UNIVERZITA PALACKÉHO V OLOMOUCI

PEDAGOGICKÁ FAKULTA

Katedra technické a informační výchovy

Bakalářská práce

Jana Nejezchlebová

Bezpečnost v digitální gramotnosti

Olomouc 2025

vedoucí práce: prof. Ing. Čestmír Serafín, Dr.

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracovala samostatně a uvedla jsem v ní veškerou literaturu a ostatní informační zdroje, které jsem použila.

V Olomouci dne 19.6.2025 …….

vlastnoruční podpis

Poděkování

Chtěla bych poděkovat mému vedoucímu práce, prof. Ing. Čestmíru Serafínovi, Dr., za vstřícný přístup, odborné vedení a trpělivost během celého procesu psaní bakalářské práce.

Taká velké díky patří celé mé rodině a partnerovi za trpělivost a rady při psaní této práce a za neustálou podporu během celého studia.

Dále děkuji členům mého skautského střediska, kteří mi umožnili provést výzkumné šetření ve vlastních řadách a ochotně mi vyšli vstříc při realizaci výzkumu.

Jana Nejezchlebová

Obsah

Úvod

Bezpečnost v digitálním světě je téma, které se ve vzdělávání začíná teprve postupně prosazovat. Ačkoli se digitální technologie staly běžnou součástí každodenního života, společnost včetně školství, se s důsledky jejich používání stále učí pracovat. V posledních letech jsme začali systematicky rozvíjet výuku digitální gramotnosti. Na školách se už neučí jen jak ovládat počítač, ale vyučujeme soubor kompetencí pro bezpečné, efektivní a odpovědné fungování v online prostředí.

Společně s vývojem digitálního světa se proměňují i formy možných hrozeb a problémů. Útočníci využívají stále sofistikovanější techniky a s rozvojem umělé inteligence se zvyšuje i obtížnost rozeznání manipulace či podvodu. Proto se stává důležitější než kdy dřív nejen výuka technických aspektů bezpečnosti, ale také důraz na rozvoj kritického myšlení. Žák by měl být schopen hodnotit věrohodnost informací, ověřovat si zdroje a chápat dopad vlastního chování v digitálním prostoru včetně toho, co sdílí a komentuje.

Ve své bakalářské práci se věnuji bezpečnosti v digitální gramotnosti. Toto téma jsem si zvolila, protože mě dlouhodobě zajímá a považuji ho za jednu z nejdůležitějších kompetencí potřebných pro kvalitní život v bezpečí. Bez potřebných znalostí je totiž velmi snadné spadnout do pasti podvodníků, či celých organizovaných skupin.

Práce je primárně zaměřila na žáky druhého stupně základních škol. Zvolila jsem tuto cílovou skupinu z důvodu mé aprobace (učitelství pro 2. stupeň ZŠ), a také protože právě v tomto věku je důležité budovat základy bezpečného online chování.

Cílem práce je zjistit, jak žáci vnímají a zvládají vybrané aspekty bezpečnosti v digitální světě specifikované v Rámcovém vzdělávacím programu. Konkrétně ochranu osobních údajů, používání hesel, rozpoznání rizikového chování, reakce na nevhodné situace, ověřování informací a uvědomění si důsledků vlastního chování online. Také podpořit prevenci a vzdělávání v oblasti digitální gramotnosti s důrazem na bezpečné a odpovědné chování žáků v online prostředí. Dalším cílem je vytvořit dotazníkové šetření, získat potřebná data od respondentů a interpretovat výsledky.

Tato bakalářská práce je koncepčně rozdělena na teoretickou a praktickou část. V teoretické části je vymezen pojem digitální gramotnost a její vývoj v kontextu vzdělávání. Dále je zde popsán rámec digitálních kompetencí DigComp 2.2, uvádím hlavní digitální hrozby (např. phishing, malware, sociální inženýrství, kyberšikana) a zaměřuji se na specifika rizik u dětí. V této části také naleznete přehled kurikulárních dokumentů, zejména Rámcovému vzdělávacímu programu pro základní vzdělávání a zásady prevence rizikového chování.

Praktická část je postavena na kvantitativním výzkumu, který probíhal formou dotazníkového šetření mezi 62 žáky 6.–9. tříd. Dotazník byl sestaven tak, aby pokryl klíčové oblasti vycházejících z RVP ZV. Naleznete zde interpretovaná data s důrazem na odhalení nejslabších míst a vyvození praktických doporučení.

1 Digitální gramotnost

Digitální gramotnost dnes patří mezi klíčová témata nejen v oblasti vzdělávání. Její potřeba je protkána do celé společnosti a schopnosti. S rostoucí mírou digitalizace je důležité, abychom byli schopni porozumět tomu, jak se v digitálním světě bezpečně, efektivně a zodpovědně pohybovat.

Není to jen o otázce technických dovedností práce s počítačem, jde i o způsob přemýšlení, rozhodování a ochrany sebe a svých dat. Bez alespoň základní úrovně digitální gramotnosti se dnes jedinec jen těžko orientuje, jak na pracovním trhu, tak i v každodenním běžném životě. Digitálně negramotný člověk naráží na problémy v mnoha oblastech. Ať už se jedná o komunikaci s úřady prostřednictvím eGovernmentu, či správa financí a komunikace s bankou. Velkým problémem může být zhoršený přístup ke zdravotní péči, kvůli digitalizaci zdravotnictví.

Než se však posuneme k rizikům a možnostem ochrany v digitálním světě, kterými se tato práce zabývá, je nutné si nejprve ujasnit, co vlastně digitální gramotnost znamená.

1.1 Vymezení pojmu digitální gramotnost a počítačová gramotnost

Význam pojmu gramotnost je obecně přijímán jako schopnost číst, psát a počítat. Burďák (2016) však pojem rozšiřuje a chápe jej jako „základní úroveň vědomostí, dovedností a postojů v určité oblasti poznání“ (s. 15). Toto širší pojetí nám tak umožnuje, přesněji definovat pojem digitální gramotnost.

Definice digitální gramotnosti není sjednocená a různé zdroje ji definují odlišně. Proto níže uvádím několik příkladů jejích definic.

Například podle Národního ústavu pro vzdělávání (2011) je digitální gramotnost chápána jako kombinace znalostí, dovedností, postojů a hodnot, díky nimž mohou jednotlivci digitální technologie používat nejen efektivně a bezpečně, ale také s jistotou, kritickým odstupem a tvůrčím přístupem. Tyto schopnosti uplatňují v profesním životě, při vzdělávání, ve volnočasových aktivitách i v rámci aktivního zapojení do společnosti.

Současné pojetí digitální gramotnosti, jak jej představuje evropský rámec DigComp 2.2, klade důraz na ještě širší spektrum kompetencí. Digitální gramotnost podle tohoto přístupu nespočívá pouze ve schopnosti používat počítač, ale zahrnuje i porozumění digitálním technologiím, kritické zhodnocení jejich obsahu a bezpečné i eticky odpovědné jednání v digitálním prostoru. Vzhledem k rychlému vývoji společnosti je digitální gramotnost

považována za jednu z nejzásadnějších kompetencí, které by měl každý občan ovládat (Joint Research Centre, 2022).

Z výše uvedených definic vyplývá, že digitální gramotnost neznamená jen schopnost používat počítač. Jedná se o komplexní soubor znalostí, dovedností, postojů a hodnot, který má široký společenský význam ve vzdělávání, profesním životě, volném čase i v rámci občanského zapojení do společnosti. Digitální gramotnost je nezbytnou kompetencí pro fungování v současné digitální společnosti a vzhledem k neustálému technologickému pokroku, se vyvíjí společně s celou společností.

