



KRAJE PRO
BEZPEČNÝ INTERNET
bud'te o klik napřed



Vnımání kyberkriminality mezi dětmi

Výzkumná zpráva

2023

Vnímání kyberkriminality mezi dětmi (výzkumná zpráva)

Projekt Kraje pro bezpečný internet

Jihlava, 2023

Obsah

Úvodní slovo	4
1. Úvod do problematiky	5
2. Identifikace výzkumu	7
3. Metodologie výzkumu	7
3.1. Výzkumný vzorek	7
3.2. Metodika výzkumu	8
3.3. Výzkumný nástroj	8
4. Výsledky výzkumu	9
4.1. Sociální sítě	9
4.2. Prevence kyberkriminality na školách	10
4.3. Znalost kyberkriminality	12
4.4. Zkušenost s kyberkriminalitou	17
5. Shrnutí výzkumu	18
6. Závěr	19
7. Literatura	20
8. O realizátorech	21
9. Kontakty na realizátory	22

Úvodní slovo

Když jsme v roce 2018 realizovali Výzkum vnímání kyberkriminality mezi žáky poprvé, byli jsme překvapeni zájmem respondentů se do šetření zapojit. Výsledky byly v některých oblastech takové, jak jsme předpokládali, ale překvapivé bylo například to, že žáci často nemají ponětí, co je kyberkriminalita, často vědí, že se taková věc nemá dělat, ale netuší, že už překračují zákon. Především se jednalo o problematiku autorských práv nebo zveřejňování fotografií osob.

Kyberprostor se za pět let výrazně změnil. Setkáváme se s novými hrozbami, novými aplikacemi nebo sociálními sítěmi, zažíváme rozmach umělé inteligence. Prožili jsme období epidemie Covid, kdy se většina našich aktivit přesunula do online prostoru. Rozhodli jsme se tedy výzkum po pěti letech zopakovat. Chtěli jsme zjistit, jak se vnímání kyberkriminality za tu dobu změnilo, jak je to s hrozbami nebo preventivními aktivitami v této oblasti. Výstupy výzkumu nám kromě porovnání situace v roce 2018 a 2023 pomohou nastavit směřování aktivit projektu KPBI a jeho partnerů. Výzkumná zpráva bude volně dostupná na webu www.KPBI.cz, kde ji budou moci využít i jiné subjekty zaměřené na prevenci kyberkriminality.

Ing. Lucie Časarová
vedoucí projektu Kraje pro bezpečný internet
Jihlava, 2023

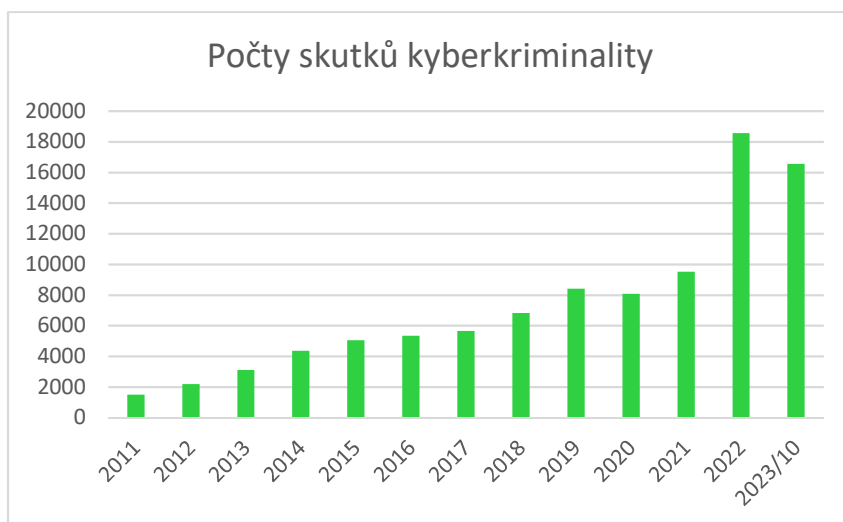
1. Úvod do problematiky

Počítače, internet, sociální sítě a kyberprostor, to je dnes běžnou součástí našeho života i života našich dětí. Podle výzkumu¹ prováděného v roce 2022 Univerzitou Palackého v Olomouci, používá sociální sítě přes 93% dětí, dle výzkumu² Ami digital index 2023 je toto procento u mladé populace 15+ dokonce 96%. Překotný rozvoj používání těchto technologií však klade zvýšené nároky na jejich uživatele. Zejména na děti, které tyto technologie využívají ve větší míře než jejich rodiče. Děti se tak používání těchto technologií učí sami. Proto je důležitá role prevence, která pomáhá předcházet rizikovému chování u dětí a učí děti správnému a bezpečnému chování v kyberprostoru.

Prevenici a konkrétně prevenci kriminality se věnuje v České republice mnoho subjektů. Problematika prevence kriminality je formulována jako součást vládní politiky v několika dokumentech. Preventivní politiku má ve své působnosti Republikový výbor pro prevenci kriminality. Ten ve své Strategii prevence kriminality v České republice na léta 2022 až 2027,³ schválené 6. 4. 2022, má prevenci kybernetické kriminality jako jeden z pilířů. Rozvoj systému prevence kyberkriminality dále zajišťuje Ministerstvo vnitra, které koordinuje součinnost jednotlivých subjektů, vč. partnerů ze státní správy, krajské i obecní samosprávy, neziskových organizací atd.

V případě prevence u dětí a mládeže má stěžejní úlohu Ministerstvo školství, mládeže a tělovýchovy, které přijalo Národní strategii primární prevence rizikového chování dětí a mládeže na období 2019 – 2027⁴. Národní strategie je závazná pro všechny podřízené instituce a koordinuje jednotlivé subjekty podílející se na prevenci ve školách a školských zařízeních.

Kybernetická kriminalita je široká skupina trestných činů, které jsou částečně nebo zcela páchané v kyberprostoru. Je to také jediný druh kriminality, jejíž počty každý rok rostou a nepředpokládá se, že by se to v následujícím období mělo měnit. Proto je nutné kyberkriminalitě věnovat zvýšenou pozornost a pokusit se s ní bojovat všemi dostupnými prostředky, v případě dětí a mládeže hlavně za pomoci prevence.



¹ <https://e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/155-deti-a-kult-krasy-v-online-svete-2022/file>

² <https://amidigital.cz/wp-content/uploads/2023/05/tahak-3.pdf>

³ <https://www.mvcr.cz/clanek/nova-strategie-prevence-kriminality-v-cr-na-leta-2022-2027-byla-schvalena-vladou.aspx>

Jedním z významných projektů, které se podílejí na prevenci rizikových jevů v kyberprostoru v České republice je i projekt Kraje pro bezpečný internet (dále jen KPBI), realizovaný pod záštitou Asociace krajů České republiky. Do projektu je od konce roku 2023 zapojeno všech 14 krajů v ČR. Projekt KPBI byl schválen Radou Asociace Krajů ČR na 6. zasedání Rady dne 3. září 2013. Od roku 2014 je projekt finančně podporován dotacemi z Programu prevence kriminality Ministerstva vnitra ČR, jednotlivými kraji a komerčními partnery. Hlavním cílem projektu je zvýšit informovanost o rizicích internetu a možnostech prevence a pomoci. V rámci projektu jsou připravovány e-learningové kurzy pro žáky a studenty, lekce pro učitele, rodiče a veřejnost, sociální pracovníky a policisty. Dále také v rámci projektu vzniklo mnoho seriálů videospotů a v roce 2023 podcasty.

