-line účtu (např. emailu, účtu na sociální síti apod.).	3 435	12,64	34,80	-22,16
Někdo zneužil tvůj online účet k tomu, aby tě dostal do problémů (např. tvým jménem obtěžoval tvé přátele).	1 350	4,97	11,82	-6,85
Někdo ti založil falešný profil na sociální siti.	1 870	6,88	-	-

Výsledky působí lehce pozitivnějším dojmem, jelikož podle statistik společnosti O2 z roku 2014, došlo k mírnému poklesu. Dominantní formou agrese mezi dětmi je stále verbální

útok s využitím platforem, jako je Facebook, Messenger, Instagram či SMS/MMS. Zároveň drtivá většina dětí zažila agresi déle než 1 týden (60 % incidentů).

Déletrvající útoky na dítě v online prostředí jsou výjimečné.

Platforma (socnet, služba)	Absolutní četnost (n)	Relativní četnost (%)
Facebook	6 330	56,41
Facebook Messenger	4 788	42,67
Instagram	3 551	31,65
SMS/MMS	1 281	11,42
YouTube	1 124	10,02
E-mail	1 065	9,49
WhatsApp Messenger	981	8,74
TikTok	859	7,66

Délka útoku	Absolutní četnost (n)	Relativní četnost (%)
méně než 1 týden	6 735	60,02
1-2 týdny	1 549	13,80
3-5 týdnů	641	5,71
1-3 měsíce	503	4,48
4-6 měsíců	234	2,09
7-12 měsíců	183	1,63
více než rok	759	6,76
neuvedlo	617	5,50

Předmětem výzkumu kyberšikany byl také původ, respektive kdo stál za útokem. Drtivá většina dětí potvrdila, že jednalo o jejich vrstevníky – ve 30 % případů se jednalo o spolužáky ze stejné třídy či to byli jejich kamarádi. Neznámé osoby na děti zaútočilo ve 20 % případů – projevy agrese v rámci sociálních sítí či online her, tedy v místech, kde se děti často pohybují. Ve více než polovině šlo o útok ze strany jednotlivce, konkrétně 51,65 %, zhruba pětina případů byl útok ze strany skupin. Co se týče pohlaví, útoky prováděli jak chlapci, tak děvčata.

Další otázka byla zaměřena na osobu agresora. Většina dotázaných dětí potvrdila, že se šlo o jejich vrstevníky – ve 30 % případů se jednalo o spolužáky ze stejné třídy či to byli jejich kamarádi. Neznámé osoby na děti zaútočily ve 20 % případů – projevy agrese v rámci sociálních sítí či online her, tedy v místech, kde se děti často pohybují. Většinou šlo o útok ze

strany jednotlivce (51,65 %), zhruba pětina případů byl útok ze strany skupiny. Co se týče pohlaví, útoky prováděli jak chlapci, tak děvčata.

Agresor	Absolutní četnost (n)	Relativní četnost (%)
Spolužák ze stejné třídy.	3 299	29,40
Bývalý kamarád.	1 840	16,40
Žák z jiné školy.	1 619	14,43
Spolužák z jiné třídy (ale stejné školy).	1 421	12,66
Člověk, kterého znám pouze z internetu.	1 318	11,75
Neznámý člověk.	978	8,72
Bývalý přítel / bývalá přítelkyně, se kterým / kterou jsem chodil / chodila.	682	6,08
Dospělá osoba, kterou jsem neznal (např. rodič spolužáka).	559	4,98
Dospělá osoba, kterou znám (např. příbuzný).	286	2,55
Učitel, který mě učí.	245	2,18
Učitel, který mě neučí, ale je ze stejné školy).	128	1,14

Agresor (kategorie)	Absolutní četnost (n)	Relativní četnost (%)
Chlapec (jednotlivec)	3 891	34,68
Dívka (jednotlivec)	2 411	21,49
Pohlaví neznámé (pachatele se nepodařilo identifikovat)	2 363	21,06
Smíšená skupina (chlapci i dívky)	1 262	11,25
Pouze chlapci (více než jeden chlapec)	741	6,60
Pouze dívky (více než jedna dívka)	484	4,31
Neuvedlo	69	0,61

4. Identifikace (kritéria identifikace). Popis klíčových otázek

V České republice existuje mnoho výzkumů, které se zaměřují na kyberšikanu ve školách či jiných školských zařízeních. Je zřejmé, že toto téma se stává velmi palčivým problémem na území České republiky. Není to nic překvapujícího, dnešní děti a mládež jsou čím dál tím více spojeni s informačními technologiemi. Přátelství a partnerské vztahy se běžně pěstují na síti a přes mobilní telefon.

Kyberšikanu samu o sobě nelze spolehlivě kontrolovat, protože elektronických zpráv či obrázků je v online prostředí nepřeberné množství. Proto tento negativní fenomén narůstá do mnohem větších rozměrů než klasická šikana. Dá se tento problém vyjádřit v číslech? Nejčastějším nástrojem pro výzkum jsou dotazníky, které se často využívají ve školských zařízeních, kde se kyberšikana vyskytuje. Jaké jsou tedy nejčastější otázky a odpovědi?

1. **Víte, co znamená pojem kyberšikana?**
   Tato uzavřená otázka se nejčastěji používá na začátku dotazníků a díky ní je hned jasné, zda respondenti vůbec daný pojem znají.

2. **Setkali jste se někdy s pojmem kyberšikana?**
   Pokud respondent odpoví kladně, pokračuje druhá část otázky - v jakém prostředí. Nejčastější odpověď je ve školách a jiných školských zařízeních.

3. **O jaký typ kyberšikany se jednalo?**
   Zde se otázka zaměřuje na druhy či typy kyberšikany. Jako například SEXTING, KYBER GROOMING nebo VYHROŽOVÁNÍM (zveřejnění sexuálních fotek či zpráv na internet).

4. **Jakým způsobem jste řešil/a kyberšikanu?**
   Z odpovědí je možné definovat, jaké způsoby řešení nejčastěji respondenti využívají. Ve školách a školských zařízeních řeší problematiku kyberšikany vedení školy a školní metodik prevence, v dalších případech pak Policie ČR nebo různé neziskové organizace např. Linka bezpečí.

5. **Jak se dá kyberšikaně zabránit?**
   Jednoduchá otázka, jejíž cílem je zjistit, zda se kyberšikana skutečně řeší a jak pro ní postupovat. Ve školách a školských zařízeních se kyberšikaně snaží zabránit hlavně přednáškami, různými projektovými dny či ve vyučovacích hodinách.

6. **Stal/a jste se obětí kyberšikany?**
   Tato uzavřená otázka logicky směřuje na děti a dospívající děti, ale i na dospělé, nejčastěji učitele, kteří se stali obětmi vlastních žáků.

7. **Jakým aktivitám se nejčastěji věnujete na internetu?**
   Otázka se vyskytuje téměř ve všech dotaznících. Zde mohou odpovídat jak děti, tak dospělí. Nejčastější odpovědí je převážně **prohlížení sociálních sítí** (Facebook, Instagram, Youtube).

8. **Komunikujete s neznámými lidmi online?**
   Tento dotaz ukazuje na samou problematiku pojmu kyberšikana. Nejčastější odpovědí je ve většině případů NE. Bohužel se někteří respondenti přiznali, že komunikovali či komunikují s neznámými lidmi.

9. **Máte zabezpečený počítač/mobil?**
   Z několika výzkumů vyplývá, že téměř polovina Čechů využívá v zaměstnání či ve škole osobní telefon nebo počítač pro práci. Z toho 18 % přiznalo, že jejich data nejsou nijak chráněna. Může tedy dojít nejen ke ztrátě osobních dat, ale i těch firemních. https://www.system4u.cz/temer-polovina-cechu-k-praci-vyuzi- va-osobni-telefon-nebo-pocitac--firemni-data-jsou-na-osobnich-zarizenich-ohrozena/

10. **Sdílíte osobní data, jako je například bydliště či datum narození na sociálních sítích?**
    Tato otázka se v dotaznících nevyskytuje příliš často, ale odpověď má vypovídající informaci o stavu společnosti.. V současné době, kdy se v online světě vyskytuje skrze Facebook či Instagram miliardy lidí, je těžké zůstat anonymem. Většina uživatelů zadá bez zaváhání na sociálních sítích většinu svých osobních údajů např. seznamovací portály. Typickým příkladem je seznamovací aplikace Tinder. Češi jsou však více opatrnější, když nemusí, tak neudávají žádné své osobní údaje.

5. Závěr, shrnutí

Význam internetu a sociálních sítí v dnešním světě v životě mladých i dospělých lidí neustále stoupá. Za pomoci elektrických zařízení a nejnovějších digitálních médií, se tyto platformy intenzivně a poměrně rychle využívají. Mnoha lidem, především ze sociálně ohrožených skupin, chybí schopnost plně využívat potenciál digitálního věku v každodenním životě. Právě v těchto případech mohou nahradit roli rodiny školy, sociální pracovníci a další odborníci. V České republice není tzv. digitální gramotnost pevně uchopena a není integrovaná ve vzdělávacích programech. Nicméně, v ČR existuje celá řada projektů a odborných poraden, které se zaměřují na tuto problematiku a pomáhají lidem pochopit podstatu a bezpečnost internetu a chování v něm.

6. Přílohy

a. Soubor nejčastěji kladených otázek a odpovědí v otázkách bezpečnosti a rizik spojených s používáním digitálních technologií a využívání online příležitostí

Cílová skupina – rodiče a prarodiče

Co to je systém včasné intervence?

Je propojení a spolupráce institucí zainteresovaných v oblasti péče o rizikové a ohrožené děti. V tomto systému vykonávají systematickou a kontinuální činnost s kriminálně rizikovými dětmi, jejich rodinami a komunitou orgány sociálně-právní ochrany dětí, Policie České republiky, obecní policie, soudy, státní zastupitelství, Probační a mediační služba, úřady práce, zdravotní, školské orgány a nestátní neziskové organizace. Proces této spolupráce bude formálně završen vytvořením informačního systému sociálně právní ochrany dětí, který realizuje Ministerstvo práce a sociálních věcí a Ministerstvo vnitra.

Proč po mně webové stránky chtějí souhlas s cookies. Co to je? Jaké to má následky?

Slovo „cookie“ (česky sušenka) je označení pro malý soubor, který je posílaný navštívenou webovou stránkou do prohlížeče. Data ze souboru jsou v prohlížeči dočasně uložena a s jejich pomocí jsou webové servery schopny sledovat a vyhodnocovat svoji návštěvnost. Poté, co se uživatel přihlásí, je jeho prohlížeči šifrovaně zaslán soubor cookie. Data z něj pak slouží k ověření autenticity uživatele u všech dalších požadavků na stránky. Data z cookie jsou smazána v okamžiku, kdy se uživatel odhlásí, zavře svůj prohlížeč, nebo když vyprší platnost souboru.

Jsou cookies bezpečné?

Ano. Soubor cookie nemůže serveru poskytnout žádná data z vašeho pevného disku, neprozradí mu emailovou adresu ani žádné jiné informace o uživateli prohlížeče. Soubor cookie je přenášen v rámci šifrovaného spojení, není ukládán na disk a má jen časově omezenou platnost.