Oproti tomu pojem počítačová gramotnost, který byl běžně používán v dřívější odborné literatuře, má užší význam. Definujeme jej jako soubor vědomostí o možnostech a schopnostech počítačů, jejich sítí a celkovém programovatelném vybavení, která pomohou jedinci efektivně použít počítačové technologie ve školním prostředí. Na rozdíl od digitální gramotnosti však nezahrnuje širší aspekty, jako je kritické myšlení, bezpečnost, etika či aktivní účast v digitálním prostoru, proto je často uváděn jako pojem podřazený pojmu digitální gramotnost. (Průcha, Walterová, & Mareš, 2009)

Ve veřejném prostoru se však často setkáváme se zaměňováním těchto pojmů. Nejčastěji k tomu dochází tehdy, kdy je digitální gramotnost mylně ztotožňována pouze s ovládáním počítače a základních aplikací. Takové pojetí však vede k okleštění celého oboru pouze na technické dovednosti. Opomíjí další klíčové oblasti, jako je kritické myšlení, bezpečné a etické chování v online prostředí, či schopnost aktivně fungovat v digitální společnosti. Zaměňování těchto pojmů není problémem pouze školství – jedná se o celospolečenský jev, který brání hlubšímu porozumění tomu, co vše digitální gramotnost skutečně obnáší.

1.2 Vývoj digitální gramotnosti

Rozvoj digitální gramotnosti se ve školství v České republice začal významněji projevovat až v 90. letech 20. století. Zatímco v zahraničí docházelo k intenzivnímu nasazování digitálních nástrojů již dříve, v Česku byl postup začleňování digitálních technologií pozvolný a zpočátku závisel především na iniciativě jednotlivých pedagogů a fyzickému vybavení škol. (Burďák, 2016)

Teprve postupem času začal stát vytvářet strategické dokumenty, které měly za cíl podporovat rozvoj digitálních kompetencí v rámci celého vzdělávacího systému. Mezi první systematické kroky patřila Strategie digitální gramotnosti ČR pro období 2015–2020, jež definovala základní směry podpory v této oblasti. Na ni navázala Strategie vzdělávací politiky

ČR do roku 2030+, která reflektuje aktuální proměny společnosti a potřebu přizpůsobit školství novým digitálním požadavkům.

Obě strategie zdůrazňují například důležitost dostupnosti digitálních technologií, kvalitní infrastruktury ve školách a také podpory pedagogů v oblasti metod a digitálního vzdělávání. Jejich společným cílem je připravit žáky na aktivní a bezpečné fungování v digitálně propojeném světě, v němž je vedle technických dovedností klíčové také kritické myšlení a schopnost zodpovědně nakládat s informacemi (Burďák, 2016).

Digitální gramotnost není důležitá pouze ve školním prostředí, ale stává se klíčovou kompetencí napříč celou společností.

První ucelené úvahy o významu digitální gramotnosti se objevují již na konci 90. let. Významný vliv měl v tomto ohledu americký autor Paul Gilster, který ve své knize *Digital Literacy* (1997) popsal digitální gramotnost jako schopnost kriticky pracovat s informacemi v online prostředí. Gilster přitom zdůrazňuje, že pouhé technické dovednosti nestačí – digitálně gramotný člověk by měl být schopen informace vyhledávat, hodnotit a odpovědně s nimi zacházet. Tento přístup se stal základním kamenem pozdějších strategií digitálního vzdělávání v řadě zemí a postupně se promítl i do evropských a národních vzdělávacích politik. (Polák, 2022)

Na evropské úrovni představovala významný impuls iniciativa eEurope, která byla spuštěna v roce 2000. Jejím cílem bylo zajistit, aby Evropská unie plně využila potenciál nových technologií a připravila občany na život v digitální společnosti. V rámci této strategie se kladl důraz nejen na zavádění technologií do škol, ale i na rozvoj digitálních dovedností obyvatelstva napříč věkovými a sociálními skupinami. eEurope podporovala přístup ke vzdělávacím zdrojům, internetovému připojení i školení pedagogů, přičemž konečným cílem bylo, aby se digitální gramotnost stala běžnou součástí všeobecného vzdělání. Tento přístup se později stal inspirací i pro domácí digitální politiku v České republice. (Polák, 2022)

1.3 Digitální kompetence a jejich rámce

Jak už bylo zmíněno v předchozím textu, digitální gramotnost se neustále vyvíjí, tak jako digitální technologie a potřeby společnosti. Více se specifikuje a zaměřuje na jednotlivé oblasti. Postupně se zpřesňuje a rozšiřuje o nové oblasti. To přináší i nutnost lépe vymezit, co všechno digitální gramotnost zahrnuje a podle jakých kritérií můžeme posoudit, zda je jedinec digitálně gramotný. Právě k tomuto účelu slouží koncept digitálních kompetencí.

Pojem kompetence je v pedagogickém kontextu definován jako „schopnost a způsobilost úspěšně zvládnout nějakou činnost a řešit určité úkoly, zejména v pracovním životě a dalších životních situacích“ (Průcha, Walterová & Mareš, 2009).

Digitální kompetence nám tak pomáhají popsat jaké konkrétní znalosti, dovednosti a postoje by měl jedinec zvládat, aby mohl efektivně využívat digitální technologie. Slouží nám tedy jako rámec, podle kterého můžeme vyhodnotit úroveň digitální gramotnosti jednotlivce a plánovat rozvoj ve vzdělávání.

V následující části se zaměřím na konkrétní přístupy k vymezování digitálních kompetencí. Hlavní pozornost věnuji evropskému rámci DigComp, který představuje jeden z nejrozšířenějších a nejuznávanějších modelů.

1.3.1 DigComp 2.2

Jedním z nejvýznamnějších nástrojů, který nám umožňuje podrobněji porozumět tomu, co digitální kompetence obnáší, je evropský rámec digitálních kompetencí pro občany – DigComp. Tento rámec vznikl na popud rostoucí potřebě definovat a strukturovat dovednosti, nezbytné pro plnohodnotné fungování jednotlivce v digitálním prostředí. Nabízí jednotný a srozumitelný systém, jenž rozděluje digitální kompetence do tematických oblastí a konkrétních dovedností. Usnadňuje jejich rozvoj, hodnocení i začlenění do vzdělávacích programů.

DigComp slouží jako orientační mapa, která pomáhá jednotlivcům, školám i institucím pojmenovat konkrétní znalosti, schopnosti a postoje potřebné pro digitální začlenění. Nejde o pevně daný učební plán, ale o flexibilní rámec, který lze přizpůsobit různým věkovým skupinám i kontextům – od základního vzdělávání přes profesní růst až po celoživotní učení. V tomto smyslu poskytuje základ pro pochopení toho, co znamená být digitálně gramotný.

Nejnovější verze tohoto rámce, DigComp 2.2, byla publikována v roce 2022 a dává nám konkrétní příklady, co by měl člověk digitálně gramotný zvládat (Joint Research Centre, 2022).

Digitální kompetence podle DigComp znamená „sebevědomé, kritické a odpovědné používání digitálních technologií pro účely učení, práce i aktivního zapojení do společnosti“. Obsahuje také témata jako mediální gramotnost, bezpečnost na internetu, schopnost tvořit obsah a orientovat se v informacích. (Joint Research Centre, 2022)

Rámec DigComp rozděluje digitální kompetence do pěti hlavních skupin:

Informační a datová gramotnost (Information and data literacy)

Tato oblast se zaměřuje na to, jak vyhledávat, hodnotit a spravovat informace. Patří sem například schopnost odlišit ověřené informace od nepravdivých (např. rozpoznání fake news), efektivně používat vyhledávače nebo porozumět základům práce s daty.

Komunikace a spolupráce (Communication and collaboration)

Zde jde o dovednosti související s komunikací prostřednictvím digitálních nástrojů. Zahrnuje schopnost bezpečně sdílet informace, dodržovat pravidla slušného chování na internetu, využívat e-maily, videohovory nebo online platformy pro spolupráci.

Tvorba digitálního obsahu (Digital content creation)

Tato kompetence vyjadřuje schopnost vytvořit a upravit digitální obsah. Nedílnou součástí je také znalost autorského práva a licencí.

Bezpečnost (Safety)

Kompetence týkající se ochrany zařízení, osobních údajů atd. Patří sem například používání silných hesel, antivirových programů, schopnost rozeznat podezřelé e-maily nebo prevence digitálního přetížení.