Pro efektivní fungování a přesné zacílení preventivní činnosti jsou nezbytné aktuální informace o znalostech a zkušenostech cílové skupiny, v tomto případě dětí a mládeže, s rizikovými jevy v kyberprostoru. V této souvislosti byl v rámci realizace projektu KPBI opětovně iniciován výzkumný projekt „Kraje pro bezpečný internet - Výzkum vnímání kyberkriminality mezi dětmi“. Stejný výzkum byl realizován již v roce 2018 a v součásti aktuálního výzkumu bude srovnání, jak se změnilo vnímání kyberkriminality mezi dětmi během pěti let.

⁴ https://www.msmt.cz/uploads/narodni_strategie_primarni_prevence_2019_27.pdf

2. Identifikace výzkumu

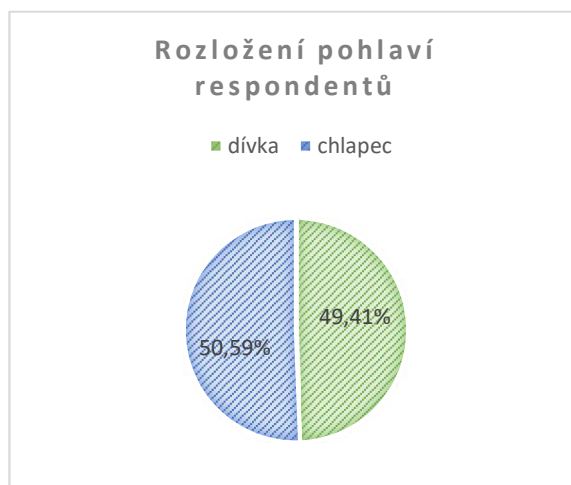
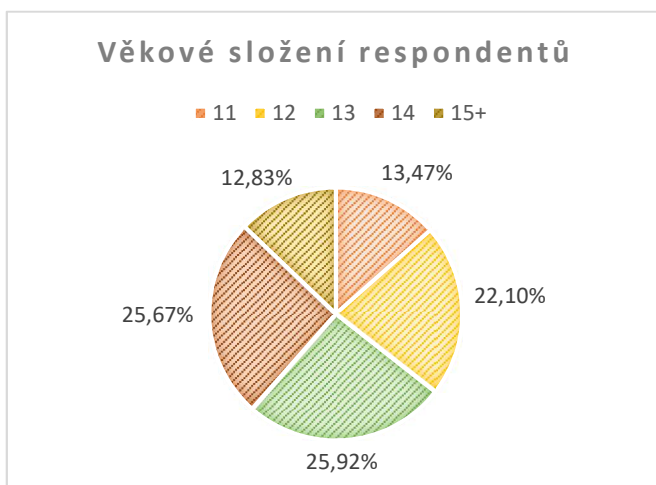
Výzkum byl realizován v rámci projektu Kraje pro bezpečný internet, na základě spolupráce Kraje Vysočina a Policie ČR. Navazuje na výzkum realizovaný v roce 2018, do kterého se zapojilo 50 917 respondentů. Cílem výzkumu bylo zjistit, jakým směrem se znalost kyberkriminality a zkušenost s ní posunula. Výzkum se zaměřuje nejen na kvantitativní analýzu dat, ale také na jejich porovnání z roku 2018 s aktuálními daty. Očekávaná návratnost byla 30 000 dotazníků, což bylo výrazně překonáno, školy měly o dotazníkové šetření zájem.

3. Metodologie výzkumu

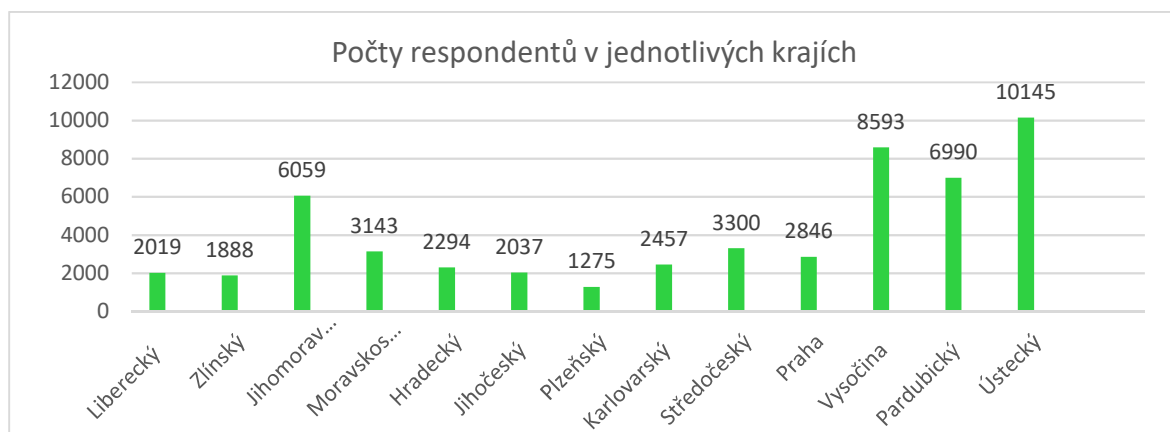
3.1. Výzkumný vzorek

Cílovou skupinou výzkumu byli žáci druhé stupně základních škol a odpovídajících tříd víceletých gymnázií ve věku od 11 do 16 let. Do výzkumu se zapojili školy ze 13 krajů. Olomoucký kraj se do projektu KPBI zapojil až po skončení výzkumného šetření a tedy se výzkumu neúčastnil. Celkem se zúčastnilo 53 049 respondentů. Školy se zapojovaly na základě dobrovolnosti a jejich kapacitních možností.

Průměrný věk respondentů byl 13,02 let, výzkumu se zúčastnilo 49,41% dívek (n=26 216) a 50,59% chlapců (n=26838), což odpovídá normálnímu vzorku populace.



Zapojení škol do výzkumu bylo v jednotlivých krajích různé. Nejvíce se zapojily školy z Ústeckého kraje (10 145 respondentů), naopak nejméně se zapojily školy z Plzeňského kraje (1 275 respondentů).



3.2. Metodika výzkumu

Výzkum byl prováděn kvantitativním dotazníkovým šetřením prostřednictvím anonymních online dotazníků. Dotazníky byly distribuovány do škol ve spolupráci s krajskými koordinátory projektu KPBI, přes odbory školství na jednotlivých krajských úřadech, manažery prevence kriminality, apod. Informace o dotazníku byly zaslány na ředitele škol, případně školní metodiky prevence. Ti dotazníky obdrželi s průvodním dopisem pro ředitele školy a s návodem pro pedagogy, kteří budou dotazníky se žáky vyplňovat. Školám bylo doporučeno, aby pedagogové dotazníky vyplňovali s žáky v rámci vyučovací hodiny Informatiky či obdobného předmětu. Metodika výzkumu i cesta distribuce dotazníků byla vyzkoušena v předchozím výzkumu a osvědčila se.

V průběhu vyhodnocování výsledků bylo zjištěno, že 1 100 dotazníků v Jihomoravském kraji bylo vyplněno pravděpodobně robotem. Tyto dotazníky byly ručně odfiltrovány a data z nich nejsou ve výsledcích zahrnuta.