Na webu mé banky je varování před phishingem. Co je to?

Slovo Phishing vzniklo spojením dvou anglických slov: Fishing (rybaření) a Phreaking (napojení na cizí telefonní linku) – v češtině je někdy překládáno jako „rhybaření“.

Phishing je označení pro podvodné e-mailové zprávy, které mají vzbudit dojem, že byly odeslány z Vám známé e-mailové adresy. Zpráva obsahuje odkaz na údajné stránky Vašeho bankovního ústavu, e-shopu, apod. a vyzývá k potvrzení osobních bankovních údajů. Phishingová zpráva může vypadat jako informace o neprovedení platby, výzva k aktualizaci bezpečnostních údajů, výzkum spokojenosti spotřebitelů apod. Cílem podvodného e-mailu je zpravidla získat Vaše osobní údaje, identifikační a autentizační údaje pro přístup k účtu, bezpečnostní kód nebo například číslo platební karty, PIN či další bezpečnostní údaje a následně je zneužit.

Jak se dostala moje e-mailová adresa do rukou útočníků? Nejde o únik dat?

Phishing je druhem spamu. Útočníci obvykle e-mailové adresy příjemců náhodně generují, nebo je kupují na černém trhu.

Co mám dělat s phishingovým e-mailem?

Na zprávu v žádném případě nereagujte, smažte ji a na odkaz neklikejte. V případě, že se tak stalo, hrozí, že poskytnete citlivé údaje útočníkům k dalšímu zneužití. Pokud jste na zprávu zareagovali, doporučujeme ihned kontaktovat klientské centrum Vašeho bankovního ústavu nebo zákaznické centrum e-shopu.

Na sociální síti mě kontaktují neznámí lidé s divnými nabídkami? Mohu zprávy od nich nějak zablokovat?

Například v Nastavení služby Lidé.cz naleznete volbu Ignorace a obdobné možnosti nabízí i jiné služby. Podezřelé nabídky, spam nebo jiné závadné zprávy je dobré zkopírovat nebo udělat screenshot a zaslat administrátorům dané služby. Nezapomeňte vždy detailně popsat Váš problém.

Na sociální síti potkávám velmi podezřelého, potenciálně nebezpečného jedince. Kde jeho nevhodné chování mohu nahlásit?

Podezřelé nabídky, spam nebo jiné závadné zprávy je dobré zkopírovat nebo udělat screenshot a zaslat administrátorům dané služby. V závažnějších případech pak kontaktujte policii.

Mám zablokovanou IP adresu a nemohu používat službu Lidé.cz. Co mohu dělat?

V případě blokace se můžete obrátit na technickou podporu služby, kterou naleznete na adrese: http://napoveda.seznam.cz

Jak se bránit v případě zneužití údajů?

Kontaktujte technickou podporu služby s žádostí o smazání údajů. V závažných případech neváhejte kontaktovat Policii ČR.

Cílová skupina – děti

Dopisuji si na chatu s někým a on teď chce, abych mu poslala svoje intimní fotky. Vyhrožuje, že když to neudělám, zneužije moje dřívější odpovědi k vymyšleným pomluvám a znemožní mě přede všemi. Co mám dělat?

Ukončit komunikaci**,** blokovat útočníka – zamezit útočníkovi v přístupu k vašemu účtu nebo telefonnímu číslu, je-li to možné i k nástroji či službě, pomocí které své útoky realizuje

oznámit útok – na kterémkoliv oddělení Policie ČR (viz www.policie.cz) http://aplikace.policie.cz/hotline/

pokud nechcete kontaktovat Policii ČR vyhledejte: www.napisnam.cz – online poradna projektu E-Bezpečí, www.horkalinka.cz – Saferinternet.cz

Někdo použil bez mého svolení na sociální síti mou citlivou fotografii a nechce jí smazat. Co mohu dělat?

Kontaktujte administrátory dané služby prostřednictvím jejich technické podpory nebo odkazem na nahlášení závadného obsahu. Nezapomeňte vždy detailně popsat váš problém.

Někdo na sociální síti vystupuje pod mou vlastní identitou. Jak tomu mohu zabránit?

Kontaktujte administrátory dané služby prostřednictvím jejich technické podpory nebo odkazem na nahlášení závadného obsahu. Nezapomeňte vždy detailně popsat váš problém. Pokud to služba nabízí, doporučujeme se na ní certifikovat.

Někdo mi na sociální sítí smazal profil a vůbec nemám ponětí proč. Jak mohu dál postupovat?

Smazaný profil většinou nelze obnovit. Buď bylo porušeno smluvní ujednání na službě a profil byl smazán správcem služby nebo bylo zneužito vaše heslo. Pro detailní informace se obraťte na technickou podporu dané služby.

b. Metodika pro pracovníky organizací (školy, volnočasové instituce, knihovny, galerie, muzea aj.) poskytující poradenství rodičům, prarodičům a dětem v otázkách bezpečnosti a rizik spojených s používáním digitálních technologií a online příležitostí

1) Počítačová gramotnost

- **Bezpečné heslo** - je pro uživatele informačních a komunikačních technologií prvotní a základní ochranou proti případným útočníkům, ochraňuje účty na internetu, v počítačích a mobilních aplikacích před krádeží informací a peněz. Heslo je řetězec nesnadno zjistitelných a uhodnutelných znaků, který se užívá jako identifikační a ověřovací prvek. Společně s uživatelským jménem často tvoří základní uživatelovu ochranu užívaných zařízení (telefon, počítač apod.) nebo k různým aplikacím, webovým službám, přístupu k počítačovým systémům, sítím apod.
  https://www.nebojteseinternetu.cz/page/3448/bezpecna-hesla/
- **Jak bezpečně na Wi-Fi** - Wi-Fi se stala podstatnou součástí našeho digitálního života. Připojení pomocí bezdrátové technologie najdete doma, ve školách, ve firmách i na veřejných místech. I mimo dosah své domácí sítě se můžeme připojit přes veřejnou Wi-Fi v kavárně, obchodu nebo na úřadu. V kapse si nosíme celé gigabyty mobilních dat. Technologie dávají našim přístrojům a nám přístup k jakýmkoli informacím a materiálům, ať jsme kdekoli. Funguje to ale i naopak. Bezdrátová komunikace v našich sítích však přináší i některá rizika.
- **Zabezpečení sociálních sítí** - Nebezpečí sociálních sítí vězí v tom, že dobrovolně poskytujeme citlivé a osobní údaje či fotky a jsou pro každého přístupné. Soukromí by si měli chránit jak dospělí, tak děti, kterým by rodiče měli vysvětlit, jak si dávat v on-line světe pozor. Cizí člověk na sociální stí nebo v diskuzi v online hře je totiž potenciálně stejně nebezpečný jako cizí člověk na ulici.
  https://www.nebojteseinternetu.cz/page/3396/socialni-site/
- **Jak chránit svá data, počítač a mobil -** Antivirové programy, bezpečná hesla a dvoufázové ověřování při přihlašování jsou základem. Ovšem ani nejlepší antivirový program vám nepomůže ochránit cenná data, pokud své přístroje necháváte bez dozoru.

https://www.o2chytraskola.cz/temata#pocitacova-gramotnost

https://www.o2chytraskola.cz/clanek/4/jak-bezpecne-na-wi-fi/2818

https://www.o2chytraskola.cz/clanek/21/zabezpeceni-socialnich-siti/2419

https://www.o2chytraskola.cz/clanek/5/jak-chranit-sva-data-pocitac-a-mobil/

https://www.jaknainternet.cz/

https://www.internetembezpecne.cz/internetem-bezpecne/navody/heslo

2) Digitální gramotnost

Je základním předpokladem bezpečného a efektivního užívání moderních informačních technologií s přístupem na internet. Proto je dnes digitální gramotnost tak často diskutované téma, které by na školách nemělo být zanedbáváno. Pro digitálně gramotné uživatele internetu je zásadní nejen znát možná nebezpečí, ale zejména jim umět předcházet a tedy využívat různé strategie posuzování vlastního chování a obsahu internetu. Tyto strategie bychom mohli pojmenovat informační gramotností ve virtuálním prostředí.

https://digifolio.rvp.cz/view/view.php?id=13123&rate=5

3) Mediální gramotnost

Představuje zjednodušeně vzato lidskou dovednost přístupu k médiím, chápání a kritického vyhodnocování jejich obsahu a případně též schopnost vytvářet vlastní sdělení.

3.1. **Fake news** v online prostředí - termínem Fake news označujeme lživé a nepravdivé zprávy (hoaxy, dezinformace) nebo také samotnou žurnalistiku, která je založena právě na úmyslném šíření těchto nepravdivých informací prostřednictvím masmédií, v posledních letech především médií sociálních (sociálních sítí). Problémem je, že se pro stále větší množství uživatelů stávají primárním zdrojem informací právě sociální sítě, které však v současnosti neoddělují pravdivé informace od informací nepravdivých - na rozdíl od médií tzv. seriózních, která si informace ověřují z více zdrojů, které pak uvádějí u jednotlivých zpráv. To znamená, že by sami uživatele sociálních sítí měli umět filtrovat obsah a oddělovat fakta od nepravdivých informací. V praxi se to však velmi často neděje. Fake news mohou být zcela vymyšlené (od základu nepravdivé), mohou však být také založeny na pravdivém základu, který je doplněn o další nepravdivé informace, které zesilují jeho schopnost penetrovat mediální prostor a rychle se v online prostředí šířit. Jedinou skutečně funkční cestou, jak se před vlivem tzv. Fake news ubránit, představuje mediální vzdělávání, které je propojeno s tzv. funkční gramotností a kritickým myšlením.

3.2. Název **hoax** pochází ze stejného anglického slova, což v překladu znamená falešná zpráva, mystifikace, novinářská kachna, poplašná zpráva, výmysl, kanadský žert. V elektronické komunikaci se význam tohoto slova nikterak nemění. Jedná se o poplašnou zprávu, která např. varuje před neexistujícím nebezpečím, před počítačovým virem, prosí o pomoc, anebo chce pouze pobavit. Často je ve zprávě kladen důraz na další přeposlání zprávy přátelům – řetězová zpráva. Většinou právě podle této žádosti o přeposlání lze hoax identifikovat.

Účel hoaxu:

- vyvolat strach,
- šířit falešnou radu,
- manipulovat s názory lidí,
- poškodit instituci, značku, firmu, výrobek,
- ohromit, zaujmout, přilákat pozornost,
- vystřelit si z důvěřivých uživatelů.

ZvolSi.info

www.hoax.cz

https://www.o2chytraskola.cz/clanek/13/fake-news-a-hoaxy/3091

4) Online komunikace:

Jednou z velkých výhod internetu je usnadnění a zrychlení komunikace. K rychlé komunikaci na internetu slouží mnoho nástrojů např. e-mail, instant messaging, chaty nebo internetové volání.