Řešení problémů (Problem solving)

V poslední oblasti se blíže specifikuje schopnost řešit technické potíže, učit se práce s novými digitálními nástroji nebo samostatně najít řešení problému.

Rámec DigComp slouží v Evropské unii jako hlavní kostrč stanovisku digitálních kompetencí. Slouží jako vodítko při tvorbě učebních plánů i vzdělávacích strategií a jeho prvky se promítají také do českého školství. (Joint Research Centre, 2022).

Obrázek 1 Pět oblastí digitálních kompetencí podle rámce DigComp 2.1 (Joint Research Centre, 2022)

2 Bezpečnost v digitální gramotnosti

V reálném světě je zajištění bezpečnosti úkolem státních bezpečnostních složek, jako je například policie. V digitálním prostředí je však situace složitější – pravomoci těchto institucí jsou omezené a možnosti efektivního zásahu jsou často nedostatečné. Útoky mohou být vedeny z druhého konce světa a dopadení anonymních nebo organizovaných skupin útočníků je značně obtížné.

Vzhledem k těmto omezením sehrává klíčovou roli v oblasti digitální bezpečnosti specializovaná státní instituce Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Tento úřad má na starosti ochranu kritické infrastruktury a vládních informačních systémů před kybernetickými útoky. Kromě toho poskytuje odbornou podporu organizacím a institucím, které usilují o zvýšení své úrovně kybernetické ochrany.

NÚKIB rovněž zajišťuje plnění evropské legislativy, konkrétně směrnice o bezpečnosti sítí a informačních systémů (NIS), v rámci České republiky. Tato směrnice ukládá vybraným odvětvím povinnost zavádět bezpečnostní opatření a hlásit závažné incidenty, které mohou ohrozit jejich provoz.

Úřad zároveň zastřešuje i oblast ochrany utajovaných skutečností a má na starosti koordinaci reakce státu na kybernetické hrozby, které mohou mít dopad na národní bezpečnost.

Nebezpečí se týká každého, kdo se v digitálním prostoru pohybuje. Každodenně dochází k útokům různého charakteru – od ohrožení bezpečnosti státu, přes napadení firemní infrastruktury, až po útoky na jednotlivce. Časté jsou také útoky na tzv. kritickou infrastrukturu, které bývají motivovány politickými nebo finančními zájmy. V České republice byly široce medializovány například kybernetické útoky na nemocnice.

Firmy a velké společnosti se každý den potýkají s různými formami kybernetických hrozeb, ať už jde o phishingové e-maily, útoky typu ransomware, nebo pokusy o průnik do jejich sítí (vysvětlením těchto pojmů se zabývám v další kapitole). Ohroženi však nejsou pouze velcí hráči, i běžní občané jsou denně vystaveni riziku podvodů a zneužití osobních údajů. Podle odhadů bank útočníci v České republice během posledního roku způsobili škody přesahující 1.39 miliardy korun, což představuje alarmující číslo a podtrhuje důležitost prevence a digitální gramotnosti zaměřené na bezpečnost. (Česká bankovní asociace, 2025)

Tyto rostoucí hrozby v digitálním prostředí ukazují, jak nezbytné je nejen technické zabezpečení systémů, ale také dostatečné povědomí a znalosti běžných uživatelů. Protože platí, že největší problém v zabezpečení systémů je uživatel. Právě schopnost orientovat se

v problematice bezpečnosti, chránit svá data a přistupovat k digitálním technologiím odpovědně, tvoří důležitou součást digitální gramotnosti.

Na druhou stranu v otázce finančních útoků se díky nástrojům pro odhalování podvodů, podařilo meziročně snížit škodu na jednoho člověka a celkově se bankám podařilo zachránit 7,95 miliardy korun. Což je úctyhodné číslo a reflektuje to velkou snahu českých bank. (Česká bankovní asociace, 2025)

Bezpečnost v digitální gramotnosti je jednou z pěti hlavních kompetencí digitální gramotnosti definovanou v evropském rámci DigComp 2.2.

Jedná se o 4. Oblast Bezpečnost (Safety), která se nadále člení na čtyři další kompetence

1. Ochrana zařízení (Protecting Devices)
2. Ochrana osobních údajů a soukromí (Protecting Personal Data and Privacy)
3. Ochrana zdraví a duševní pohody (Protecting Health and Well-being)
4. Ochrana životního prostředí (Protecting the Environment)

Každá z těchto kompetencí je v rámci DigComp dále rozpracována do osmi úrovní obtížnosti od základní orientace s podporou, přes samostatné rozhodování, až po expertní úroveň.

Tyto čtyři oblasti bezpečnostních kompetencí rámce DigComp nejsou důležité pouze pro odborníky, či dospělé uživatele digitálních technologií, ale hrají klíčovou roli také ve vzdělávání dětí. Právě u žáků základních škol je potřeba budovat základy bezpečného chování v digitálním prostředí co nejdříve. Děti jsou totiž velmi aktivními uživateli technologií, často však bez potřebného porozumění rizikům, která jim hrozí. (Joint Research Centre, 2022)

Z tohoto důvodu je význam digitální bezpečnosti ve vzdělávání na prvním i druhém stupni základní školy stále aktuálnější.

2.1 Význam digitální bezpečnosti pro žáky ZŠ

Začleňování témat souvisejících s digitální bezpečností do výuky je nezbytné už od nejmladších ročníků základní školy. Současná generace dětí vyrůstá v prostředí plném digitálních technologií, se kterými přichází do kontaktu velmi brzy – často dříve, než si vůbec osvojí základní principy bezpečného chování. Ačkoli jsou tyto děti často vnímány jako „digitálně zdatné“, jejich přirozené dovednosti se zpravidla vztahují pouze k technickému ovládání zařízení, nikoliv ke schopnosti rozpoznat rizikové situace nebo zodpovědně pracovat s informacemi. („Digitální vzdělávání zvyšuje bezpečnost“, 2024)

Zatímco v reálném světě bývají děti vedeny k opatrnosti dospělými – rodiči, pedagogy nebo jinými autoritami – v digitálním prostředí často chybí dostatečné vedení. Mnoho rodičů se v oblasti online bezpečnosti neorientuje, případně podceňuje rizika, která jejich dětem hrozí. O to větší zodpovědnost pak leží na školách, které by měly fungovat jako stabilní prvek v oblasti preventivní výchovy k digitální gramotnosti. („Digitální vzdělávání zvyšuje bezpečnost“, 2024)

Zároveň však nelze přehlédnout, že i pro samotné pedagogy je toto téma často nové a komplexní. Výuka digitální bezpečnosti vyžaduje nejen didaktickou, ale také technickou přípravu, schopnost reagovat na rychle se měnící prostředí a znalost vhodných nástrojů. Z tohoto důvodu je klíčové, aby učitelé měli k dispozici kvalitní oporu v kurikulárních dokumentech, metodikách a vzdělávacích materiálech. V českém prostředí lze vycházet například z rámcového vzdělávacího programu, dále existuje řada specializovaných iniciativ (např. e-Bezpečí, JSNS, NÚKIB), které poskytují výukové materiály, scénáře hodin i konkrétní příklady prevence.

Pokud žákům nebude poskytnuto dostatečné povědomí o hrozbách a dovednosti, jak se v digitálním prostředí bezpečně pohybovat, mohou následky sahat daleko za rámec školní docházky. Dlouhodobě může být ohrožen jejich duševní vývoj, mezilidské vztahy i schopnost bezpečně se zapojit do života společnosti.

Děti zpravidla neumí rizika samy rozpoznat, a to ani v případě, že jim byla základní pravidla sdělena. Důvěřivost, impulzivita a touha po sociálním uznání mohou snadno převážit nad obezřetností. Mladší žáci často vůbec netuší, co vše může být nebezpečné – od zasílání osobních údajů neznámým osobám, přes klikání na podezřelé odkazy a až po přebírání návyků z manipulativního obsahu na sociálních sítích.