3.3. Výzkumný nástroj

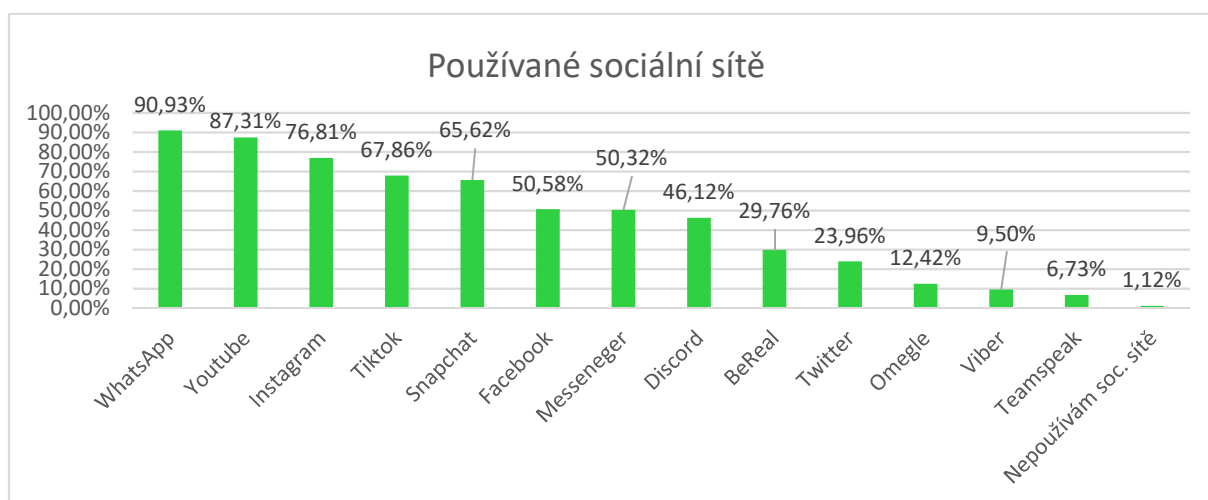
Vlastní dotazník byl zpracován v programu Google Forms a byl distribuován do škol prostřednictvím průvodního dopisu s online odkazem. Pro každý kraj byla vytvořena jedna verze dotazníku, tak aby bylo možné výsledky třídit dle jednotlivých krajů. Dotazník neověřoval IP adresu ani opakované vyplnění, neboť bylo očekáváno vyplňování více dotazníků na stejných zařízeních v rámci jedné školy, kdy se v jedné počítačové učebně vystřídá více tříd.

Dotazník byl složen ze čtyř částí. První část obsahovala 6 otázek týkajících se statistického třídění, používaných sociálních sítí, absolvovaných a preferovaných preventivních programů. Druhá a třetí část zjišťovala znalosti žáků v oblasti kyberkriminality. Druhá část byla tvořena 1 výčtovou otázkou s 36 možnostmi, třetí část tvořila baterie 21 otázek, s hodnotící škálou dle závažnosti jednání. Poslední část obsahovala 26 dichotomických otázek zjišťujících zkušenosti žáků s kyberkriminalitou.

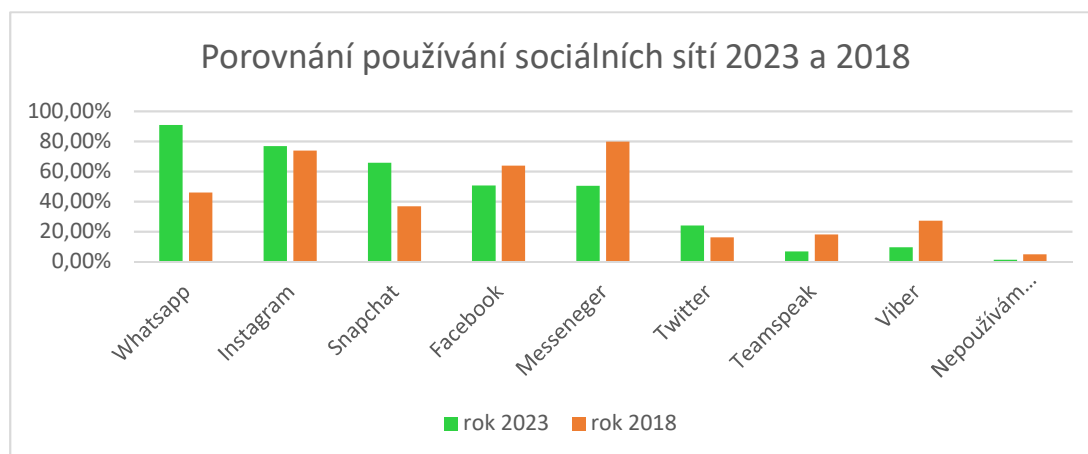
4. Výsledky výzkumu

4.1. Sociální sítě

Žáci byli dotazováni, na jakých sociálních sítích mají účet. Otázka byla částečně otevřená, kromě výčtu možností měli žáci možnost vyplnit další názvy. Výsledky se mezi kraji výrazněji nelišily, nejvíce užívanou sociální sítí byl WhatsApp (průměrně 90,93%), následovaný sítí Youtube (87,31%) a Instagram (76,81%). Odpověď „Nepoužívám sociální sítě“ zvolilo pouze 1,12% žáků. Zajímavostí je, že v otevřených otázkách se objevovalo, že WhatsApp mají žáci zřízený, protože to chce po nich škola pro komunikaci.



Ve srovnání s rokem 2018 je zde patrný rapidní nárůst užívání sociálních sítí. Toto je zapříčiněno mimo jiné pandemií COVID, kdy žáci museli začít používat sociální sítě pro komunikaci se školou a s ostatními spolužáky v rámci online výuky. V roce 2018 byla nejužívanější sociální síť Messenger (79,8%), následovaná Instagramem (73,8%) a Facebookem (63,7%). Síť BeReal ještě neexistovala, TikTok se teprve začínal objevovat, ve výsledcích byl zmíněn v jednotkách procent.