- Nejpoužívanější formou je e-mail, který slouží k odesílání, doručování a přijímání elektronických zpráv. Stejně jako u jiných forem je jeho výhodou rychlost a možnost posílání příloh.
- Instant messaging umožňuje uživatelům sledovat, kteří jejich přátelé jsou právě připojeni, posílat zprávy, chatovat nebo posílat soubory. Výhodou je rychlost a okamžité odeslání zprávy nebo obsahu příjemci. Mezi nejznámější instant messaging patří ICQ, AIM, Jabber, Windows Live Messenger nebo Skype.
- Chat nabízí uživatelům možnost komunikovat s více lidmi najednou. Jeho předností je možnost interakce s uživateli. Většina provozovaných chatů probíhá v anonymitě, tzn. lidé na nich vystupují pod přezdívkami, nikoli pod pravými jmény.
- Skype je program, který umožňuje provozovat internetovou telefonii. Program umožňuje telefonovat mezi svými uživateli zdarma nebo pomocí jiných služeb za poplatek, např. na pevné linky. Další výhodou je zasílání zpráv a souborů mezi uživateli sítě.
- Sociální sítě jsou na internetu místem k setkávání lidí, sdílení zážitků, obsahu. V rámci pojmů virtuálního světa je můžeme definovat jako online službu, která na základě registrace umožní vytvořit profil uživatele, pod kterým lze tuto službu využívat zejména ke komunikaci, sdílení informací, fotografií, videa atd. s dalšími registrovanými uživateli.

5) Rizika online komunikace

Díky možnostem, které internet nabízí, se můžete velice snadno seznámit, podělit se o své zážitky nebo sdílet obsah. Internet boří hranice i čas a umožňuje lidem po celém světě komunikovat v reálném čase. S nárůstem moderních technologií nebo aplikací to lze jednoduše přes e-mail, instant messaging, sociální sítě, chaty nebo třeba volání přes internet. S možností komunikace přes internet ale vznikají i určitá rizika. Největším rizikem je ztráta soukromí. To, co na internetu zveřejňujeme nebo posíláme, již nelze ve většině případů vrátit zpět.

www.o2chytraskola.cz

https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/

6) Kyberšikana

Kyberšikana, též kybernetická šikana, počítačová šikana či cyberbullying je kolektivní označení forem šikany prostřednictvím elektronických médií, jako je internet a mobilní telefony, které slouží k agresivnímu a záměrnému poškození uživatele těchto médií. Stejně jako tradiční šikana zahrnuje i kyberšikana opakované chování a nepoměr sil mezi agresorem a obětí. Aktéry kyberšikany jsou (obdobně jako u klasické šikany): Agresor – Oběť – Přihlížející (publikum).

- Znaky kyberšikany: Anonymita – útočník zpravidla vystupuje anonymně, vystupuje pod falešnými přezdívkami (nicky), vytváří jednoúčelové e-mailové schránky nebo falešné profily na sociálních sítích, a díky tomuto pocitu anonymity je posílena jeho odvaha v použití agresivnější formy útoku.

- Profil útočníka – ve virtuálním světě neplatí pravidla klasické šikany – nezáleží zde na věku, pohlaví, fyzické síle útočníka, sociálním postavení apod. Převládají převážně znalosti a dovednosti v užívání informačních a komunikačních technologií.
- Místo a čas útoku nelze předpokládat – zatímco u klasické šikany lze předpokládat, kdy a kde k útoku dojde (o přestávce ve třídě, po vyučování před školou, v odpoledních hodinách na hřišti apod.), u kyberšikany útok může přijít kdykoliv a kdekoliv. Třeba o půlnoci a prostřednictvím různých kanálů: SMS, emailem, videem na videoportálu (např. youtube.com), příspěvkem na sociální síti apod; šíření kyberšikany pomáhá útočníkovi „publikum".
- Zejména možnost sdílení nebo následné přeposílání škodlivých příspěvků zvyšuje intenzitu vedeného útoku. Útočníkovi tedy postačí příspěvek publikovat pouze jednou, o jeho opakování a šíření se často postará ono „publikum". Jednání tohoto obecenstva nepřímo ale velice důrazně zvyšuje negativní psychický dopad na oběť.
- Není snadné rozeznat dopad kyberšikany na oběť – vzhledem k tomu, že dopady kyberšikany jsou spíše v rovině psychické, je nesnadné je na oběti rozeznat nebo poznat oběť samotnou. Na rozdíl od klasické šikany u kyberšikany je o mnoho složitější vysledovat varovné signály – modřiny, potrhané a špinavé oblečení apod. Oběť se často uzavírá do sebe a přestává komunikovat s okolím, ať už ze strachu, že útočník zintenzivní své útoky, ze studu nebo strachu z nepochopení problému rodiči nebo učiteli.

Prostředky kyberšikany:

- textové zprávy prostřednictvím mobilních telefonů,
- fotografie a videoklipy zachycené přes kamery mobilních telefonů a následné zveřejněné na internetu,
- telefonní hovory,
- e-mailové zprávy,
- chatové místnosti,
- tzv. instant messaging (ICQ, Skype aj.),
- internetové stránky, blogy,
- sociální sítě,
- on-line hraní her.

Nejčastější projevy kyberšikany:

- verbální ponižování, urážení, zesměšňování,
- prolomení elektronického (např. e-mailového účtu,
- opakované obtěžování (prozvánění, spamování apod.),
- vyhrožování nebo zastrašování,
- publikování ponižující fotografie,
- ostrakizace, vyloučení z virtuální komunity,
- happy slapping (v překladu „zábavné fackování"),
- zveřejňování cizích tajemství s cílem poškodit oběť.

https://www.o2chytraskola.cz/clanek/7/kyberneticka-sikana/2799

https://www.policie.cz/clanek/prevence-kybersikana.aspx

https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/

Metodické doporučení k primární prevenci rizikového chování u dětí a mládeže (Dokument MŠMT č. j.: 21291/2010-28) – Příloha 7 Kyberšikana

Jako **flaming** se označuje agresivní chování projevující se urážkami, nadávkami a vyhrožováním. Jedná se o jev v dnešní době velmi populární a běžný uživatel se s tímto chování může setkat u komentářů fotografií nebo přímo při konverzaci. Flaming nemá za cíl nic jiného než rozčílit, naštvat, ponížit oběť a to zcela beztrestně a většinou i anonymně. Podle výzkumu je flaming jako slovní napadení ve virtuálním prostředí čtyřikrát častější než v reálném životě. A právě anonymita je to, co ve většině případů hraje klíčovou roli v kyberšikaně a způsobuje tenkou hranici mezi běžným uživatelem a agresorem.

https://medium.com/edtech-kisk/vybran%C3%A9-typy-kyber%C5%A1ikany-a-jej%C3%AD--preventivn%C3%AD-opat%C5%99en%C3%AD-bbd1254eb227

Kybergrooming lze vysvětlit jako psychickou manipulaci dítěte dospělým prostřednictvím moderních komunikačních technologií s cílem získat důvěru oběti, vylákat ji na osobní schůzku a zpravidla sexuálně zneužít. Nejčastěji se vyskytuje v rámci instant messengerů (Facebook Messenger, Skype), sociálních sítí (Facebook, Twitter, Badoo), internetových seznamek (libimseti.cz) a různých blogovacích stránek. Obětí kybergroomingu se může stát prakticky kdokoliv, zpravidla se ale jedná o dívky ve věku 11-17 let, často užívající informační a komunikační technologie, trpící nedostatkem sebedůvěry, pocitem osamění. Jsou otevřené manipulaci a neznalé rizik internetové komunikace. Kybergroomer je zpravidla sexuální útočník využívající informační a komunikační technologie k prosazení svého cíle. Často se vydává za jinou osobu, než ve skutečnosti je, dle vybrané oběti. Pokud se snaží spřátelit se s 12 letou dívkou, vydává se za 14 letého chlapce. Významnou vlastností kybergroomera (není však pravidlem) je trpělivost – vydrží si s obětí psát i několik měsíců, jen aby pevně získal její důvěru.

https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/ kybergrooming/

https://www.o2chytraskola.cz/clanek/25/kybergrooming/2096

https://www.jaknainternet.cz/page/3664/kybergooming-aneb-pretvarovani-na-internetu/

Kyberstalking – který je od 1. 1. 2010 klasifikován jako trestný čin, lze jednoduše nazvat nebezpečným pronásledováním. Útočník využívá informační a komunikační technologie k dlouhodobému, opakovanému a stupňovanému kontaktování – pronásledování své oběti, ve které chce úmyslně vyvolat pocit strachu o své soukromí, zdraví nebo život.

Některé formy kyberstalkingu

- zasílání zpráv SMS
- telefonáty a prozvánění
- zasílání zpráv prostřednictvím messengerů a e-mailů
- opakované komentování příspěvků oběti na sociálních sítích
- vkládání příspěvků na profily sociálních sítí oběti
- krádež identity oběti – následné vystupování jejím jménem
- kontaktování oběti pod falešnou identitou (několika falešnými identitami)
- monitorování počítače oběti speciálními programy (keyloggery apod.)
- zveřejňování informací ze života oběti, obtěžující kontaktování přátel oběti aj.

Některé motivy kyberstalkera:

- obtěžovat, vyhrožovat a vydírat oběť,
- demonstrovat svou sílu,
- poškodit oběť před společností,
- opětovné navázání vztahu po odmítnutí aj.

https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyber-stalking

https://www.o2chytraskola.cz/clanek/26/kyberstalking/

Termínem **sexting** se označuje elektronické rozesílání textových zpráv, fotografií či videí se sexuálním obsahem. Často se také stává prostředkem pro vydírání dětí v rámci tzv. kybergroomigu. Sexting ve velkém rozsahu podporuje šíření pornografie mladistvých a dětí. Ve všech státech světa je toto počínání zakázané. Jedinou a účinnou obranou proti zveřejnění sextingového obsahu je takový nepořizovat a neposílat!

https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/sexting/

https://www.o2chytraskola.cz/clanek/11/sexting/

Krádež identity (někdy označováno jako Identity theft) lze v rámci počítačové hantýrky označit jako zmocnění se virtuální identity oběti útočníkem. V praxi to znamená krádež přístupových údajů k emailové schránce, uživatelskému účtu na sociálních sítích, v počítačové hře apod. a následné vydávání se útočníka za oběť. Pokud se útočníkovi nepodařilo získat přihlašovací údaje, praxe, zejména na sociálních sítích, může vypadat i tak, že jsou útočníkem z profilu oběti postahována veškerá dostupná data (profilový obrázek, jméno, uvedené informace k osobě apod.) a tyto využije k založení duplicitního profilu oběti. Tímto falešným profilem poté oslovuje přátele oběti. V pojetí kyberšikany útočník odcizenou identitu využívá zpravidla k:

- poškození oběti (přidávání nevhodných statusů, komentářů a nevhodná – účelová komunikace s přáteli oběti),
- odcizení citlivých dat oběti (např. za účelem následného vydírání),
- získání citlivých dat přítele oběti (takové, které by přítel oběti sdělil pouze jí),
- páchání trestné činnosti jménem oběti.

https://www.policie.cz/clanek/ztrata-identity.aspx

https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyber-sikana/kradez-identity

7) Kyberkriminalita

Termínem počítačová kriminalita (též kybernetická kriminalita, internetová kriminalita, kyberkriminalita či kybernalita) se označují trestné činy zaměřené proti počítačům nebo trestné činy páchané pomocí počítače. Jde o nelegální, nemorální a neoprávněné konání, které zahrnuje zneužití údajů získaných prostřednictvím výpočetní techniky nebo jejich změnu. Nejčastější projevy kyberkriminality jsou:

7.1. Podvodné jednání (podvodné inzeráty, falešné e-shopy, phishing, sociální inženýrství, porušování autorského práva apod.)