Specifické hrozby se navíc liší podle věku – zatímco dospělí se nejčastěji stávají terčem finančně motivovaných útoků, děti a dospívající bývají častěji ohroženi například kyberšikanou, groomingem nebo citovým vydíráním. Nelze ale říct, že se tyto oblasti vzájemně nepropojují i děti mohou být zasaženy finančními podvody.

Naopak mohou dospívající svým porozuměním technologiím edukovat dospělé. Proto je výchova k digitální bezpečnosti základním předpokladem pro rozvoj kompetentních, sebevědomých a odpovědných digitálních občanů.

3 Hrozby v digitálním prostoru

Celkově hrozby v digitálním prostoru, kterým čelíme jako jednotlivci se netýkají jen ohrožení našich financí nebo ztráty dat. Rizika na sítích se mohou dotknout i našeho světonázoru a snadno můžeme podlehnout konspiračním teoriím nebo čistě manipulativním fake news.

Hrozby v digitálním prostoru, kterým čelí dospělí lidé, děti a mladiství se v některých aspektech liší a v některých se mohou překrývat. Je však třeba zmínit důležitost edukace dětí i proto, že nejsou jen nejsnadněji zranitelná skupina. Mají i sílu edukovat starší populaci, která si za mladší chodí často pro radu ohledně požívání digitálních technologií.

3.1 Hlavní typy hrozeb

3.1.1 Phishing

Phishingje jednou z nejrozšířenějších forem kybernetických útoků. Jejich cílem je získat citlivé údaje, jako přihlašovací údaje, čísla platebních karet a další osobní informace. Útočníci využívají manipulaci a důvěru obětí tím, že se vydávají za důvěryhodné osoby či instituce. Jedná se často o podvodné emaily, vypadající na první pohled jako pravé, které mají za účel vylákat z nás naše osobní údaje, např. přihlášení ke školním účtům nebo sociálním sítím. (NÚKIB, 2015)

3.1.2 Malware a ramsorware

Malware je obecné označení pro škodlivý software, jehož cílem je narušit, poškodit nebo zneužít počítačový systém. I když se nejedná o klasický počítačový virus, může způsobit značné škody. Některé typy malwaru se dokáží samy šířit a využívat napadené zařízení k dalším činnostem bez vědomí uživatele. Typickým příkladem je tzv. cryptojacking, kdy je zařízení zneužito k těžbě kryptoměn. (O2 Chytrá škola, n.d.)

Významným a zároveň velmi rizikovým typem malwaru je ransomware. Tento škodlivý software zablokuje přístup k systému nebo zašifruje jeho data a následně požaduje po uživateli zaplacení výkupného – nejčastěji v kryptoměně – výměnou za obnovení přístupu. Zásadním problémem zůstává, že ani po zaplacení výkupného nemusí dojít k odblokování systému. Ransomware tak představuje nejen technickou, ale i etickou a právní výzvu v oblasti digitální bezpečnosti.

Tyto typy škodlivého softwaru mohou ohrozit jakékoli zařízení připojené k internetu – včetně chytrých telefonů, tabletů nebo herních konzolí. Účinná prevence nespočívá pouze v používání antivirových a antimalwarových nástrojů, ale také v edukaci uživatelů a v jejich odpovědném chování při práci v digitálním prostředí. (ESET, n.d.)

3.1.3 Sociální inženýrství

Sociální inženýrství představuje formu psychologické manipulace, jejímž cílem je přimět konkrétní osobu nebo skupinu osob k neúmyslnému sdílení citlivých informací, nebo k provedení určité činnosti, která by za běžných okolností nebyla uskutečněna. Tento typ útoku často spoléhá na přirozenou důvěřivost, nedostatek obezřetnosti, nebo nízkou informovanost oběti.

Podstatou této techniky je vytvořit takovou situaci, v níž oběť mylně vyhodnotí skutečný stav věcí. Jinými slovy, místo toho, aby útočník složitě obcházel technická bezpečnostní opatření, snaží se dosáhnout svého cíle prostřednictvím manipulace – například tím, že přiměje uživatele, aby sám své přístupové údaje dobrovolně sdělil. Sociální inženýrství je tedy založeno na zneužití mezilidské komunikace a důvěry, nikoliv na technologickém útoku. (Zoner software, n.d.)

3.1.4 Fake news, derinformace a manipulativní obsah

Fake news, dezinformace a manipulativní obsah označují informace, které jsou záměrně nebo neúmyslně nepravdivé a mají za cíl ovlivnit postoje, chování nebo přesvědčení jednotlivců či skupin. (Kopecký, 2022)

V prostředí sociálních sítí, kde algoritmy zvýhodňují obsah, na který uživatelé intenzivně reagují, se tyto informace šíří velmi rychle a často bez jakékoli zpětné kontroly.

Vliv těchto jevů se ukázal velmi výrazně například během pandemie covidu-19, kdy byly veřejné debaty zahlceny řadou dezinformací týkajících se očkování, původu viru nebo účinnosti ochranných opatření. Tyto dezinformace často vznikaly v zahraničí, ale šířily se i v českém prostředí a ovlivnily vnímání velké části veřejnosti.

Pro mnohé uživatele internetu je obtížné odlišit důvěryhodný zdroj od manipulativního, obzvlášť pokud se nachází v tzv. sociální bublině, tedy prostředí, kde jsou jedinci obklopeni lidmi a názory, které potvrzují jejich vlastní přesvědčení.

Zajímavým příkladem je rozšíření konspiračních teorií, například víra v tzv. „placatou Zemi“, která byla nedávno zviditelněna na sociálních médiích. Ačkoli se může jednat o extrémní případ, výzkumy ukazují, že i v rozvinutých zemích se stále najdou lidé, kteří podobným teoriím věří. (Sedláčková & Čihák, 2021)

Nejde přitom jen o selhání systému vzdělávání, ale o komplexní souhru vlivů, včetně způsobu fungování algoritmů na sociálních sítích, které uživateli nabízejí stále více obsahu souvisejícího s tím, co dříve zhlédl nebo na co reagoval – tzv. efekt králičí nory (rabbit hole effect), kdy se člověk postupně noří do stále extrémnějšího a zkreslenějšího obsahu.

V českém online prostředí se stále častěji objevuje tzv. manosféra – soubor komunit, které na první pohled mohou působit jako platforma pro vzájemnou podporu chlapců a mladých mužů. Tyto skupiny ale často postupně přecházejí od rad o sebevědomí, kondici nebo životním úspěchu k toxickým narativům, například že „ženy jen využívají muže“ nebo že „feminismus ničí společnost“. (Kopecký, 2025)

Tímto způsobem se vytváří ideologický tlak, který učí mladé muže distancovat se od rovnosti a začít nahlížet na ženy s nedůvěrou či předsudky. Přijímání těchto názorů může mít pro dospívající jedince závažné psychologické dopady: frustraci, pocit nesouladu s představami o úspěchu či silném mužství, a i vznik nenávistných postojů vůči ženám. (Kopecký, 2025)

V zahraničí je s tímto jevem spojována i kontroverzní postava Andrewa Tatea, který čelí obviněním z trestných činů včetně obchodování s lidmi a sexuálního vykořisťování. (Humpálová & Skalický, 2024)

3.2 Specifické hrozby pro děti a mládež

Děti a mladiství čelí jiným hrozbám a rizikům než dospělá populace. Primárně nebývají cílová skupina finančních podvodů. Neboť penězi ve větší míře nedisponují. Jsou však, ale také snadnou obětí jiných manipulativních útoků a často nemusí chápat ,že jim někdo chce uškodit. Zvlášť, když takové prostředí neznají.