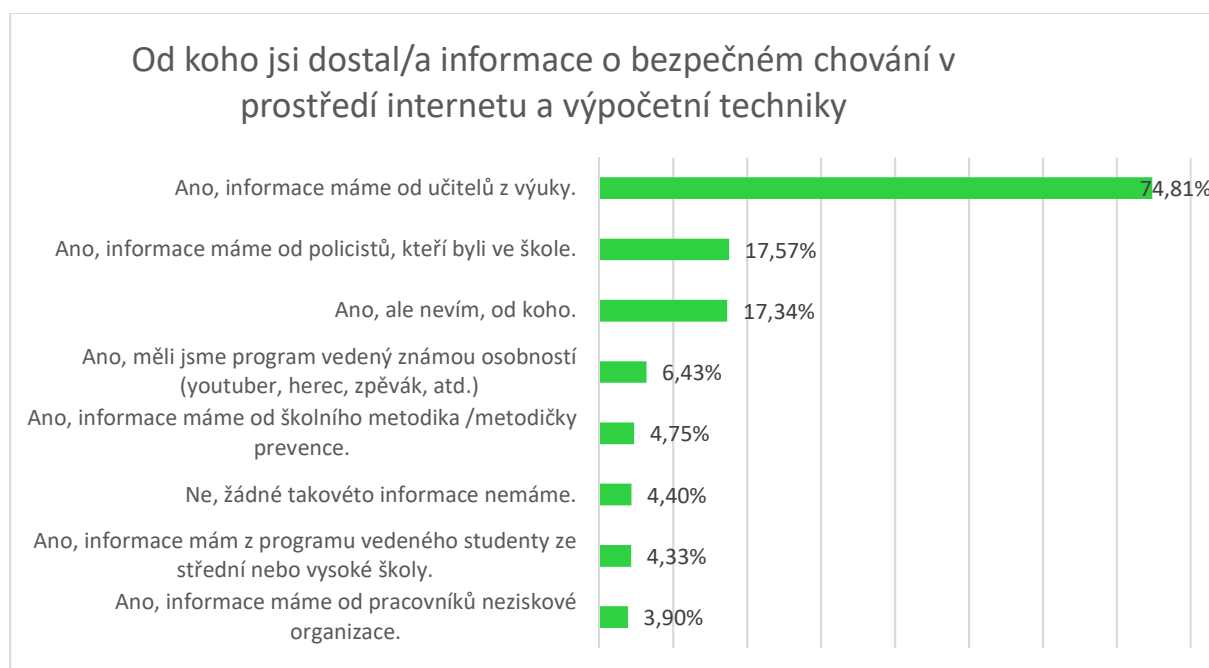


4.2. Prevence kyberkriminality na školách

V další části byli žáci dotazováni, od koho informace o kyberkriminalitě získali a o jaká témata mají při preventivních programech zaměřených na kyberkriminalitu zájem. Tato otázka ve výzkumu z roku 2018 nebyla a byla do dotazníku doplněna na podnět krajských koordinátorů KPBI. Poslední otázka byla zaměřena na to, od koho by rádi tyto informace slyšeli. Odpovědi mohou napomoci preventivním pracovníkům, jakou formu preventivních programů zvolit, aby žáky zaujala.

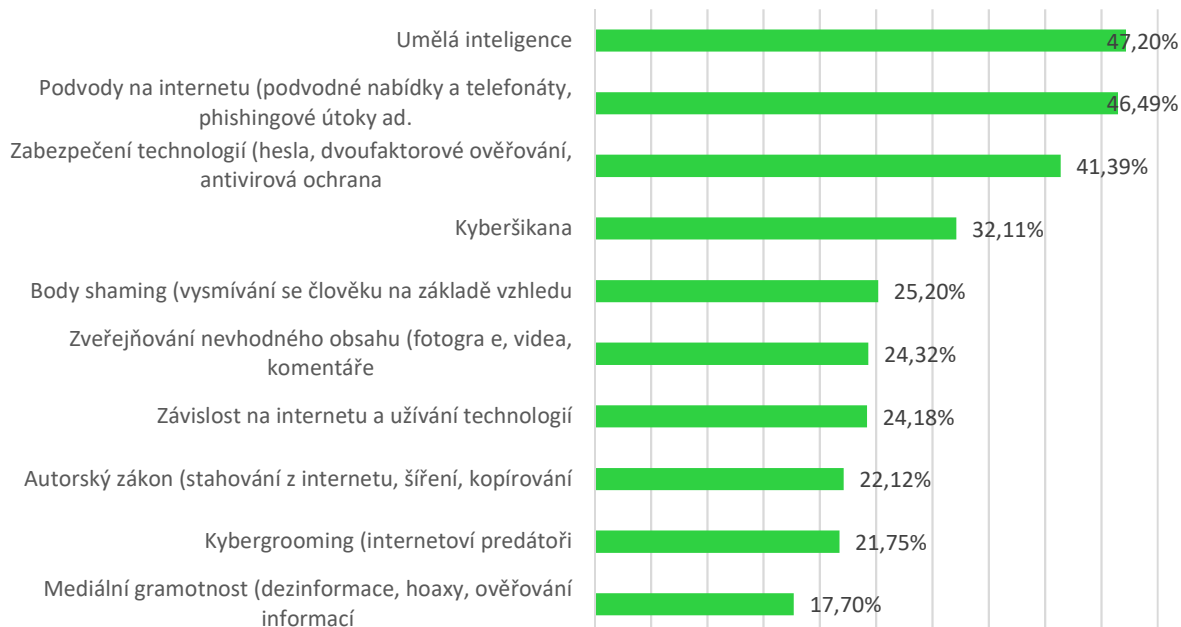
Procentuální rozdíl jednotlivých odpovědí byl mezi kraji výrazný, ale pořadí jednotlivých odpovědí se neměnilo. Nejčastěji žáci získávají informace od učitelů, celkově 74,81 %, na druhém místě jsou pak policisté, celkově 17,57 %, následované odpovědí „ano, ale nevím od koho“ 17,34 %. Otázka byla částečně otevřená, nejčastěji byla doplňována možnost „od rodičů“. Součet odpovědí je více než 100%, protože bylo možné vybrat více odpovědí. Toto rozložení odpovědí je shodné, jako ve výzkumu realizovaném v roce 2018.

Z rozdílů mezi kraji je největší rozptyl u odpovědi „Ano, informace máme od policistů, kteří byli ve škole.“ V Praze tuto možnost zvolilo 31,2% žáků, v Karlovarském kraji 24,42% a v Kraji Vysočina 23,36%. Nejméně tuto možnost zvolili žáci v Pardubickém kraji a to 11,67%.



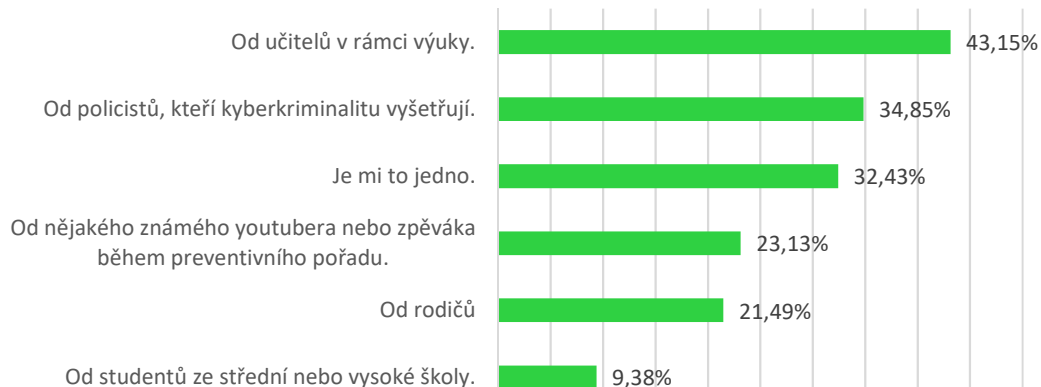
Na otázku, o jaká témata z oblasti bezpečného chování v kyberprostoru mají žáci zájem, nejvíce z nich odpovědělo, že o téma umělé inteligence (47,2%), následovně podvody na internetu (46,49%) a zabezpečování technologií (41,39%). Nejméně mají žáci zájem o téma mediální gramotnosti (17,7%). Při porovnání odpovědí mezi kraji nebyl v odpovědích výrazný rozptyl, pohyboval se v jednotkách procent.

O jakých tématech by ses rád v rámci bezpečného chování na internetu dověděl/a více?



Žáci by nejraději informace o kyberkriminalitě a bezpečném chování na internetu slyšeli od svých učitelů v rámci výuky (43,15%), na druhém místě od policistů, kteří se kyberkriminalitě věnují (34,85%), následované odpovědí „Je mi to jedno“ (32,43%). Při porovnání odpovědí mezi kraji byl procentuální vyjádření v odpovědích rozptýl, pořadí odpovědí se však neměnilo.

Od koho bys rád slyšel/a informace o kyberkriminalitě a bezpečném chování na internetu?