- **Internetové bankovnictví** je jednou z možností přímého bankovnictví, kdy jste s bankou ve styku elektronicky prostřednictvím internetu. Umožňuje ovládat bankovní účet pohodlně z domova a běžné finanční operace realizovat v několika vteřinách přes Internet. Internet ale se svými takřka neomezenými možnostmi představuje i určitá rizika.

  https://www.jaknainternet.cz/page/1186/internetove-bankovnictvi/

- **Spam (spamming)** neboli zasílání nevyžádané elektronické pošty - jedná se o necílené hromadné rozesílání e-mailů s převážně reklamním sdělením.

  https://www.internetembezpecne.cz/internetem-bezpecne/podvodne-praktiky/spam/

- **Sociální inženýrství** - způsob manipulace vybrané osoby nebo skupiny osob za účelem získání informace nebo nenápadného donucení k určitému jednání (akci), která využívá lidské naivity, neobezřetnosti a hlouposti. Jeho smysl spočívá v uvedení oběti do situace, o které se domnívá, že je jiná, než ve skutečnosti je. Jinými slovy: není třeba uživateli prolamovat heslo speciálními programy, když jej útočník může uvést do situace, kdy je sám dobrovolně sdělí.

  https://www.internetembezpecne.cz/internetem-bezpecne/podvodne-praktiky/socialni-inzenyrstvi/

- **Phishing** je podvodná technika využívající informační a komunikační technologie k získávání citlivých údajů. Zpravidla je v prvotní fázi celého podvodu použito sociální inženýrství. Princip spočívá ve velmi věrohodném napodobení žádosti (např. z banky nebo obdobné instituce), upozornění od provozovatele emailové schránky nebo sociální sítě tak, aby uživatel byl „nucen“ zadat své přihlašovací údaje. Tyto zprávy a žádosti jsou šířeny převážně emailem. Ten rovněž obsahuje odkaz, na nějž je nutné kliknout k následnému přihlášení. Po odkliknutí odkazu se však uživatel neocitá na webových stránkách instituce, která je v emailu uváděna, ale na podvržených webových stránkách útočníka.

  Zadáním přihlašovacích údajů do formuláře na takto podvržených webových stránkách je uživatel „předává“ útočníkovi k dispozici a ten je poté využije ke svému prospěchu, ať se jedná o přihlašovací údaje k internetovému bankovnictví, emailové schránce nebo profilu na sociální síti.

  https://www.internetembezpecne.cz/internetem-bezpecne/podvodne-praktiky/phishing/

- **Podvodné-shopy** – nakupování na Internetu má několik nesporných výhod. Nemusíte nikam chodit, máte velký výběr, ceny většinou bývají lepší než v kamenných obchodech a také vám zboží dorazí až ke dveřím. Nakupování přes Internet má však i svá rizika a to jsou podvodné e-shopy. Tyto e-shopy se navíc často snaží názvy či vzhledem napodobovat ty už existující známé. Podezřelé bývají obzvlášť výrazně levnější e-shopy, které umožňují pouze platbu předem. Proto je také vhodné vyhledat si obchod na některém ze serverů, které se zabývají jejich recenzemi a hodnocením. Z těchto informací si lze často udělat představu o kvalitě a fungování.

  https://www.o2chytraskola.cz/clanek/8/nakupovani-online

  https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/online-nakupy/

  https://bezpecne-online.saferinternet.cz/pro-rodice-a-ucitele/nakupovani-na-internetu

  https://www.nebojteseinternetu.cz/page/3381/on-line-nakupovani/

https://www.jaknainternet.cz/page/1224/placeni-na-internetu/

- **Hacking** - neoprávněný přístup k počítačovému systému a nosiči informací dle ust. § 230 trestního zákoníku je trestným činem, který je využitelný pro většinu jednání označovaného jako tzv. hacking, narušování dat, narušování systému a v neposlední řadě i zneužívání zařízení. Nejtypičtějším příkladem, který bývá prošetřován, je jednání pachatele, který překoná zabezpečení počítačového systému a získá přístup k údajům oběti, s nimiž může dál libovolně nakládat. Součástí těchto jednání bývá mimo jiné šíření škodlivých kódů, implementace tzv. backdoorů do volně přístupných software atp. Stále častější formou je napadení emailových účtů, účtů na sociálních sítích nebo účtů internetového bankovnictví k získávání citlivých informací s možností jejich poškození či zničení nebo získání finančního prospěchu.

  https://www.policie.cz/clanek/prevence-kybersikana.aspx

- **Digitální stopa** - virtuální prostředí není anonymním prostředím. Každý uživatel zanechává v internetu určité informace a to ať jen surfuje, vyhledává skrze Google, prohlíží zeď Facebooku, anebo nakupuje. Jedná se o různorodé záznamy o činnosti uživatele ve virtuálním prostředí a soubor těchto informací nazýváme digitální stopa. Digitální stopu uživatel vytváří veškerou svou činností ve virtuálním prostředí a tyto data jsou na internetu cenným artiklem, za který jsou společnosti schopny platit nemalé peníze. Hovoří-li se o rizicích digitálních stop, v zásadě se jedná o ztrátu soukromí a možné zneužití digitální stopy. Kybernetičtí útočníci dokáží digitální stopu zneužít různorodým způsobem, ať už se jedná o krádež osobních údajů (příjmení, datum narození, rodné číslo, bydliště, čísla kreditních karet apod.), krádež hesel, mailových účtů, profilů na sociálních sítích, příp. zneužití této digitální identity ke spáchání protiprávního jednání (podvody, vydírání následným phishingovým útokům apod.). Informace z digitální stopy jsou také často zneužívány ke kyberšikaně.

  Komplexní smazání digitální stopy je v dnešní době prakticky nemožné. Lze ji ale dílčími kroky minimalizovat odstraněním závadového příspěvku, příp. odstraněním profilu uživatele ze sociální sítě.

  https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/

  https://www.jaknainternet.cz/page/3651/digitalni-stopa/

8) Netolismus

Termínem netolismus označujeme závislost (závislostní chování, či závislost na procesu) na tzv. virtuálních drogách. Mezi ně patří zejména počítačové hry, sociální sítě, internetové služby, různé formy chatu, mobilní telefony, televize.

Psychologická a sociální rizika netolismu se projevují významným zasažením do organizace času, nepravidelností v jídle, nebo nedostatkem spánku. Zhoršují se mezilidské vztahy v rodině, ve škole, nebo v zaměstnání. Zvyšuje se riziko závislostního chování nejen k počítači, ale i k alkoholu a dalším drogám. Zatěžování nervového systému vede

k poruchám paměti a komunikačních schopností. Problematickým se může stát odtržení od reality a rizika spojená s netolismem rostou zejména u těch, kteří mají problémy v reálném světě a ty kompenzují ve světě virtuálním.

Příznaky netolismu:

- méně vykonané práce,
- pocit prázdnoty, když člověk není u počítače,

- ztráta kontroly nad časem stráveným u počítače,
- brzké vstávání k počítači, nebo ponocování u počítače,
- rostoucí nervozita a neklid, když člověk delší dobu nemůže hrát,
- přemýšlení o počítači, když ho člověk zrovna nepoužívá,
- zkreslování, zatajování informací o své závislosti,
- hraní kvůli úniku od osobních problémů,
- narušené vztahy s rodinou,
- opuštění dřívějších zájmů a přátel,
- zanedbávání učení a zhoršující se školní výsledky.

www.poradenskecentrum.cz/pocitacovazavislost.php

http://poradna.adiktologie.cz/article/zavislost-na-internetu/

http://www.msmt.cz/vzdelavani/socialni-programy/metodicke-dokumenty-doporuceni-a-pokyny

Metodické doporučení k primární prevenci rizikového chování u dětí a mládeže (Dokument MŠMT č. j.: 21291/2010-28) – Příloha 15 - Netolismus

9) Kybernemoci

Nadměrné používání informačních a komunikačních technologií má na zdraví člověka velmi často negativní dopad. Ten se projevuje např. nárůstem počtu obézních dětí, zvýšením počtu očních onemocnění, rozvojem cukrovky, onemocnění srdce apod. S nadměrným používáním informačních a komunikačních technologií se však pojí také celá řada onemocnění, se kterými jsme se v minulosti běžně nesetkávali. Ta se označují jako tzv. kybernemoci, které se týkají jak fyzického, tak i duševního zdraví člověka a setkává se s nimi téměř každý aktivní uživatel digitálních technologií, např. esemeskový krk a tabletové rameno, syndrom falešného zvonění, myšitida apod.

https://www.o2chytraskola.cz/clanek/12/zdravi-v-kyberprostoru/2129

Doporučené internetové odkazy

Metodické doporučení k primární prevenci rizikového chování u dětí a mládeže (Dokument MŠMT č.j.: 21291/2010-28)

Metodické doporučení Ministerstva školství, mládeže a tělovýchovy k primární prevenci rizikového chování u dětí, žáků a studentů (dále jen „žák“) ve školách a školských zařízeních vymezuje aktuální terminologii, která je v souladu s terminologií v zemích EU a začlenění prevence do školního vzdělávacího programu a školního řádu, popisuje jednotlivé instituce v systému prevence a úlohu pedagogického pracovníka, definuje školní preventivní program, doporučuje postupy škol a školských zařízení při výskytu rizikových forem chování dětí a mládeže.

Materiál a jednotlivé přílohy naleznete zde:

Příloha 7 - Kyberšikana

Příloha 9 - Extremismus, rasismus, xenoffobie, antisemitismus

Příloha 11 - Záškoláctví

Příloha 14 - Krizové situace spojene s násilím

Příloha 15 - Netolismus

Příloha 18 - Rizikové sexuílní chování

Metodický portál RVP.CZ https://rvp.cz/informace/ vznikl jako hlavní metodická podpora pedagogů a k podpoře zavedení rámcových vzdělávacích programů ve školách. Jeho smyslem bylo vytvořit prostředí, ve kterém se budou moci učitelé navzájem inspirovat a informovat o svých zkušenostech.

O2 Chytrá škola www.o2chytraskola.cz je portál o internetové bezpečnosti a gramotnosti pro děti, rodiče a pedagogy. Informace, články, videa a výzkumy zdarma ke stažení.

Projekt studentů Masarykovy univerzity https://zvolsi.info/ zaměřený na vzdělávání v oblasti mediální gramotnosti, klade si za cíl zvýšit povědomí uživatelů o dezinformacích, fake news, hoax apod.