3.2.1 Sexuální zneužití, sexting, grooming

Sexuální zneužívání dětí v online prostředí, patří mezi závažné a obtížně postižitelné jevy současné digitální doby. Útočníci často zneužívají anonymity internetu a falešné identity k navazování kontaktu s dětmi, zejména prostřednictvím sociálních sítí, chatovacích aplikací

nebo online her. Děti si mnohdy neuvědomují rizika, která jim v digitálním světě hrozí a ztrácejí přirozené zábrany. Výsledkem může být sdílení citlivého obsahu, který je následně zneužit k vydírání nebo veřejnému šíření. Jakmile se takový materiál dostane na internet, je jeho úplné odstranění prakticky nemožné.

Sexting, tedy dobrovolné zasílání vlastních intimních fotografií nebo videí, představuje častý projev zneužití důvěry. Děti mnohdy netuší, že tímto jednáním mohou nejen ohrozit svou psychiku, ale zároveň se nevědomky dopouštět i trestného činu, například výroby dětské pornografie (§ 192 trestního zákoníku) nebo ohrožování výchovy dítěte (§ 201).

Kybergrooming představuje promyšlený způsob manipulace, kdy dospělá osoba navazuje kontakt s dítětem s cílem vybudovat důvěru a následně jej přimět k osobní schůzce, nebo k sexuálním aktivitám online. Pachatelé využívají různé komunikační kanály a často nabízejí dítěti odměnu výměnou za erotické chování před kamerou. Tento jev bývá spojován s trestným činem svádění k pohlavnímu styku (§ 202 trestního zákoníku) a je o to nebezpečnější, že se může odehrávat bez fyzického kontaktu, čistě prostřednictvím internetu. (Policie České republiky, bez data)

To, v jaké míře je rozšířené sexualizované násilí na dětech a mladistvých na sítích se do povědomí široké veřejnosti dostalo prostřednictvím dokumentárního filmu V síti od Víta Klusáka a Barbory Chalupové.

Tvůrci v něm ukázali, jak snadno je možné pro teenagery spadnout do pasti „predátora“ – neoficiální pojmenování pro pachatele, kteří cíleně navazují kontakt s nezletilým za účelem zneužití, používané v dokumentu i v médiích.

Dokumentární film ukazuje, jak snadno se může dvanáctiletá dívka stát terčem sexuálního násilí. Stačí vytvořit falešný profil na běžné sociální síti a během několika minut se ozývají desítky dospělých mužů s explicitními požadavky, včetně žádostí o intimní fotografie. Pachatelé používají manipulativní strategie – navazují důvěru, předstírají porozumění či zájem a postupně přecházejí k sexualizovaným tématům. Tento postup se označuje jako grooming.

Ve filmu byly tyto situace zdokumentovány v reálném čase prostřednictvím interakce dospělých hereček, které vystupovaly jako dvanáctileté dívky. Pachatelé nevěděli, že komunikují s fiktivními postavami. Dokument doplňují rozhovory s odborníky, kteří rozebírají chování obětí i útočníků. (Klusák & Chalupová, 2020)

Způsob zobrazení pachatelů však může vést k mylnému dojmu, že jde výhradně o osoby trpící pedofilií. Tento stereotyp neodpovídá skutečnosti – většinu případů páchají běžní jedinci, kteří využívají moc, anonymitu a příležitost v online prostoru. Mýtus o „pedofilních predátorech“ zjednodušuje problém a odvádí pozornost od nutnosti systematické prevence.

Pachatelé nejsou vždy cizinci na internetu, často jde o osoby z blízkého okolí dítěte. Proto je důležité vnímat toto riziko komplexně – jako důsledek nedostatečné ochrany dětí a rizik spojených s digitální komunikací. (Kopecký, 2019)

3.2.2 Kyberšikana

Kyberšikana je forma šikany, která využívá technologie počítače, mobilní telefony, tablety, odehrávající se nejčastěji na sociálních sítích. Je charakteristická opakovaným a zákeřným chováním, často posilovaným dalšími uživateli prostřednictvím sdílení, či komentování škodlivého obsahu. Na rozdíl od jednorázového obtěžování způsobuje kyberšikana dlouhodobý psychický tlak, oběť nemá prostor k obrany a existuje nerovnováha moci mezi útočníkem a obětí.

Podle výzkumu z roku 2009 téměř polovina dětí u nás je vystavena nějaké formě kyberšikany. A to ve formě dehonestujících útoků, vyhrožování a vydírání atd. (Krejčí & Kopecký, 2010)

A to bylo ještě před masovým rozšířením sociálních sítích mezi mladistvé.

3.2.3 Ztráta mezilidských kontaktů

Ztráta přirozených mezilidských kontaktů je fenoménem, který zasahuje celou společnost. V případě dětí a dospívajících však představuje závažné riziko pro jejich zdravý psychický a sociální vývoj. Komunikace, která se v minulosti odehrávala převážně ve fyzickém prostoru, se dnes ve velké míře přesouvá do online prostředí. Zvláště pro mladší uživatele, kteří si často ještě nedokáží plně uvědomit šíři a rizika digitálního světa, může tato změna představovat značnou psychickou zátěž.

Digitální komunikace prostřednictvím textových zpráv a emotikonů bývá ochuzena o neverbální složky, které jsou klíčové pro správné porozumění a budování vztahů. Takto zjednodušená forma komunikace může vést k nejistotě, nedorozuměním a v některých případech i ke vzniku sociálních úzkostí či fobií. Iluze „dokonalého světa“, kterou vytvářejí sociální sítě, může u dětí a dospívajících podporovat pocity méněcennosti, což následně přispívá k jejich větší izolaci od reálného světa.

Typickým příkladem úbytku přirozené sociální interakce lze pozorovat ve školním prostředí. Zatímco dříve byly přestávky prostorem pro budování vztahů skrze přímou komunikaci a společné hry, dnes jsou stále častěji vyplňovány individuální aktivitou na mobilních zařízeních – ať už se jedná o sledování obsahu na sociálních sítích, hraní her, či

natáčení videí. Takové aktivity, byť mohou působit jako společné, nenaplňují základní potřeby dětí v oblasti přímé mezilidské interakce a emočního vývoje.

Výrazný negativní dopad měla v tomto směru pandemie covidu-19, kdy došlo k plošnému uzavření škol a omezení běžných sociálních kontaktů. Dlouhodobá izolace a přesun vzdělávání do online prostoru, přispěly ke zhoršení duševního zdraví u mnoha dětí. Statistické údaje i klinická praxe potvrzují nárůst výskytu depresí, úzkostí a dalších psychických obtíží u školní mládeže právě v důsledku tohoto období.

V neposlední řadě je nutné zmínit také fenomén tzv. parasociálních vztahů, kdy děti navazují jednostranné emocionální pouto s osobami z internetového prostředí – například influencery nebo herci. Tyto vztahy sice mohou dočasně suplovat pocit blízkosti, nicméně nevedou k rozvoji sociálních dovedností a schopnosti fungovat v reálných vztazích.

4 Vzdělávání v bezpečnosti v digitální gramotnosti

V návaznosti na předešlé kapitoly se podíváme na to, co nám určuje vzdělávání a jak máme v České republice vymezeno, co se mají žáci na základních školách učit v tomto okruhu.

4.1 Legislativa a strategické dokumenty

Bezpečnost v digitálním prostředí je v současném RVP ZV reflektována jako důležitá součást digitální gramotnosti. Tento dokument tvoří základ pro tvorbu školních vzdělávacích programů (ŠVP) a určuje nejen oblasti vzdělávání, ale také očekávané výstupy a průřezová témata. V aktuální platné verzi jsou posíleny témata spojená s digitální gramotnosti a už se nebere jen jako schopnost ovládat počítač, ale i jako schopnost se bezpečně orientovat v digitálním prostoru.

4.2 Očekávané výstupy v oblasti digitální bezpečnosti dle RVP ZV

Očekávané výstupy v oblasti bezpečnosti v digitální gramotnosti podle Rámcového vzdělávacího programu pro základní vzdělávání 2023 se zaměřují na to, aby žáci dokázali bezpečně a zodpovědně používat digitální technologie, rozpoznali rizika digitálního prostředí a dokázali se jim přiměřeně bránit. Cílem je, aby žáci získali nejen technické dovednosti, ale také porozuměli tomu, jak jejich chování v online prostředí ovlivňuje je samotné i ostatní.