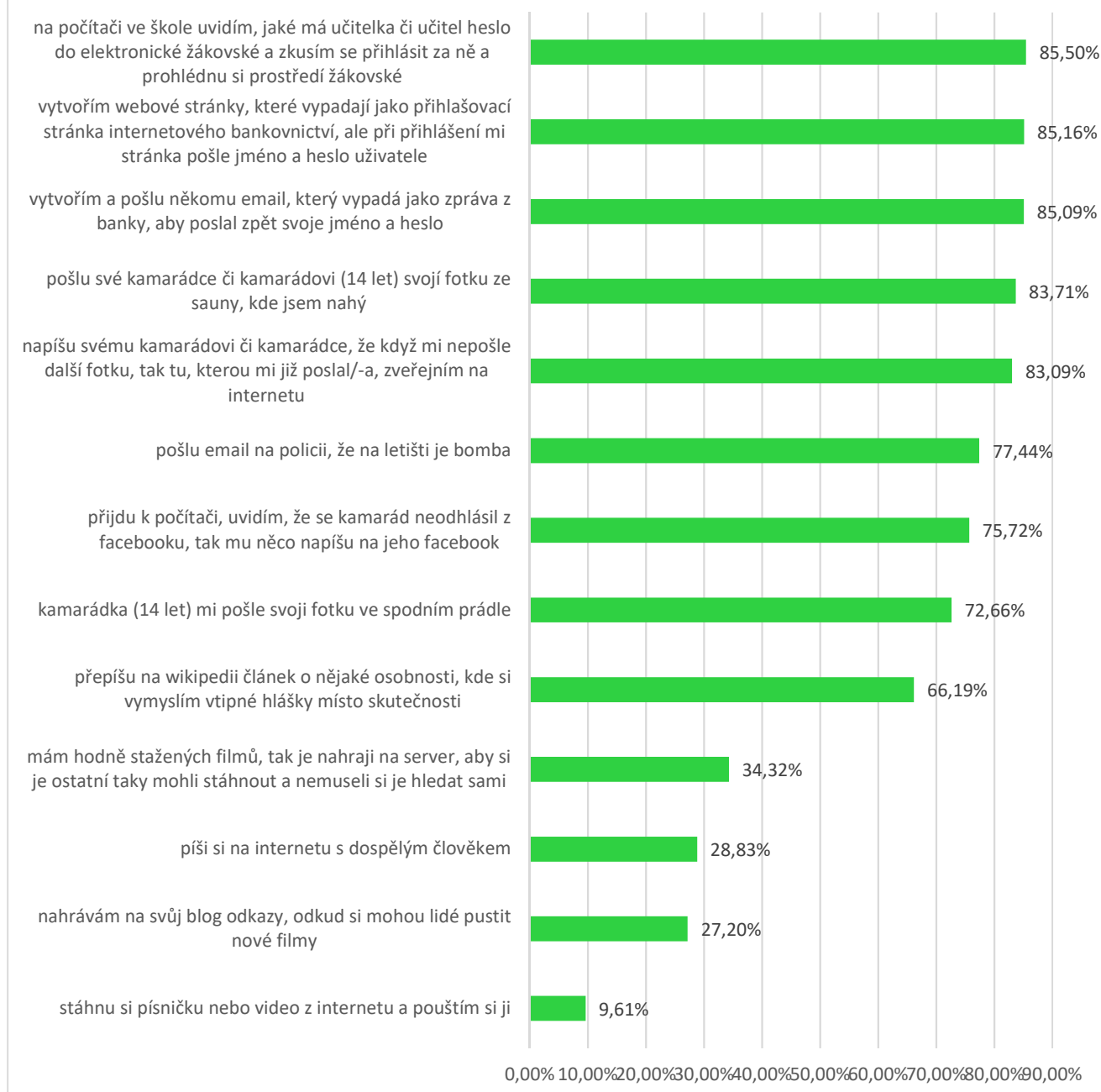
4.3. Znalost kyberkriminality

Ve druhé části dotazníku byla zjišťována znalost kyberkriminality u žáků. V první otázce žáci vybírali z nabídnutých možností, jaké jednání je podle nich kyberkriminalita, tedy, co se nesmí na internetu dělat. Otázka byla oproti předchozímu výzkumu zkrácena, aby žáci vybírali z méně možností, a byla lehce přeformulována. Na výběr bylo 36 možností, ve kterých byly příklady jak legálních, tak nelegálních činností. Jednotlivé druhy kyberkriminality byly uvedeny ve více možnostech.

Výsledky mezi jednotlivými kraji se výrazně nelišily, rozptyl výsledků mezi kraji se pohyboval do pěti procent. Nejvíce se lišily odpovědi u kraje Libereckého, kde žáci, s výjimkou odpovědi „stáhnu si písničku nebo video z internetu a pouštím si ji“, u všech odpovědí dali od 1% do 6% více kladných odpovědí, tedy že dané jednání je kyberkriminalitou. V porovnání s rokem 2018 došlo v jednotlivých projevech kyberkriminality k mírnému nárůstu kladných odpovědí, a to o jednotky procent. Výjimkou je zasílání fotografií nezletilých, kde toto jednání jako kyberkriminalitu označilo téměř o deset procent více žáků.

Nejvíce žáků označilo jako kyberkriminalitu „na počítači ve škole uvidím, jaké má učitelka či učitel heslo do elektronické žákovské a zkusím se přihlásit za ně a prohlédnu si prostředí žákovské“. Průměrně to bylo 85,5% žáků. Dále příklady phishingu, „vytvořím webové stránky, které vypadají jako přihlašovací stránka internetového bankovníctví, ale při přihlášení mi stránka pošle jméno a heslo uživatele“ (85,16%) a „vytvořím a pošlu někomu email, který vypadá jako zpráva z banky, aby poslal zpět svoje jméno a heslo“ (85,09%). Největší rozptyl byl u otázek týkajících se případů kyberkriminality neoprávněného přístupu k počítačovému systému. Odpovědi se pohybovaly od 85,50% u „na počítači ve škole uvidím, jaké má učitelka či učitel heslo do elektronické žákovské a zkusím se přihlásit za ně a prohlédnu si prostředí žákovské“ až po 66,06% u „zjistím si heslo k blogu kamaráda a na jeho blog nahraju za něj nějaké vtipné hlášky“. Odpovědi se lišily podle jednání, které odpověď nabízela. Žáci pravděpodobně rozlišují jednotlivé aktivity dle závažnosti jednání, přestože každý případ neoprávněného přístupu k počítačovému systému je trestný.