Server Hoax.cz www.hoax.cz – cílem serveru je informovat uživatele internetu o poplašných, nebezpečných a zbytečných řetězových zprávách, tzv. hoaxů.

Projekt Internetem Bezpečně https://www.internetembezpecne.cz/ si formou různorodých vzdělávacích aktivit klade za cíl zvýšit povědomí uživatelů o rizicích v internetovém prostředí.

Bezpečně on-line, projekt národního centra bezpečnějšího internetu https://bezpecne-on-line.saferinternet.cz/, který usiluje o zvyšování povědomí o bezpečnějším užívání internetu.

Linka bezpečí www.linkabezpeci.cz – poradenská linka zaměřená na prevenci rizikového chování apod.

Portál Policie ČR www.policie.cz/web-prevence.aspx informuje o svých akcích a projektech v rámci prevence, kyberkriminality, extrémismu, terorismu apod.

E-Bezpečí http://www.e-bezpeci.cz/ projekt zaměřený na prevenci rizikového chování na Internetu.

Poradna E-Bezpečí www.napisnam.cz poradenská linka zaměřena na prevenci rizikového chování na Internetu.

Projekt Seznam se bezpečně www.seznamsebezpecne.cz zaměřený na prevenci rizikového chování na internetu. Na stránkách je zřízen formulář pro dotazy týkající se nejrůznějších problémů spojených s on-line prostředím.

Projekt Nebuď oběť! www.nebudobet.cz zaměřený na rizika internetu a komunikačních technologií.

Projekt E – Nebezpečí pro učitele www.e-nebezpeci.cz je zaměřen na vzdělávací aktivity pro učitele všech typů škol, kteří potřebují získat nové znalosti a dovednosti v oblasti rizikového chování spojeného s využíváním informačních a komunikačních technologií, zejména internetu a mobilních telefonů.

Projekt Buď safe online www.budsafeonline.cz je pod záštitou MŠMT, který se zaměřuje na vzdělávání a prevenci v oblasti bezpečnosti na internetu u dětí na základních školách. Volí formu interaktivní, živé besedy, workshopy, kde dětem na konkrétních příkladech z praxe názorně ukazují, jak předcházet rizikům spojeným s používáním internetu a moderních

technologií. To pak kombinují s prezentací na internetu v podobě webových stránek a videí zaměřených na jednotlivé hrozby.

Za projektem stojí technologická společnost Avast – globální lídr v oblasti digitálního zabezpečení a ochrany soukromí. Se svojí sítí detekce hrozeb je jednou z nejpokročilejších na světě a díky technologiím strojového učení a umělé inteligence dokáže okamžitě zjišťovat a zastavovat útočící hrozby.

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) https://www.nukib.cz/cs/vzdelavani/ se v rámci vzdělávání zaměřuje na dovednosti bezpečného a etického využívání digitálních technologií a internetu. Cílovou skupinou pro vzdělávání jsou primárně úředníci a zaměstnanci veřejné správy, do sekundární skupiny patří žáci MŠ, ZŠ, SŠ a veřejnost včetně rodičů a seniorů.

Rozcestníky NUKIB:

- pro školy (MŠ, ZŠ, SŠ, školní preventisty) https://www.nukib.cz/cs/vzdelavani/skoly/
- pro veřejnost (rodiče, senioři) https://www.nukib.cz/cs/vzdelavani/verejnost/
- pro státní správu (zaměstnanci státní správy, správci sítě, preventisté) https://www.nukib.cz/cs/vzdelavani/statni-sprava/
- Kontaktní výuka v oblasti kybernetické bezpečnosti směrem k žákům, pedagogům i rodičům https://www.nukib.cz/cs/vzdelavani/kontaktni-vzdelavani/
- Elearningové kurzy kybernetické bezpečnosti https://www.institutpraha.cz/kurzy/kyberneticka-bezpecnost/

Jeden svět na školách https://www.jsns.cz/projekty/medialni-vzdelavani podporuje kritické myšlení a mediální gramotnost žáků a studentů ZŠ a SŠ.

Projekt **Jak na internet** www.jaknainternet.cz je jedním z projektů sdružení CZ.NIC, správce národní domény CZ. Cílem tohoto projektu je přiblížit internet a jeho možnosti co nejširší skupině občanů České republiky.

Projekt **Nenech to být** www.nntb.cz je založený studenty pod společností FaceUp Technology, který zaštítilo MŠMT. Webová platforma a mobilní aplikace bojující proti šikaně a vylučování z kolektivu na školách po světě, umožňuje rychlou a anonymní komunikaci mezi studenty a učiteli ohledně problémů ve školním prostředí. Mimo jiné se Nenech to být podílí na osvětě a spolupracuje s organizacemi a influencery na preventivních aktivitách proti šikaně. NNTB funguje na principu on-line schránky důvěry, pomocí které mohou děti anonymně upozornit na problematické vztahy v kolektivu. Upozornění poté putuje do rukou metodika prevence, výchovného poradce či školního psychologa v závislosti na tom, koho škola při registraci určila. Následně může škola žákovi podle informací z upozornění pomoci.

Dětské krizové centrum www.ditekrize.cz se zabývá krizovou pomocí, ochranou dětí, diagnostikou a terapií syndromu týraného, zneužívaného a zanedbávaného dítěte, poskytuje odbornou pomoc dětem a jejich rodinám.

c. Návrh mezigeneračního vzdělávacího programu pro oblast bezpečnosti a rizik spojených s používáním digitálních technologií a využíváním online příležitostí:

Bezpečně v kyberprostoru – principy bezpečného pohybu a komunikace v kyberprostoru

Obsah:

Základním předpokladem bezpečného a efektivního užívání moderních informačních technologií s přístupem na internet, je být dostatečně digitálně gramotným. Kurz je zaměřen na problematiku bezpečného využívání online zdrojů a přináší ucelený pohled na tuto oblast. Pro digitálně gramotné uživatele je zásadní nejen znát možná nebezpečí, ale zejména jim umět předcházet a tedy využívat různé strategie posuzování vlastního chování a obsahu internetu. Účastníci se podrobněji seznámí s různými typy rizikového chování na internetu, jako je zveřejňování osobních údajů, kyberstalking, kybergrooming, kyberšikana, či sexting. Vzdělávací program se zaměřuje na současnou aktuální problematiku informační bezpečnosti a zahrnuje informace o možných útocích kyberagresorů a možné způsoby obrany. Podrobný přehled témat výuky: On-line a off-line komunikační služby Internetu, chat, e-mail, distribuce souborů, sociální sítě. Kyberšikana. Nepřátelské chování na Internetu (flaming), urážky, nadávky a vyhrožování. Manipulace s cílem sexuálního zneužití oběti (kybergrooming, childgrooming). Obtěžování a pronásledování oběti (stalking). Represivní prostředky (legislativa, školní předpisy, role školy a učitele). Zásady bezpečné komunikace v kyberprostoru. Výchovná prevence (pozitivní školní a rodinné klima, výchova k mravním hodnotám).

Vzdělávací cíl:

Účastníci si prohloubí znalosti o fungování a možnostech kyberprostoru, ale i o rizicích, která jsou s ním spojena. Orientují se v různých typech rizikového chování, které se mohou v kyberprostoru rozvinout. Dokáží analyzovat rizikové chování a jeho dopady ve skupině dětí, se kterou pracují, a zvolit adekvátní kroky k řešení. Znají principy bezpečného chování v kyberprostoru, umějí použít vhodné aktivity pro prevenci nežádoucího chování na internetu.

Hlavním cílem VP je příprava pedagogických pracovníků na prevenci nevhodných komunikačních praktik v prostředí Internetu. Účastníci dokážou rozpoznat základní typy rizikové komunikace v prostředí Internetu a GSM sít. Budou schopni navrhnout preventivní řešení, případně nápravné techniky. Důraz je kladen na prevenci, odbornou přípravu a v širších souvislostech vytváření pozitivního prostředí ve škole. Vzdělávací program seznámí účastníky s různými způsoby komunikace na internetu i s aktuálními postupy preferovanými mládeží, představí rizika pohybu v tomto prostoru, dopady negativního chování a principy bezpečné komunikace. Účastníci si osvojí základní techniky řešení situace a intervence.

Cílová skupina:

- ředitelé škol a školských zařízení
- učitelé 1.stupně ZŠ
- učitelé 2.stupně ZŠ
- učitelé SOŠ a SOU
- učitelé gymnázií
- učitel - metodik prevence
- výchovní poradci

- vychovatelé školských zařízení
- učitelé – vedoucí zájmových kroužků a klubů
- pedagogové volného času
- ostatní pracovníci ve vzdělávání (zájmové a neformální, NNO apod.)

Počet hodin: 8

MODUL 1: On-line a off-line komunikační služby Internetu, chat, e-mail, distribuce souborů, sociální sítě

Možnosti internetu

Zdroj informací, možnost sdílení a sdělení informací (email, soubory, videa, články, blogy, web stránky, profily…), komunikace, hry, nákup a prodej zboží-služeb, e-bankovnictví, sex…

Možnosti mobilu

Komunikační prostředek: volání, SMS, MMS zprávy, fotografování, video dokumentace, internet v mobilu (viz výše), MP3 (hudba), hry…

Možnosti připojení

Bezdrátová, pevná, mobilní komunikační technologie k propojení mezi dvěma a více elektronickými zařízeními, jakými jsou například mobilní telefon, PDA, osobní počítač nebo náhlavní souprava (kabel, bluetooth , Wi-Fi, infra, mobilní operátoři,…..)

Internetové prohlížeče

Webový prohlížeč (též browser) je počítačový program, který slouží k prohlížení World Wide Webu (WWW). Program umožňuje komunikaci s HTTP serverem a zpracování přijatého kódu (HTML, XHTML… apod.), který podle daných standardů zformátuje a zobrazí webovou stránku. Textové prohlížeče zobrazují stránky jako text (obrázky apod.) obvykle velmi jednoduše formátovaný.

Nejznámější jsou: Windows Internet Explorer, Mozilla Firefox, Safari, Google Chrome, Opera

Internetové vyhledávače

Internetový vyhledávač je služba, která umožňuje na Internetu najít webové stránky, které obsahují požadované informace. Uživatel zadává do rozhraní vyhledávače klíčová slova, která charakterizují hledanou informaci a vyhledávač obratem na základě své databáze vypisuje seznam odkazů na stránky, které hledané informace obsahují.

Nejznámější jsou: Google – www.google.cz (com), Seznam – www.seznam.cz, Atlas, Centrum, ICQ, Yahoo a další.

Používané www profily: www.facebook.com, www.lide.cz, www.myspace.com, www.spoluzaci.cz a další…

Komunikační programy

ICQ (I seek you – hledám tě) – posílání textových zpráv, offline posílání zpráv, skupinové chatování odesílání SMS zpráv, odesílání souborů a hry.

Skype – telefonování, posílání textových zpráv, offline posílání zpráv, skupinové chatování odesílání SMS zpráv, odesílání souborů…

a další…

Videa on – line - Youtube – www.youtube.com – YouTube je největší internetový server pro sdílení video a audio souborů.