Žák by měl v oblasti bezpečného chování v digitálním prostředí být schopen využívat digitální technologie bezpečně a odpovědně, například při komunikaci přes sociální sítě, e-mail nebo různé online platformy. Dále by měl být schopen rozpoznat potenciálně nebezpečné chování na internetu, jako je kyberšikana, nevyžádané zprávy nebo kontakt s neznámými osobami. Měl by si chránit svoje osobní údaje, tedy jméno, adresu, fotografie nebo přístupové údaje, a chápat, proč je důležité tyto informace nesdílet veřejně. Součástí očekávaných výstupů je také schopnost dodržovat zásady kyberneticky odpovědného chování – například vytvářet si silná a bezpečná hesla, pravidelně zálohovat důležitá data nebo chránit zařízení pomocí antivirového softwaru.

Důležitou součástí vzdělávání v oblasti bezpečnosti je také rozvoj kritického myšlení. Žák by měl být veden k tomu, aby si osvojil dovednosti potřebné k rozpoznání manipulativního nebo zavádějícího obsahu. To zahrnuje schopnost zhodnotit věrohodnost zdrojů informací, ověřit si pravdivost sdělení a aktivně přemýšlet nad tím, jaký vliv na něj mohou mít informace šířené prostřednictvím digitálních médií. Měl by chápat, že nejen jeho vlastní chování

v digitálním prostředí má dopad, ale i to, co sdílí, komentuje nebo lajkuje, se může promítnout do reálného života. Kritické myšlení je klíčové i v tom smyslu, že pomáhá předcházet šíření dezinformací a podvodného obsahu.

Neméně důležité je vzdělávání žáků v oblasti digitální etiky a právních norem spojených s používáním technologií. Děti by měly porozumět tomu, co znamená autorské právo, kdy je možné používat cizí fotografie, texty nebo hudbu, a jak správně citovat zdroje. Měly by být schopné odlišit eticky přijatelné chování v online prostředí od jednání, které je nevhodné, ohrožující nebo dokonce protiprávní. Například šíření urážlivých komentářů, zastrašování jiných osob nebo sdílení cizího obsahu bez svolení může mít vážné následky. Děti by tak měly být informovány o tom, že za svá jednání nesou odpovědnost, i když probíhají v anonymním prostředí internetu.

V neposlední řadě se očekává, že si žák vytvoří zdravý vztah k technologiím. Měl by si být vědom rizik spojených s nadměrným používáním digitálních zařízení, jako je například závislost na hrách, neustálé sledování sociálních sítí nebo nedostatek spánku kvůli používání zařízení v nočních hodinách. Výuka by měla podporovat rovnováhu mezi online a offline aktivitami, a žák by měl být schopen si stanovit vlastní hranice v používání digitálních technologií. Tím se nejen předchází fyzickým a psychickým obtížím, ale také se rozvíjí schopnost samostatného rozhodování a seberegulace. (MŠMT, 2023)

4.3 Shrnutí klíčových zásad účinné prevence rizikového chování

Při prevenci rizikového chování spojeného s digitálními technologiemi je důležité vycházet ze zásad, které reflektují věk dětí, jejich digitální zkušenosti a psychickou vyspělost. Účinná prevence by měla být především systematická, dlouhodobá a přizpůsobená konkrétní věkové skupině. Zatímco u mladších dětí se doporučuje zaměřit na základní pravidla bezpečného chování online (například tvorba silných hesel či opatrnost při komunikaci s cizími osobami), u starších žáků je vhodné rozvíjet porozumění složitějším tématům, jako jsou kyberšikana, nebezpečné výzvy nebo zneužití soukromých údajů.

Preventivní programy by neměly být jednorázové, ale měly by na sebe navazovat a podporovat postupné budování postojů, znalostí a dovedností. Vhodné je zapojovat žáky aktivně – pomocí diskusí, práce s příběhy, modelových situací nebo pracovních listů. Klíčem je, aby se žáci učili nejen rozpoznat rizikové situace, ale také aktivně přemýšleli o jejich možném řešení a dopadech.

Dobrým přístupem je využití výukových metod založených na řešení konkrétních problémů (tzv. problem-based learning), kdy žáci zkoumají reálné či fiktivní situace a hledají způsoby, jak by bylo možné daný problém bezpečně zvládnout. Taková forma výuky podporuje rozvoj kritického myšlení, argumentace a schopnosti spolupráce.

Prevence by měla být realizována v bezpečné atmosféře, která umožňuje otevřené vyjádření názorů bez strachu z odsouzení. Děti a mladí lidé potřebují prostor, kde se mohou cítit respektováni, a kde se preventivní program nestává místem další stigmatizace nebo zesměšnění.

Velmi důležité je také to, aby prevence nepůsobila zastrašujícím dojmem. Cílem není vyvolávat strach, ale podporovat informované, odpovědné a vědomé chování. Žáci by měli odcházet s pocitem porozumění, nikoli úzkosti. Pokud se při prevenci využívají filmy, videa nebo jiné multimediální materiály, měly by být vždy doprovázeny vysvětlením, řízenou diskusí a možností reagovat.

V neposlední řadě je klíčové, aby preventivní programy vedli lidé, kteří mají nejen odborné znalosti v oblasti digitální bezpečnosti, ale i potřebné pedagogické a komunikační dovednosti. Kvalita výuky závisí nejen na obsahu, ale i na schopnosti vytvořit s žáky vztah a bezpečný prostor pro otevřenou debatu. (Kopecký et al., 2023)

5 Výzkumná část

Praktická část této bakalářské práce je zaměřena na zjištění úrovně znalostí, postojů a dovedností žáků druhého stupně základních škol v oblasti bezpečnosti v digitální gramotnosti. Cílem výzkumného šetření bylo zjistit, jak žáci vnímají a zvládají vybrané požadavky definované v Rámcovém vzdělávacím programu pro základní vzdělávání, které se týkají bezpečného a odpovědného chování v digitálním světě.

Pozornost byla věnována především oblastem, jako je ochrana osobních údajů, tvorba bezpečných hesel, schopnost rozpoznat rizikové chování na internetu, reakce na nevhodné situace a uvědomění si možných důsledků vlastního jednání v online prostoru.

Sběr dat probíhal prostřednictvím online dotazníkového šetření, které bylo realizováno pomocí nástroje Survio.com. Do výzkumu se zapojili žáci navštěvující 2. stupeň základních škol. Jedná se především o žáky z mého domovského skautského střediska na Blanensku, kde bylo možné výzkum realizovat s ohledem na přímý kontakt s účastníky a jejich zákonnými zástupci. Výsledky tohoto šetření přinášejí cenné informace o tom, jak jsou žáci v této oblasti připraveni a kde se nacházejí slabá místa, která by mohla být dále rozvíjena v rámci školní výuky.

5.1 Výzkumné otázky:

Stanovila sem tyto výzkumné otázky:

- Jak moc žák chrání svoje osobní údaje a uvědomuje si co je v pořádku sdílet online?
- Zná žák pojem bezpečné heslo a používá bezpečná hesla?
- Dokáže žák rozpoznat rizikové chování na internetu
- Ví žák, co dělat, když se střetne s nevhodným chováním na internetu například na sociálních sítích.
- Dokáže žák rozlišit pravdivé a nepravdivé informace na internetu.
- Uvědomuje si žák důsledky svého chování v online prostředí, včetně možných právních dopadů?
- Liší se úroveň znalostí podle pohlaví a věku respondentů?

Odpovědi na tyto výzkumné otázky umožní lépe porozumět, nakolik jsou žáci vybaveni potřebnými kompetencemi pro bezpečné a odpovědné chování v digitálním světě.

5.2 Metodologie výzkumu

Výzkumná část této bakalářské práce je postavena na kvantitativním přístupu, který umožňuje analyzovat větší množství dat a následně je zobecnit pro danou cílovou skupinu. Kvantitativní metoda byla zvolena s ohledem na povahu výzkumných otázek, které se zaměřují na měření znalostí, postojů a chování žáků v oblasti bezpečnosti v gramotnosti.