Výběr označ kyberkriminalitu

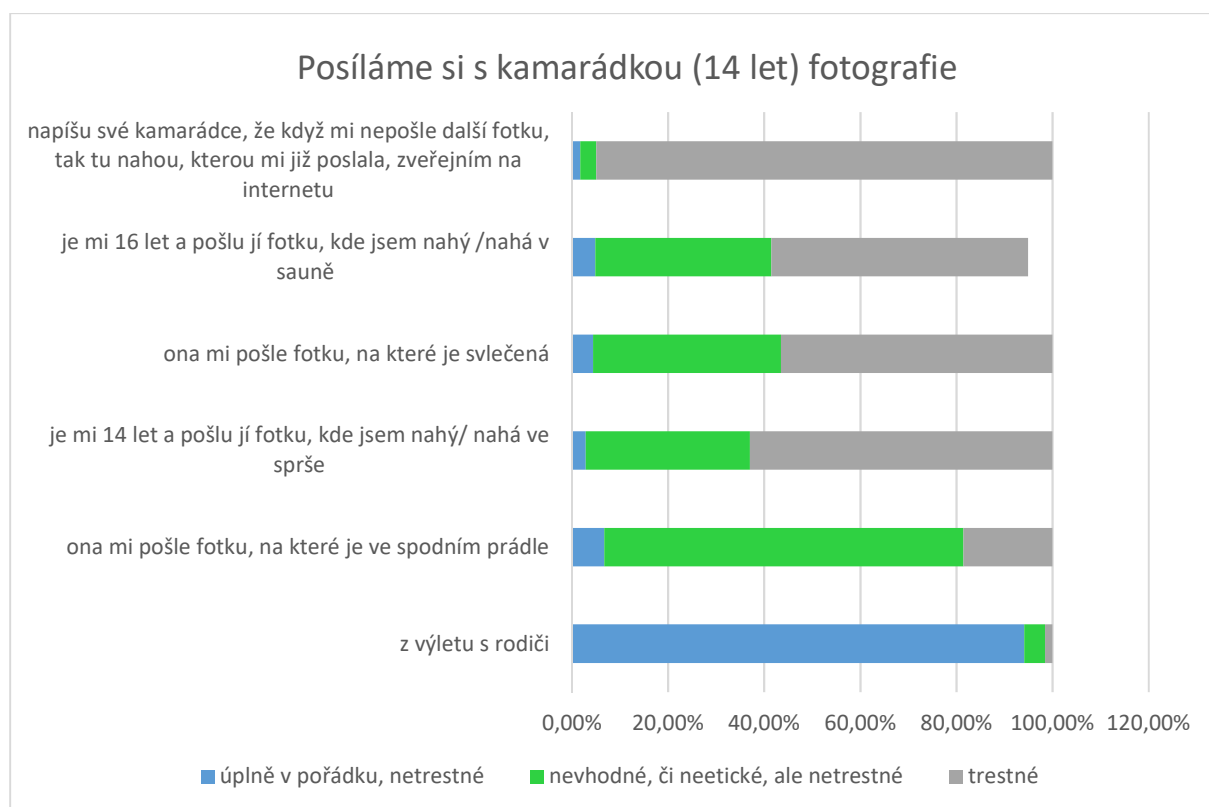


Třetí část dotazníku byla zaměřena na zjištění, kde mají žáci hranici, jaké jednání je dle jejich názoru ještě v kyberprostoru přijatelné a co již ne. Z výběru otázek žáci označovali, jak je jednání, dle jejich názoru, závažné. Byla zvolena čtyřbodová škála, od 1 – „úplně v pořádku, netrestné,“ 2 – „nevhodné či neetické, ale stále netrestné,“ 3 – „trestné“. V původním dotazníku z roku 2018 byla možnost trestné rozlišena na 3 – „trestné, ale tolerováno“ až po 4 – „trestné, nepřijatelné“, ale po připomínkách ze strany krajských koordinátorů o nevhodnosti možnosti, ve které by si žáci mohli myslet, že jednání je sice trestné, ale tolerováno, byly tyto možnosti sloučeny.

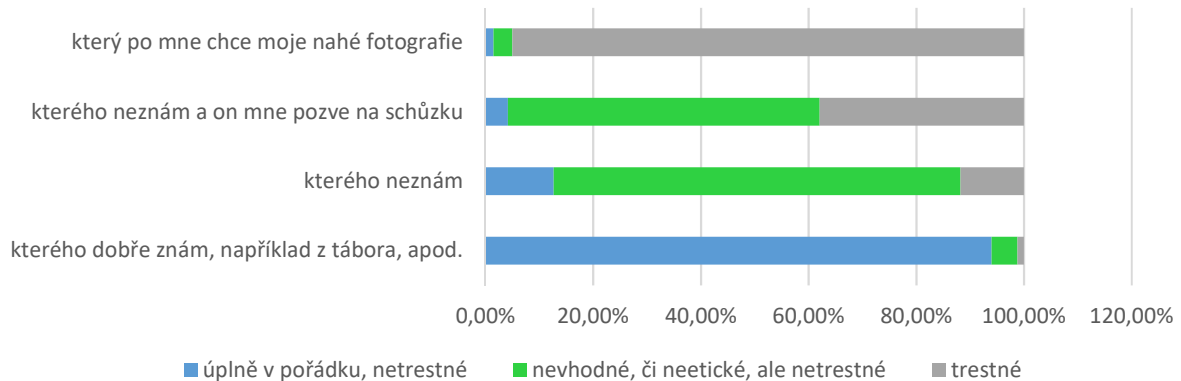
Pro tuto část byly zvoleny boxy otázek týkajících se zasílání fotografií, internetové komunikace s cizí osobou, neoprávněných přístupů k blogu, a nahrávání videa na internet. V možnostech byly uvedeny příklady jak zcela legálních jednání, tak jednání trestných.

Z výsledků je patrné, že žáci mají velice malé povědomí o tom, jaké jednání je trestné a jaké není, ani o rizikovosti dalších jevů. Například možnost „posíláme si fotografie s kamarádkou (14 let) a ona mi pošle fotografii, kde je svlečená“ označilo jako trestné pouze 56,48% žáků, 36,58% žáků označilo, že jednání je nevhodné, ale není trestné.

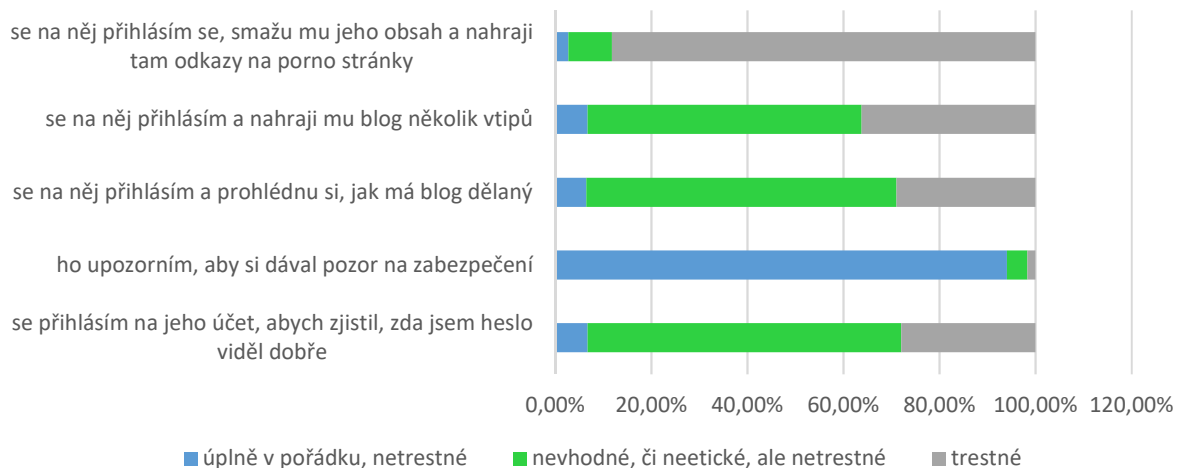
Rozdíly mezi kraji byly minimální, odchylka od průměru se pohybovala v nižších jednotkách procent. Výsledky z roku 2023 a 2018 nelze úplně porovnat, protože se změnila možnosti odpovědí. Pokud sloučíme skupiny 3 a 4 z původního dotazníku, tak u některých odpovědí je rozdíl přes 20%.