Sociální sítě

(z angl. social network nebo community network) v rámci pojmů virtuálního světa můžeme definovat jako online službu, která na základě registrace umožní vytvořit profil uživatele, pod kterým lze tuto službu využívat zejména ke komunikaci, sdílení informací, fotografií, videa atd. s dalšími registrovanými uživateli. Sociální sítě jsou fenoménem současné doby. Používání sociálních sítí je velice populární, ale je potřeba dbát na bezpečnost a ochranu soukromí. Narůstá také počet podvodů prostřednictvím sociálních sítí.

Facebook

Statistiky potvrzují, že Facebook je nepopiratelným lídrem na poli sociálních sítí. Číslo, jež je této skutečnosti důkazem, je ohromující -1,871 miliardy aktivních uživatelů po celé planetě (leden 2017).

Internetbanking

Díky Internetu už to nemusí znamenat fronty na poště a vyplňování složenek, banky totiž nabízejí internetové bankovnictví. Internetbanking umožňuje ovládat bankovní účet pohodlně z domova a běžné finanční operace realizovat v několika vteřinách přes Internet. Protože ale Internet se svými takřka neomezenými možnostmi představuje i určitá rizika, je důležité vědět, jak celý systém vlastně funguje a na co si dát pozor.

MODUL 2: Kyberšikana

Je forma agrese, která se uplatňuje vůči jedinci či skupině osob s použitím informačních nebo komunikačních technologií (počítačů, tabletů, mobilních telefonů a dalších moderních komunikačních nástrojů), a ke které dochází opakovaně, ať už ze strany původního agresora či dalších osob - tzv. sekundárních útočníků (např. opakované sdílení nahrávky, opakované komentování apod.). Ačkoli je kyberšikana zpravidla definována jako činnost záměrná, může vzniknout i nezáměrně – např. jako nevhodný vtip, který se v on-line prostředí vymkne kontrole. Kyberšikana je často zaměňována s tzv. on-line obtěžováním.

MODUL 3: Flaming

Jde o nepřátelské chování útočníka vůči oběti ve virtuálním světě. Je to výrazně vyhrocená a agresivní diskuze až hádka na internetu. Někteří uživatelé úmyslně podobné diskuze provokují vkládáním různých kontroverzních příspěvků, urážením účastníků diskuzí apod. Výzkumy ukazují, že slovní napadání je ve virtuálním prostředí až čtyřikrát častější než v reálném životě.

MODUL 4: Kybergrooming

V překladu jde o manipulaci v kyberprostoru s cílem přimět uživatele k osobní schůzce. Útočník, který se většinou vydává za někoho jiného, si vyhledá vhodnou osobu, ve které postupem času vzbudí důvěru a přinutí ji k osobní schůzce, kde pak nějakým způsobem oběť zneužije či využije. V této oblasti jsou nejvíc ohroženy děti, které jsou závislé na technologiích, tráví na internetu většinu času a většinu přátel mají pouze ve virtuálním světě.

MODUL 5: Kyberstalking

V překladu jde o pronásledování v kyberprostoru nejčastěji pomocí SMS, chatu, emailu, telefonu, sociálních sítí, skypu apod. Oběti většinou pronásledovatele (stalkera) znají, často jde o bývalého milence/milenku, kamaráda, zrazeného přítele nebo milovníka. Stalker může být ale i neznámý, a to v případě, že si oběť vyhlédl náhodně na internetu. Pronásledované oběti hrozí naprostá ztráta soukromí, osobních údajů a pocitu bezpečí. Stalking je od 1. června 2010 trestný čin.

MODUL 6: Represivní prostředky (legislativa, školní předpisy, role učitele)

Legislativní rámec (úroveň státu):

Na úrovni státu se prevence rizikového chování – v našem případě kyberšikany či šikany – řídí v obecné rovině řadou strategických dokumentů, ze kterých pak vycházejí dokumenty dílčí. **Mezi strategické dokumenty, které jsou s prevencí kyberšikany spojeny, patří zejména:**

- Zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), ve znění pozdějších předpisů,
- Zákon č. 563/2004 Sb., o pedagogických pracovnících a o změně některých zákonů, ve znění pozdějších předpisů,
- Metodické doporučení k primární prevenci rizikového chování u dětí a mládeže č. j.: 21291/2010-28,
- Metodický pokyn ministryně školství, mládeže a tělovýchovy k prevenci a řešení šikany ve školách a školských zařízeních čj. MSMT-21149/2016,
- Strategie prevence kriminality 2016–2020 (definovaná ve víceletých cyklech Usnesením vlády ČR),
- Národní strategie primární prevence rizikového chování dětí a mládeže na období 2013–2018 (Ministerstvo školství ČR, 2013).

Legislativní rámec (úroveň školy):

Školy jsou povinny zajistit bezpečnost a ochranu zdraví svých žáků a zároveň vytvářet podmínky pro předcházení vzniku sociálně patologických jevů. Tato povinnost je dána školským zákonem (Zákon 561/2004 Sb., 2012), konkrétně § 29, který se zaměřuje na bezpečnost a ochranu a zdraví ve školách. Školami se rozumí školy a školská zařízení.

Strategické dokumenty školy vztahující se k prevenci rizikového chování:

1. Vnitřní řád školského zařízení, školní řád
2. Školní preventivní strategie
3. Preventivní program školy (dříve Minimální preventivní program)
4. Krizové plány

Mezi dalšími dokumenty, které jsou úzce s primární prevencí na základní škole propojeny, mohou patřit např.:

Program poradenských služeb ve škole – ten zahrnuje popis činností, rozdělení rolí

a vymezení odpovědnosti školních poradenských pracovníků, vytvoření časového prostoru na poskytované služby, způsoby komunikace a spolupráce v rámci poradenského pracoviště i vně se specializovanými poradenskými pracovišti ve školství (pedagogicko-psychologická poradna, speciálně-pedagogické centrum, středisko výchovné péče)

a s relevantními organizacemi mimo školství.

Plán dalšího vzdělávání pedagogů – zahrnuje školení pedagogů a ve zvýšené míře pracovníka pověřeného řešením šikany (zpravidla školního metodika prevence) a třídních učitelů (zejm. v prevenci šikanování, v oblasti komunikace, řešení konfliktů, účinné preventivní strategie v praxi školy, interakce mezi učitelem a žákem).

Preventivní a poradenské služby se v prostředí školy poskytují zejména prostřednictvím tzv. školních poradenských pracovišť, která jsou definována vyhláškou Vyhláška č. 72/2005 Sb., o poskytování poradenských služeb ve školách a školských poradenských zařízeních, ve znění pozdějších předpisů.

Poradenské služby ve škole jsou obvykle zajišťovány výchovným poradcem, školním metodikem prevence, případně školním psychologem/školním speciálním pedagogem a jejich konzultačním týmem složeným z vybraných pedagogů (Ciklová, 2014). Cílem školních poradenských pracovišť je především poradenská podpora žáků, rodičů i pedagogů.

Role učitele:

- Posilovat empatii mezi žáky.
- Pracovat na klimatu třídy, školy.
- Vést k úctě k druhým lidem.
- Dávat žákům pozitivní zpětnou vazbu.
- Vytvářet dobré vztahy mezi žáky i kolegy.
- Důsledně zakročovat vůči seznatelným individuálním projevům agrese.

MODUL 7: Zásady bezpečné komunikace v kyberprostoru. Výchovná prevence (pozitivní školní a rodinné klima, výchova k mravním hodnotám)

Zanést do školního řádu pravidla používání ICT, intranetu a mobilních telefonů (během vyučování, přestávkách, v prostorách *školy,….*)

Informovat žáky o netiketě *a „listině práv na internetu“.*

Instalovat a využívat software, který v učebnách vyučujícímu umožňuje informovat se přes svůj počítač, co právě žák na své ploše dělá nebo zaznamenává provoz. (informovat o tomto opatření žáky a systém nezneužívat).

Být vzorem vhodného užívání moderních technologií.
Podporovat pozitivní využívání technologií

Posílit empatii mezi žáky
Pracovat na klimatu
Vést k úctě k druhým

Dávat pozitivní zpětnou vazbu
Vytvářet dobré vztahy

d. Metodika pro lektory mezigeneračního vzdělávacího programu pro oblast bezpečnosti a rizik spojených s používáním digitálních technologií a využíváním online příležitostí určený pro presenční použití ve školách, volnočasových institucích apod.

Bezpečně v kyberprostoru – principy bezpečného pohybu a komunikace v kyberprostoru

Úvod

Základním předpokladem bezpečného a efektivního užívání moderních informačních technologií s přístupem na internet, je být dostatečně digitálně gramotným. Co to obnáší a proč je to tak důležité? Proč je dnes digitální gramotnost tak často diskutované téma, které by na školách nemělo být zanedbáváno? Tento vzdělávací program by měl pomoci účastníkům uvědomit si důležitost vzdělání v této oblasti a naučit se rozlišovat schopnost digitálních domorodců technologie laicky využívat nebo být opravdu digitálně gramotným. Pro digitálně gramotné uživatele internetu je zásadní nejen znát možná nebezpečí, ale zejména jim umět předcházet a tedy využívat různé strategie posuzování vlastního chování a obsahu internetu. Tyto strategie bychom mohli pojmenovat informační gramotností ve virtuálním prostředí. Informační gramotnost pro nás představují zejména 4 klíčové dovednosti jako je vyhledávání informací, posuzování relevance, etické užívání a zejména jejich samostatné publikování.

Možnosti on-line komunikace a jejich rizika

Internet

- nabízí uživatelům nepřeberné množství možností - umožňuje snadnou a rychlou komunikaci (včetně např. telefonování a videochatování zdarma), poskytuje přístup k obrovskému množství informací z celého světa a umožňuje celosvětově informace vyhledávat.
- poskytuje prostor a nástroje pro naši vlastní seberealizaci, podporuje kreativitu a umožňuje sdílet výsledky našeho úsilí s velkým množstvím uživatelů.
- umožnil vzniknout generaci blogerů, youtuberů, streamerů a influencerů, kteří začali vytěsňovat (minimálně u dětského publika) zažitá masmédia. Publikovat díky dostupným nástrojům dnes může v podstatě kdokoli.
- proměnil vzdělávání, díky němu získali zájemci o (sebe)vzdělávání přístup k podstatě neomezeným zdrojům informací (dnes již není problém např. studovat online na prestižních evropských či amerických univerzitách), online výukovým aplikacím i komplexním vzdělávacím prostředím.
- je velmi důležitý také v oblasti bezpečnosti, umožňuje přístup k informacím v případě různých přírodních katastrof, lokalizovat osoby v nebezpečí, informuje o nebezpečích spojených např. se zahraničními cestami do ciziny v případě rizika teroristických útoků či živelných katastrof, poskytuje informace pro záchranné systémy apod.
- umožňuje bavit se, hrát si, uvolnit se, relaxovat a odpočinout si.

Co nám hrozí na internetu?