Dotazník obsahuje uzavřené otázky, škálové otázky umožňující respondentům vyjádřit míru souhlasu či nesouhlasu s různými tvrzeními. Otázky jsou sestaveny s cílem pokrýt základní tematické okruhy bezpečnosti v digitálním prostředí, které vycházejí z očekávaných výstupů RVP ZV a doporučení odborné literatury. Charakter dotazníku je neinvazivní, otázky se vztahují k běžnému chování v online prostředí a nezasahují do soukromí respondentů.

Cílovou skupinu výzkumu tvoří žáci ve věku 11–15 let, kteří odpovídají věkovému rozpětí druhého stupně základní školy (6.–9. třída). Celkový počet respondentů činil 62 žáků, přičemž 38 z nich vyplnilo dotazník online na základě e-mailového odkazu sdíleného jejich rodiči a 24 respondentů vyplnilo dotazník osobně během skautské schůzky.

Otázky v dotazníku jsou tematicky rozděleny do několika oblastí: povědomí o osobních údajích, používání hesel, rozpoznávání rizikového chování, reakce na ohrožující situace, ověřování informací a uvědomění si důsledků digitálního chování. Dotazník neobsahuje žádné osobní ani citlivé údaje a jeho vyplnění je plně anonymní. Součástí dotazníku jsou také základní demografické otázky (věk, pohlaví, školní ročník), které slouží k dalšímu zpracování dat a porovnávání odpovědí mezi různými skupinami.

Výzkum jsem prováděla v měsících květen a červen 2025. Získaná data jsme následně exportovali z platformy Survio.com a zpracovali pomocí programu Microsoft Excel**.** Podrobnosti k etickému zajištění výzkumu a informovaným souhlasům jsou uvedeny v následující kapitole.

5.3 Etické aspekty výzkumu

Při realizaci výzkumného šetření byl kladen důraz na dodržení etických zásad, zejména s ohledem na to, že výzkumu se účastnili nezletilí respondenti ve věku 11–15 let. Sběr dat probíhal výhradně anonymní formou a nebyly shromažďovány žádné citlivé osobní údaje, které by mohly vést k identifikaci konkrétní osoby.

Dotazník byl distribuován dvěma způsoby. První část výzkumného vzorku obdržela dotazník prostřednictvím odkazu zaslaného e-mailem zákonným zástupcům. V e-mailu jsme

uvedli účel výzkumu, ujištění o anonymitě a žádost, v případě souhlasu s účastí svého dítěte rodič odkaz předal svému dítěti k vyplnění.

Druhou část respondentů jsme oslovili osobně v rámci skautské schůzky. Zde byl zákonným zástupcům předložen tištěný informovaný souhlas, který byl po vysvětlení účelu výzkumu podepsán. Tyto podepsané formuláře jsme archivovaly. Z důvodu ochrany osobních údajů nejsou součástí příloh. Účast všech respondentů byla dobrovolná a žáci mohli výzkum kdykoli ukončit.

5.4 Výsledky výzkumu

Dotazník vyplnilo 62 respondentů. V následujícím rozložení:

	Ženy	Muži	Celkem respondentů
6. třída	4	3	7
7. třída	15	6	21
8. třída	20	6	26
9. třída	6	2	8

Tabulka 1 Rozložení respondentů výzkumu

5.4.1 Ochrana osobních údajů a online sdílení

Výzkumná otázka č. 1:

Jak moc žák chrání svoje osobní údaje a uvědomuje si, co je v pořádku sdílet online?

Tato otázka byla zjišťována pomocí následujících tří položek dotazníku:

- Q3: Vím, co jsou osobní údaje.
- Q4: Vím, jaké údaje je bezpečné sdílet online.
- Q5: Na sociálních sítích a hrách si hlídám, co o sobě sdílím.

Odpovědi byly zaznamenány na pětibodové Likertově škále a převedeny do numerických hodnot od −2 (negativní postoj) do +2 (pozitivní znalost/postoj). Průměrné hodnoty těchto tří položek byly využity k hodnocení povědomí žáků o ochraně osobních údajů. Průměrné hodnoty odpovědí napříč celým souborem:

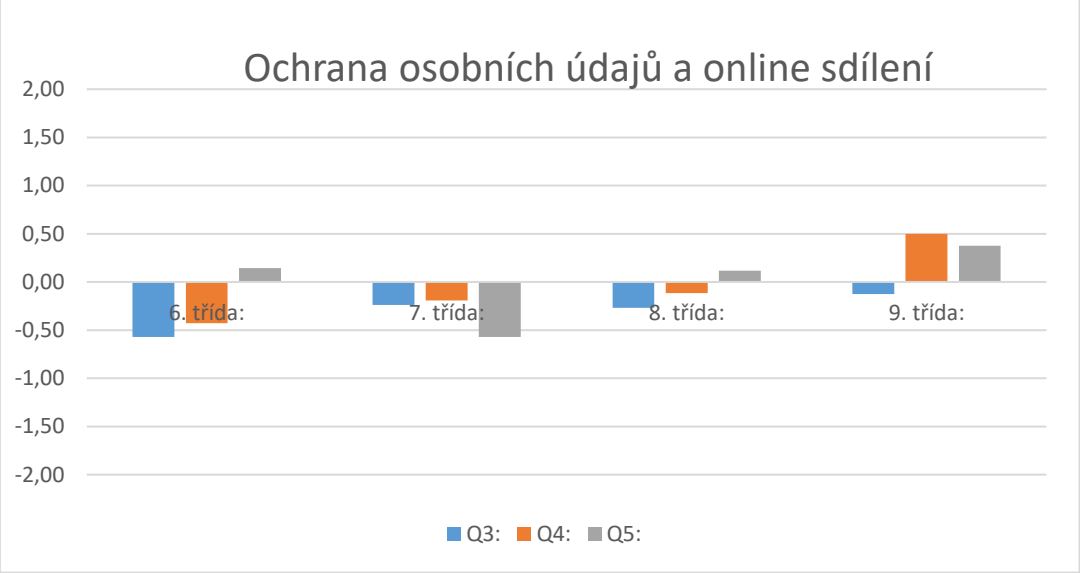
- Q3: -0.3
- Q4: -0.1
- Q5: -0.1

Rozložení podle tříd:

	Q3:	Q4:	Q5:
6. třída:	-0,57	-0,43	0,14
7. třída:	-0,24	-0,19	-0,57
8. třída:	-0,27	-0,12	0,12
9. třída:	-0,13	0,50	0,38

Tabulka 2 Rozložení tříd – Ochrana osobních údajů

Graf vyhodnocení:



Graf 1 Ochrana osobních údajů a online sdílení

Z výsledků vyplývá, že většina žáků má pouze částečné či nízké povědomí o ochraně osobních údajů. Nejnižší hodnoty byly zaznamenány u mladších žáků (zejména v 6. třídě), kde se průměrné skóre v oblasti porozumění pojmu osobní údaj (Q3) pohybovalo hluboko v negativních hodnotách (−0,57). Významný posun k lepším výsledkům je patrný u žáků 9. ročníku, kteří jako jediní dosáhli kladného skóre ve všech třech položkách – zejména u otázky Q4 („Vím, co je bezpečné sdílet online“), kde výsledek byl +0,50.

Výsledky ukazují, že žáci sice s přibývajícím věkem vykazují lepší výsledky, přesto jsou celkové hodnoty většinou spíše slabé až neutrální. Zejména alarmující je výsledek u otázky Q5 u 7. třídy (−0,57), který ukazuje na velmi nízkou míru uvědomění ohledně řízení vlastního chování na sociálních sítích.

Data tedy ukazují na potřebu systematické edukace v oblasti ochrany osobních údajů, a to již od nejnižších ročníků druhého stupně ZŠ. Praktické dovednosti, jako je rozlišování toho, co je vhodné sdílet, a kontrola nad vlastním digitálním obsahem, nejsou dostatečně rozvinuty.