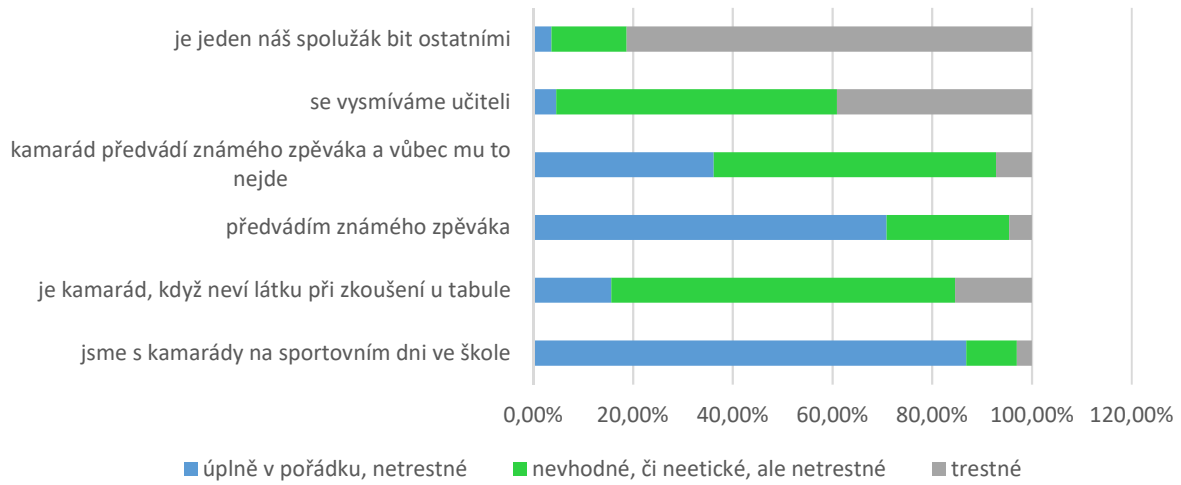
Na internetu si se mnou píše dospělý



Uvidím, jaké má kamarád/-ka heslo na svůj blog, takže



Umístím na internet video, na kterém

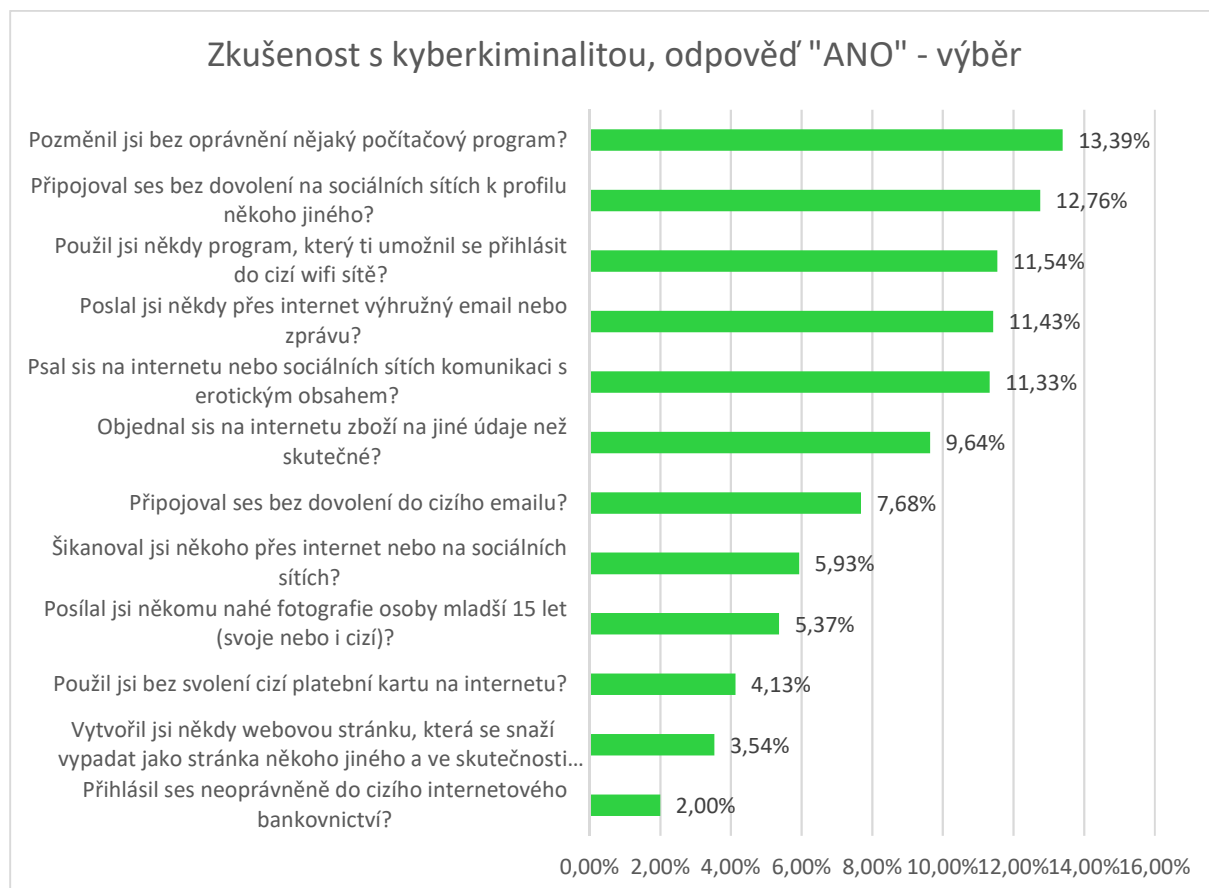


4.4. Zkušenost s kyberkriminalitou

Poslední část dotazníku obsahovala dichotomické otázky, pomocí kterých bylo zjišťováno, zda žáci mají zkušenosti s kyberkriminalitou či dalšími rizikovými jevy na internetu.

Nejrozšířenějšími druhy kyberkriminality, které žáci přiznali, že někdy dělali nebo zkoušeli, bylo porušování autorských práv 13,39% u odpovědi „Pozměnil jsi bez oprávnění nějaký počítačový program“, respektive 9,4% „Nahráváš staženou hudbu na internet, nebo tam nahráváš odkazy, odkud je lze stáhnout“. Dále následoval neoprávněný přístupem k počítačovému systému 12,76% „Připojoval ses bez dovolení na sociálních sítích k profilu někoho jiného“, respektive 11,54% „Použil jsi někdy program, který ti umožnil se přihlásit do cizí Wi-Fi sítě.“ Z dalších rizikových chování uvedli respondenti nejčastěji vyhrožování po internetu ve 11,43% a sexting v 11,33%.

Odpovědi na otázky v poslední části dotazníkového šetření měly z celého dotazníku nejmenší rozptyl mezi kraji. U většiny odpovědí byl rozptyl odpovědí od celkových výsledků do 1%. Pokud porovnáme aktuální výsledky z roku 2023 s výsledky z roku 2018, je zde patrný lehký nárůst jednání, které žáci přiznávají. Nejvíce u odpovědi „Pozměnil jsi bez oprávnění nějaký počítačový program?“, 5%, u dalších jednání je nárůst od 0% do 3%. Jediný výraznější pokles je u možnosti „Použil jsi někdy program, který ti umožnil se přihlásit do cizí wifi sítě?“, a to 3,68%.



5. Shrnutí výzkumu

Náš výzkum se zaměřil na znalosti žáků druhého stupně základních škol problematiky kyberkriminality a toho, jakého jednání se sami na internetu dopouštějí. Žáci jsou v prostředí kyberprostoru stále aktivnější, zejména na sociálních sítích. Pouze 1% respondentů uvedlo, že neužívá sociální síť. Jako nejužívanější sociální sítě uvedli WhatsApp, na kterém má svůj účet přes 90% respondentů, následovanými sítí Youtube (87%) a Instagram (77%).