- Zneužití našich osobních údajů a informací.
- Zneužití informací o tom, kde se pohybujete a jak trávíte čas.
- Zneužití fotografií, záznamů z webkamery, zvukových záznamů.
- Setkání s různými podvodníky, s uživateli, kteří se vydávají za někoho jiného, než kým opravdu jsou, s cílem vás oklamat a poškodit, využít pro svůj prospěch.
- Lživé informace o nějakém tématu.
- Manipulace. To znamená, že na internetu můžou být představovány různé hodnoty, normy, pravidla a postoje jako ty pravé, zdravé a normální i přes to, že opak je pravdou.
- Setkání s agresivními uživateli, se sexuálními devianty.
- Kyberšikana.
- Ztráta virtuální identity – může se stát, že se vám někdo naboural do uživatelského účtu nebo profilu a změní ho podle svých představ s tím, že se vydává za vás.
- Závislost na užívání internetu.
- Zhoršení vztahů s kamarády nebo s rodinou kvůli tomu, že komunikujete hlavně online a tak trochu zapomínáte, jaké to je komunikovat z oči do očí.
- Ohrožení různými počítačovými viry, které se šíří například pomocí e-mailu.

Sociální sítě

Sociální síť (z angl. social network nebo community network) v rámci pojmů virtuálního světa můžeme definovat jako online službu, která na základě registrace umožní vytvořit profil uživatele, pod kterým lze tuto službu využívat zejména ke komunikaci, sdílení informací, fotografií, videa atd. s dalšími registrovanými uživateli. Sociální sítě jsou v současné době velice často diskutovaným tématem a jsou označovány za celosvětový fenomén. Používání sociálních sítí je velice populární, ale je potřeba dbát na bezpečnost a ochranu soukromí. Narůstá také počet podvodů prostřednictvím sociálních sítí.

Sociální sítě lze rozdělit do několika kategorií:

- Profilově založené sociální sítě (Facebook, Baidu Tieba, VKontakte, LinkedIn
- Obsahově založené sociální sítě (YouTube.com, Instagram, Snapchat, Last.fm, Pinterest)
- Virtuální sociální sítě (Second Life, World of Warcraft, World of Tanks)
- Micro-blogovací sociální sítě (Twitter, Jaiku)
- Komunikační služby (Facebook Messenger, WhatsApp, Viber)

V současné době je se značným náskokem největší sociální sítí Facebook s téměř dvěma miliardami registrovaných uživatelů (1,87 miliardy – leden 2017). 1,2 miliardy uživatelů se na Facebook denně přihlásí prostřednictvím mobilních telefonů. Přes 9 % uživatelů tvoří děti ve věku 13 – 17 let. Věkový limit pro vstup na Facebook je 13 let. Problémy sociální sítě Facebook vycházejí především z koncentrace velkého množství osobních a citlivých údajů, které mohou být různým způsobem zneužity. Celosvětově je zaznamenána řada případů, kdy z Facebooku unikly osobní údaje (např. prostřednictvím aplikací a her propojených s Facebookem).

Facebook obsahuje velké množství osobních údajů, které lze zneužít nejrůznějšími způsoby a má velmi problematickou blokaci.

Rizika sociálních sítí

Každé užívání sociální sítě zpravidla obnáší sdělování a sdílení osobních údajů, myšlenek, zážitků a dalších informací udržujících dobré vztahy s přáteli. Je ale třeba si uvědomit, že vše to, co se na internetu zveřejní, již většinou nelze vzít zpět. Je namístě si dobře rozmyslet, co o sobě a svém soukromí uživatel na internetu zveřejní. A praxe potvrzuje, že zejména děti se svým soukromím na internetu nakládat neumějí! Denně je internetovými zloději odcizeno mnoho virtuálních identit (např. profilů na sociální síti), včetně všech fotografií a konverzací s dalšími uživateli.

Kyberšikana

Kyberšikana, též kybernetická šikana, počítačová šikana či cyberbullying je kolektivní označení forem šikany prostřednictvím elektronických médií, jako je internet a mobilní telefony, které slouží k agresivnímu a záměrnému poškození uživatele těchto médií. Stejně jako tradiční šikana zahrnuje i kyberšikana opakované chování a nepoměr sil mezi agresorem a obětí. Aktéry kyberšikany jsou (obdobně jako u klasické šikany): Agresor – Oběť – Přihlížející (publikum).

Znaky kyberšikany:

- Anonymita – útočník zpravidla vystupuje anonymně, vystupuje pod falešnými přezdívkami (nicky), vytváří jednoúčelové e-mailové schránky nebo falešné profily na sociálních sítích, a díky tomuto pocitu anonymity je posílena jeho odvaha v použití agresivnější formy útoku;
- Profil útočníka – ve virtuálním světě neplatí pravidla klasické šikany – nezáleží zde na věku, pohlaví, fyzické síle útočníka, sociálním postavení apod. Převládají převážně znalosti a dovednosti v užívání informačních a komunikačních technologií;
- Místo a čas útoku nelze předpokládat – zatímco u klasické šikany lze předpokládat, kdy a kde k útoku dojde, u kyberšikany útok může přijít kdykoliv a kdekoliv. Třeba o půlnoci a prostřednictvím různých kanálů: SMS, emailem, videem na videoportálu (např. youtube.com), příspěvkem na sociální síti apod; šíření kyberšikany pomáhá útočníkovi „publikum“;
- Zejména možnost sdílení nebo následné přeposílání závadových příspěvků zvyšuje intenzitu vedeného útoku. Útočníkovi tedy postačí příspěvek publikovat pouze jednou, o jeho opakování a šíření se často postará ono „publikum“. Jednání tohoto publika nepřímo ale velice důrazně zvyšuje negativní psychický dopad na oběť;
- Není snadné rozeznat dopad kyberšikany na oběť – vzhledem k tomu, že dopady kyberšikany jsou spíše v rovině psychické, je nesnadné je na oběti rozeznat nebo poznat oběť samotnou. Na rozdíl od klasické šikany u kyberšikany je o mnoho složitější vysledovat varovné signály – modřiny, potrhané a špinavé oblečení apod. Oběť se často uzavírá do sebe a přestává komunikovat s okolím, ať už ze strachu, že útočník zintenzivní své útoky, ze studu nebo strachu z nepochopení problému rodiči nebo učiteli.

Prostředky kyberšikany:

- textové zprávy prostřednictvím mobilních telefonů,
- fotografie a videoklipy zachycené přes kamery mobilních telefonů a následné zveřejněné na internetu,
- telefonní hovory,
- e-mailové zprávy,
- chatové místnosti,

- tzv. instant messaging (ICQ, Skype aj.),
- internetové stránky, blogy,
- sociální sítě,
- on-line hraní her.

Nejčastější projevy kyberšikany:

- verbální ponižování, urážení, zesměšňování,
- prolomení elektronického (např. e-mailového účtu,
- opakované obtěžování (prozvánění, spamování apod.),
- vyhrožování nebo zastrašování,
- publikování ponižující fotografie,
- ostrakizace, vyloučení z virtuální komunity,
- happy slapping (v překladu „zábavné fackování“),
- zveřejňování cizích tajemství s cílem poškodit oběť.

a) Flaming

Flaming se označuje agresivní chování projevující se urážkami, nadávkami a vyhrožováním. Jedná se o jev v dnešní době velmi populární a běžný uživatel se s tímto chování může setkat u komentářů fotografií nebo přímo při konverzaci. Flaming nemá za cíl nic jiného než rozčílit, naštvat, ponížit oběť a to zcela beztrestně a většinou i anonymně. Podle výzkumu je flaming jako slovní napadení ve virtuálním prostředí čtyřikrát častější než v reálném životě. A právě anonymita je to, co ve většině případů hraje klíčovou roli v kyberšikaně a způsobuje tenkou hranici mezi běžným uživatelem a agresorem.

Rady, doporučení: Oběť flamingu by si měla v první řadě uvědomit, že není potřeba každého přesvědčovat o své pravdě, i kdyby byl sebevíc v právu. Agresorovi, který se dopouští flamingu, většinou stejně nezáleží na argumentech, jde mu pouze o vyprovokování hádky a urážení se. Proto by si uživatelé sociálních sítí měli udržet zdravý nadhled a vměšovat se do co nejmenšího množství hromadných diskusí a diskutovat raději osobně, kde si podobné nádavky většina agresorů nedovolí.

b) Kybergrooming

Kybergrooming lze vysvětlit jako psychickou manipulaci dítěte dospělým prostřednictvím moderních komunikačních technologií s cílem získat důvěru oběti, vylákat ji na osobní schůzku a zpravidla sexuálně zneužít. Kybergrooming se nejčastěji vyskytuje v rámci instant messengerů (Facebook Messenger, Skype), sociálních sítí (Facebook, Twitter, Badoo), internetových seznamek (libimseti.cz) a různých blogovacích stránek. Obětí kybergroomingu se může stát prakticky kdokoliv, zpravidla se ale jedná o dívky ve věku 11-17 let, často užívající informační a komunikační technologie, trpící nedostatkem sebedůvěry, pocitem osamění. Jsou otevřené manipulaci a neznalé rizik internetové komunikace. Kybergroomer je zpravidla sexuální útočník využívající informační a komunikační technologie k prosazení svého cíle. Často se vydává za jinou osobu, než ve skutečnosti je, dle vybrané oběti. Pokud se snaží spřátelit se s 12 letou dívkou, vydává se za 14 letého chlapce. Významnou vlastností kybergroomera (není však pravidlem) je trpělivost – vydrží si s obětí psát i několik měsíců, jen aby pevně získal její důvěru.

Rady, doporučení: Nejdůležitější prevencí proti kybergroomingu je neposkytovat nikomu cizímu žádné soukromé materiály, i kdyby se zdál být důvěryhodný sebevíc. Zvýšená pozor-

nost by také měla být v případě, že si osoba, která nás kontaktovala, nepřeje, aby o vašem vztahu někdo věděl. Dávat si mimořádný pozor, když má dojít ke schůzce s osobou, kterou znáte pouze z internetu, nejlépe se podobným schůzkám úplně vyhnout.

c) Kyberstalking

Kyberstalking – který je od 1. 1. 2010 klasifikován jako trestný čin, lze jednoduše nazvat nebezpečným pronásledováním. Útočník využívá informační a komunikační technologie k dlouhodobému, opakovanému a stupňovanému kontaktování – pronásledování své oběti, ve které chce úmyslně vyvolat pocit strachu o své soukromí, zdraví nebo život.

Některé formy kyberstalkingu

- zasílání zpráv SMS,
- telefonáty a prozvánění,
- zasílání zpráv prostřednictvím messengerů a e-mailů,
- opakované komentování příspěvků oběti na sociálních sítích,
- vkládání příspěvků na profily sociálních sítí oběti,
- krádež identity oběti – následné vystupování jejím jménem,
- kontaktování oběti pod falešnou identitou (několika falešnými identitami),
- monitorování počítače oběti speciálními programy (keyloggery apod.),
- zveřejňování informací ze života obětiobtěžující kontaktování přátel oběti aj.