Co se týká znalostí, jaké jednání je v kyberprostoru trestné, žáci měli nejnižší znalost týkající se problematiky porušování autorských práv, kde sdílení filmů označilo jako trestné jen 34% žáků. Nejvíce žáků označilo jako kyberkriminalitu příklady neoprávněného přístupu k počítačovému systému (přes 85%) a phishingový útok (také přes 85%). Ve srovnání s výsledky výzkumu z roku 2018 stoupla znalost žáků, jaké jednání je v kyberprostoru trestné o jednotky procent, s výjimkou zasílání fotografií nezletilých osob, kde příklady tohoto jednání označilo jako trestné téměř o 10% více žáků než u výzkumu v roce 2018.

Na otázku, jakého závadového jednání se žáci na internetu dopustili, mělo nejčastější zastoupení porušování autorských práv, konkrétně crackování (přes 13%), následované neoprávněným přístupem k počítačovému systému, konkrétně neoprávněným přístupem k sociálním sítím jiné osoby (téměř 13%). Následovalo vyhrožování přes internet a zasílání komunikace s erotickým obsahem (přes 11%). Ve srovnání s výsledky výzkumu z roku 2018 stoupla zkušenost žáků s příklady jednání, které by mohlo být kyberkriminalitou od 1 do 6%.

Výzkum zjišťoval také, jaké informace o kyberbezpečnosti žáky zajímají a od koho by je rádi slyšeli. Žáci uvedli, že by tyto informace slyšeli nejraději od svých učitelů v rámci výuky (přes 43%) následované odpovědí od policistů, kteří kyberkriminalitu vyšetřují (téměř 35%). Nejvíce měli zájem o téma umělé inteligence (přes 47%) a podvodů na internetu (přes 46%).

6. Závěr

Z výsledků výzkumu vyplývá, že žáci nejsou jen oběti, ale i potenciální pachatelé kyberkriminality a je potřeba tomu vhodně upravit preventivní působení. V současné době probíhá změna rámcových vzdělávacích programů a bylo by vhodné do výuky zařadit časovou dotaci a výše zmíněná témata, aby se problematice bezpečného používání informačních a komunikačních technologií v kyberprostoru mohli učitelé plnohodnotně věnovat v rámci výuky, tak jako se věnují od první třídy výuce matematiky nebo češtiny. V této souvislosti by muselo dojít taktéž k průběžnému odbornému vzdělávání pedagogů, aby byli v těchto oblastech dostatečně vzděláni.

Sami žáci uvedli, že by tyto informace nejraději dostali od pedagogů. Je škoda nevyužít tohoto preferovaného komunikačního kanálu. Další subjekt, který by bylo vhodné více do preventivní činnosti zapojit, je sama policie (Policie ČR). Současný stav, kdy jsou spojené funkce tiskového a preventivního pracovníka na krajském ředitelství policie, je nevyhovující, policie tím na prevenci nemá dostatečné personální kapacity. Žáci sami by dle výsledků průzkumu informace od policie uvítali, neboť policii vnímají jako atraktivní prvek, a je tudíž škoda tohoto potenciálu nevyužít. Větší zapojení policistů do prevence prováděné na školách by mohlo také pomoci budovat pozitivní důvěru a vztah budoucí generace k policejnímu sboru a autoritám obecně.

7. Literatura

- Strategie prevence kriminality v České republice na léta 2022 až 2027 schválená 6.4.2022 dostupné z <https://www.mvcr.cz/clanek/strategie-prevence-kriminality-v-ceske-republice-na-leta-2022-az-2027.aspx>
- Národní strategie primární prevence rizikového chování dětí a mládeže na období 2019 – 2027 dostupné z https://www.msmt.cz/uploads/narodni_strategie_primarni_prevence_2019_27.pdf
- AMI digital index 2022 dostupné z <https://amidigital.cz/wp-content/uploads/2022/08/ami-digital-index-2022.pdf>
- AMI digital index 2023 (tahák) dostupné z <https://amidigital.cz/wp-content/uploads/2023/05/tahak-3.pdf>
- Děti a kult krásy v on-line světě
Kamil Kopecký, René Szotkowski, Jana Kvintová, Lucie Křeménková, Dominik Voráč
Univerzita Palackého v Olomouci, 2022
dostupné z <https://e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/155-deti-a-kult-krasy-v-online-svete-2022/file>
- Vnímání kyberkriminality mezi dětmi (výzkumná zpráva)
Projekt Kraje pro bezpečný internet
Jihlava, 2018
dostupné z https://www.kpbi.cz/prilohy/157_vyzkum_final.pdf

8. O realizátorech

Projekt Kraje pro bezpečný internet

Projekt Kraje pro bezpečný internet je realizován pod záštitou Asociace krajů ČR. Do projektu je zapojeno 14 krajů ČR. Partnery projektu jsou sdružení CZ.NIC, Policie ČR a společnosti Microsoft a Gordic. Hlavním cílem projektu je zvýšit informovanost o rizicích internetu a možnostech prevence a pomoci v oblasti bezpečného užívání IT technologií. Cílovými skupinami projektu jsou děti a mládež, rodiče, pedagogové, sociální pracovníci, policisté, úředníci a senioři. V rámci projektu byly pro jednotlivé cílové skupiny připraveny e-learningové lekce či krátké videospoty (pro seniory, děti a mládež, rodiče) nebo podcasty, které jsou zdarma a volně dostupné na www.KPBI.cz. E-learningové kurzy pro vybrané cílové skupiny jsou dále doplněny o prezenční semináře. Každoročně jsou v rámci projektu KPBI organizovány konference pro odbornou veřejnost, zástupce krajů či policie.

pplk. Ing. Mgr. Tomáš Daňhelka

rada, Úřad služby kriminální policie a vyšetřování

V době covidové pandemie si děti zvykly trávit větší množství času v kyberprostoru, hlavně na sociálních sítích. Kyberprostor však před ně klade množství nástrah, ale i lákadel. Naštěstí se bezpečnému chování v kyberprostoru věnuje velké množství preventivních programů ať již na školách, tak přímo na sociálních sítích. Osobně se domnívám, že prevence je důležitá a sám jsem se na preventivních aktivitách ve své práci i mimo ní podílel. Za svých více jak 17 let praxe u policie jsem se však setkával i s tím, že děti nejsou jen oběti, ale i pachatelé, zvláště v oblasti kybernetické kriminality.

Ve spolupráci s projektem Kraje pro bezpečný internet jsme se tomuto tématu zkusili věnovat více a v roce 2018 se nám podařilo realizovat výzkum Vnímání kyberkriminality mezi dětmi, jehož se zúčastnilo přes 50 000 žáků základních škol. Ve výzkumu jsme zjišťovali, co si žáci myslí, že se v kyberprostoru může a nemůže dělat a jakého závadového jednání se sami dopouštějí. V roce 2023 jsme se výzkum rozhodli zopakovat a zjistit, jak se od minulého výzkumu změnilo chování a znalosti žáků. Doufám, že výsledky pomohou lépe zaměřit a zacílit prevenci kyberkriminality na základních školách.

9. Kontakty na realizátory

Ing. Lucie Časarová, vedoucí projektu Kraje pro bezpečný internet, Krajský úřad Kraje Vysočina, 721 947 046, casarova.l@kr-vysocina.cz

pplk. Ing. Mgr. Tomáš Daňhelka, Úřad služby kriminální policie a vyšetřování, tomas.danhelka@pcr.cz