Některé motivy kyberstalkera

- obtěžovat, vyhrožovat a vydírat oběť,
- demonstrovat svou sílu,
- poškodit oběť před společností,
- opětovné navázání vztahu po odmítnutí aj.,

Rady, doporučení: Při řešení podobné situace je ze všeho nejdůležitější rozvázat s agresorem veškeré kontakty, nepodněcovat ho k hovoru, nediskutovat s ním, měnit trasu do školy/do práce, ale hlavně je třeba si shromažďovat veškerý materiál, který by později mohl sloužit jako důkazní (kopie konverzací a výhružným e-mailů, vzkazy, výpisy hovorů atd.).

Zásady bezpečné komunikace v kyberprostoru

Základním způsobem, jak lze předcházet kyberšikaně či minimalizovat její dopad, je především všeobecná primární prevence. Jejím cílem je předcházet rizikovému chování. Prevenci zaměřenou na oblast kyberšikany a dalších forem kybernetické agrese lze realizovat ve formě specifické i nespecifické.

Specifickou primární prevenci lze rozdělit do 3 úrovní, na:

a) Prevenci všeobecnou (zasahuje celou třídu, školu apod. bez rozdílu). Sem lze zahrnout aktivity typu dlouhodobé preventivní programy, interaktivní besedy, projektové dny atd. Zároveň lze témata primární prevence zahrnout do výuky, propojit s průřezovými tématy a klíčovými kompetencemi žáka.

b) Prevence selektivní (zasahuje osoby, u kterých jsou ve zvýšené míře přítomny rizikové faktory pro vznik a vývoj různých forem rizikového chování, např. děti z vyloučených lokalit, děti s poruchami chování apod.).

c) Prevence indikovaná (zacílena na situace, kdy se ve třídě/škole již kyberšikana vyskytla).

Nespecifická prevence je pak zaměřena na rozvoj zdravého klimatu ve třídě a škole, posilování dobrých vztahů mezi dětmi apod.

Jak předcházet kyberšikaně na úrovni školy:

- Zanést do školního řádu pravidla používání ICT, intranetu a mobilních telefonů (během vyučování, přestávkách, v areálu školy).
- Informovat žáky o netiketě a „listině práv na internetu“. O této listině by měli být informováni i rodiče nezletilých žáků, např. vyvěšením na webových stránkách škol.
- Instalovat a využívat software, který v učebnách vyučujícímu umožňuje informovat se přes svůj počítač, co právě žák na své ploše dělá. (Informovat o tomto opatření žáky a systém nezneužívat!)
- Být vzorem vhodného užívání moderních technologií.
- Pracovat na povědomí žáků o rizikovém chování na internetu.
- Definovat kompetence v rámci školy a na akcích konaných školou mimo místo, kde se uskutečňuje vzdělávání).
- Začlenit témata spojená s rizikovým chováním na internetu do výuky.
- Vzdělávat pedagogy.
- Podporovat pozitivní využívání technologií.

Jak předcházet kyberšikaně na úrovni jednotlivých pedagogů:

- Posilovat empatii mezi žáky.
- Pracovat na klimatu třídy, školy.
- Vést k úctě k druhým lidem.
- Dávat žákům pozitivní zpětnou vazbu.
- Vytvářet dobré vztahy mezi žáky i kolegy.
- Důsledně zakročovat vůči individuálním projevům agrese.

Desatero dobrého „kybernetického rodiče“

1. Vzdělávejte se

Svět informačních a komunikačních technologií je velice dynamické prostředí a k získání patřičného nadhledu je třeba se neustále zajímat o nové online služby, technologické novinky, ale také kybernetické hrozby. Pokud Vás dítě svými znalostmi v oblasti informačních a komunikačních technologií převyšuje, umožněte mu vás vzdělávat – tímto jednoduchým trikem rodič získá kromě aktivní komunikace s dítětem také přehled o tom, jak na internetu tráví čas, o co jeví zájem.

2. Buďte i “virtuálním” přítelem a komunikujte

V opravdovém světě chce mít většina rodičů přehled o tom, s kým se jeho dítě stýká – ve virtuálním světě by tomu nemělo být jinak. Staňte se přítelem svého dítěte na sociálních sítích, které užívá. Nezískáte tím nejen přehled o jeho „virtuálních“ přátelích, ale i další zdroj informací o zálibách nebo momentálních náladách dítěte. Diskutujte o tom, jaké služby na internetu využívá a proč. Ptejte se i na rizika s užívanými službami spojená, poznáte, zda si je jich dítě vědomo a zda by si dokázalo poradit.

3. Respektujte své dítě

Svět našich dětí je značnou mírou opřen o to, co je právě moderní, nebo jak by se sami vyjádřili – co je IN a TRENDY. Dítě může být kolektivem odmítáno kvůli nošení neznačkových oděvů stejně tak jako kvůli online službám, které užívá nebo naopak neužívá. Nezřídka si dítě zřídí profil na sociální síti i přes zákaz rodičů, neboť je k tomu kolektivem nepřímo donuceno. Pokud by tak dítě neučinilo, mohlo by se stát terčem posměchu nebo až obětí kyberšikany.

4. I na internetu jsou lži a podvodníci

Vzdělávejte se společně a naučte se hledat kvalitní zdroje informací. Naučte děti, že ne vše, co je na internetu psáno, musí být pravdou! A stejně tak jako lidé lžou ve světě reálném, lži i ve světě virtuálním, a ne každý uživatel internetu je ve skutečnosti tím, za koho se vydává. Naučte své dítě ověřovat informace na internetu získané.

5. Naučte své děti chránit si své soukromí

Upozorněte dítě, aby nikde na internetu nesdělovalo své osobní údaje a vysvětlete proč. Neuvádět zejména: příjmení, adresu bydliště a školy, přístupová hesla, rodné číslo, číslo mobilního telefonu, osobní e-mail, věk (hl. u mladších dětí), intimní fotografie, videa a informace, rodinnou, finanční a vztahovou situaci, nepřítomnost rodiny doma (dovolená apod.)

Pomáhejte dítěti chránit si své soukromí užitím správných uživatelských jmen k jednotlivým službám a aplikacím a k nim i kvalitních silných hesel. Vysvětlete dětem, že je nebezpečné setkávat se s přáteli z internetu, které osobně neznají.

6. Posilujte netiketu

Netiketa je ekvivalent pravidel slušného chování pro internetové prostředí. Stejně jako v reálném světě je třeba se k ostatním chovat stejně, jako bychom si přáli, aby se ostatní chovali k nám. Pod domnělou anonymitou internetu jsou si uživatelé schopni napsat navzájem i taková slova, která by nikdy v reálném rozhovoru tváří v tvář nikdy neužili.

Rovněž dětem vysvětlete, že nevhodným chováním na internetu se může stát i pachatelem trestného činu (např. sdílení obsahu chráněného autorským zákonem, přechovávání dětské pornografie apod.).

7. Kontrolujte!

Využijte dostupných prostředků k monitorování činnosti svého dítěte ve virtuálním prostředím. V tomto případě se nejedná o nějaké omezování osobní svobody dítěte, jak bývá někdy mylně uváděno. Jedná se o stejnou činnost, jako byste dohlíželi na své dítě na dětském hřišti. Pokud by ze země zvedlo injekční stříkačku a chtělo si s ní hrát, také byste zasáhli! Proto např. namátkově kontrolujte historii navštívených webových stránek nebo komunikaci dítěte – najdete-li závadovou komunikaci, zálohujte ji jako případný důkaz. Jedná-li se o závažnou závadovou komunikaci, kontaktujte Policii ČR a zálohu ponechte odborníkům. V případě potřeby užijte speciální programy na kontrolu činnosti dítěte ve virtuálním prostředí.

8. Buďte oporou – ne vychovatelem

Reagujte na případné nevhodné chování dítěte na internetu přiměřeně, aby nemělo zábrany v budoucnu s vámi o případných problémech hovořit. Nezakazujte dítěti po špatné zkušenosti další užívání internetu nebo jeho služeb. Začne před vámi svou opravdovou činnost skrývat. Rozumně prodiskutujte vzniklý problém a vysvětlete rizika. Vysvětlete, že pokud se

stanou obětí virtuálních predátorů, není to jejich chyba a není ostuda se s tím někomu svěřit. V případě potřeby sami vyhledejte pomoc např. na Rodičovské lince 840 111 234 (www.rodicovskalinka.cz) nebo na Policii ČR.

9. Kontrolujte čas strávený ve virtuálním prostředí

Na základě vzájemné dohody upřesněte pravidla užívání internetu – zejména čas jeho užíváním strávený. V tomto případě ignorujte návody, ve kterých je uvedeno, že je nutné striktně dodržovat domluvený nebo stanovený čas. Každé dítě je individuální a je třeba rozlišit, zda dítě tráví svůj čas na internetu tři hodiny u počítačové hry nebo se samo z vlastního zájmu snaží pochopit základy programování. S ohledem na tyto aktivity dokáže každý rodič sám odhadnout optimální dobu strávenou jejich dítětem ve virtuálním prostředí. A pokud je dítě skutečně okouzleno programováním – světem jedniček a nul, motivujte jej a určitě vyzkoušejte online kurzy programování pro děti na www.code.org, http://scratch.mit.edu nebo https://hourofcode.com.

10. Buďte citliví ke změnám v chování dítěte

Jakákoliv změna v chování dítěte může být varovným signálem, že nemusí být vše v pořádku. Dítě se mohlo stát obětí kyberšikany nebo může být vydíráno ze strany neznámého pachatele. Laxnost a nečinnost může mít tragické následky.

Sledujte varovné příznaky dítěte:

- snaží se být více o samotě, přestává otevřeně hovořit o tom, co jej na internetu např. pobavilo; při užívání telefonu nebo počítače vyžaduje soukromí, po příchodu rodiče telefon zamyká nebo u počítače přepne okno prohlížeče (či jej zcela vypne);
- maže svou aktivitu v zařízení (historii prohlížených webových stránek apod.); přestává hovořit o tom, s kým se na internetu stýká a jaké aktivity tam provádí.

Forma, metody a prostředky VP

Forma VP – prezenční

Metody VP – doporučeny diskusní, situační a inscenační metody, demonstrace na konkrétních případech – rozborová situace a rozbor konkrétních případů, prožitkové metody, aktivní sociální učení

Prostředky – skupinové, hromadné vyučování

Materiální – flipchart, fixy, projektor

Nemateriální – situační, inscenační a prožitkové metody

Použité zdroje

http://www.msmt.cz/vzdelavani/socialni-programy/metodicke-dokumenty-doporuceni-a-pokyny

www.bezpecnyinternet.cz

www.e-bezpeci.cz

www.napisnam.cz

www.e-nebezpeci.cz

http://prvok.upol.cz

www.seznamsebezpecne.cz

www.linkabezpeci.cz

www.bezpecne-online.cz

www.ditekrize.cz

www.uoou.cz

www.nntb.cz

www.nebudobet.cz

www.internetembezpecne.cz

www.sikana.org

www.saferinternet.cz

www.pdf.upol.cz

www.medium.com

www.o2chytraskola.cz

http://www.rozhlas.cz/teens/slusne/_zprava/internet-jaka-nebezpeci-na-nas-ci-haji--1017632

www.kyber-sikana.eu

www.jsns.cz

www.nukib.cz

www.budsafeonline.cz