Závěr k hypotéze č. 1:

→ Hypotéza H1 („Většina žáků chápe, co jsou osobní údaje, a ví, co je bezpečné sdílet online“) nebyla plně potvrzena.

Zatímco starší žáci (zejména 9. třída) vykazují částečně lepší výsledky, u většiny zkoumaného vzorku přetrvává slabé či neujasněné povědomí o ochraně osobních údajů a bezpečném online chování. Hypotézu lze tedy označit za částečně vyvrácenou a je vhodné doporučit důraznější zařazení tématu do výuky v nižších ročnících druhého stupně ZŠ.

5.4.2 Bezpečnost hesel

Výzkumná otázka č. 2:

Zná žák pojem bezpečné heslo a používá bezpečná hesla?

Tato oblast byla zkoumána pomocí následujících otázek:

- Q6: Vím, co znamená bezpečné heslo.
- Q7: Používám stejné heslo k více účtům.

U otázky Q7 byla správná odpověď invertována, protože z hlediska bezpečnostních doporučení je správně „Ne“, protože hesla by měla být pro různé účty odlišná.

Průměrné hodnoty odpovědí:

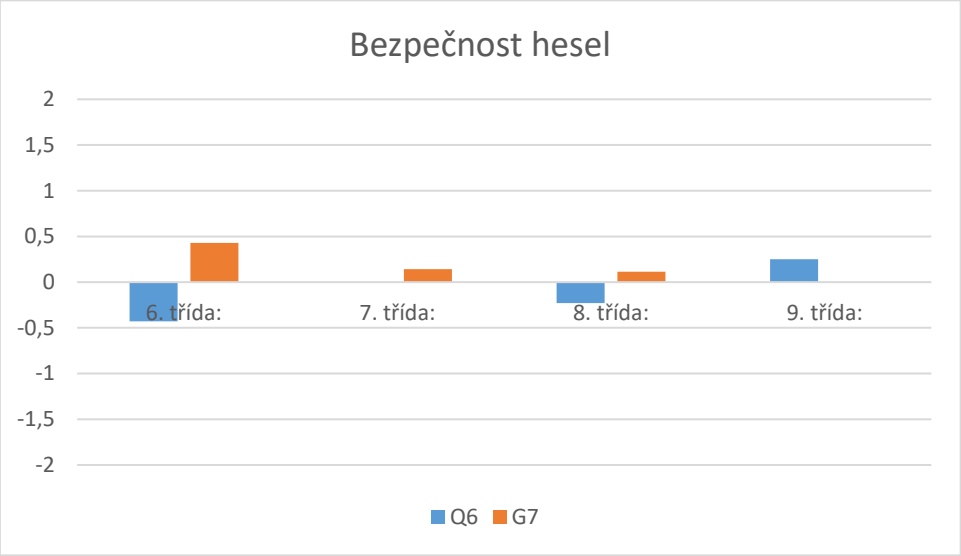
- Q6: Průměr odpovědi: -0.1
- Q7: Průměr odpovědi: 0.1

Rozložení odpovědí mezi třídami:

	Q6	G7
6. třída:	-0,43	0,43
7. třída:	0	0,14
8. třída:	-0,23	0,11
9. třída:	0,25	0

Tabulka 3 Rozložení tříd – Bezpečnost hesel

Grafické zobrazení:



Graf 2 Bezpečnost hesel

Vyhodnocení:

Z výsledků vyplývá, že žáci mají smíšené povědomí o bezpečných heslech. Odpovědi na otázku Q6 (znalost pojmu) se pohybují převážně v pásmu mírně negativním až neutrálním, což naznačuje, že část žáků si význam bezpečného hesla plně neuvědomuje. Nejvyšší skóre vykázali žáci 9. třídy (+0,25), zatímco nejnižší bylo u 6. třídy (−0,43).

U otázky Q7, která se týká praktického chování, je situace o něco lepší – průměrná hodnota je kladná (+0,1), což značí, že část respondentů hesla alespoň neduplikuje. Nejlépe dopadli opět žáci 6. třídy, což může být dáno tím, že si zatím nezakládají tolik účtů. Naopak v 9. třídě je skóre nulové, což může naznačovat horší praktické návyky nebo nižší důslednost v ochraně účtů.

Celkově lze říct, že přestože část žáků základní principy zabezpečení hesel zná, uplatňování těchto znalostí v praxi zůstává nejednotné a často nedostatečné. Výsledky ukazují na mezeru mezi teoretickým povědomím a skutečným chováním.

Závěr k otázce č. 2:

→ Hypotéza H2 („Žáci znají pojem bezpečné heslo, ale ve větší míře používají stejné heslo na více účtech“) je potvrzena.

Zjištění podporuje předpoklad, že žáci sice do určité míry rozumí, co je bezpečné heslo, ale v praxi bezpečnostní doporučení často nedodržují. Výsledky tak potvrzují potřebu zaměřit se nejen na vysvětlení pojmu, ale především na osvojení správných návyků a konkrétních preventivních opatření při tvorbě a používání hesel.

5.4.3 Rozpoznání rizikového chování

Výzkumná otázka č. 3:

Dokáže žák rozpoznat rizikové chování na internetu?

Otázky:

- Q8: Poznám, když se někdo chová na internetu podezřele.
- Q9: Psát si na internetu s cizími lidmi považuji za bezpečné.

Průměrné hodnoty odpovědí:

- Q8: Průměr odpovědi: 0.15
- Q9: Průměr odpovědi: 0.1

Rozložení odpovědí mezi třídami:

	Q8	Q9
6. třída:	-0,43	-0,43
7. třída:	-0,14	-0,14
8. třída:	-0,12	-0,12
9. třída:	0,00	0,12

Tabulka 4 Rozložení tříd – Rozpoznání rizikového chování

Většina respondentů dokázala rozpoznat podezřelé chování (Q8). Nicméně někteří žáci stále považují kontakt s cizími osobami na internetu za bezpečný, což je varující.

Tato zjištění naznačují, že rozpoznání rizika se zlepšuje s věkem, ale určitá naivita nebo důvěřivost zejména u mladších ročníků přetrvává.

Závěr k otázce č. 3:

→ Hypotéza H3 (*„Žáci dokáží rozpoznat rizikové chování“*) je částečně potvrzena – většina žáků dokáže rozpoznat rizikové chování.

5.4.4 Reakce na nevhodné chování online

Výzkumná otázka č. 4:

Ví žák, co dělat, když se střetne s nevhodným chováním na internetu?

Otázka:

- Q10: Vím, co dělat, pokud mě někdo nebo něco online ohrožuje.

Průměrné hodnoty odpovědí:

- Q10: Průměr odpovědi: 0.2

Rozložení odpovědí mezi třídami:

	Q10
6. třída:	-0,71
7. třída:	0,33
8. třída:	0,19
9. třída:	0,13

Tabulka 5 Rozložení tříd – Reakce na nevhodné chování online

Průměrné skóre bylo mírně pozitivní. To naznačuje, že většina respondentů má představu, jak reagovat, i když ne vždy dostatečně prakticky. Rozdíly mezi třídami opět ukazují, že starší žáci si v krizových situacích dokážou poradit lépe.

Závěr k otázce č. 4:

→ Hypotéza H4 (*„Žáci vědí, jak se zachovat při setkání s nevhodným chováním“*) je většinově potvrzena.

5.4.5 Schopnost ověřit pravdivost informací

Výzkumná otázka č. 5

Dokáže žák rozlišit pravdivé a nepravdivé informace na internetu?

Otázka:

- Q11: Rozpoznám pravdivou a nepravdivou informaci na internetu.

Průměrné hodnoty odpovědí:

- Q11: Průměr odpovědi: -0.3

Rozložení odpovědí mezi třídami:

	Q11
6. třída:	-0,71
7. třída:	0,33
8. třída:	-0,19
9. třída:	0,13

Tabulka 6 Rozložení tříd – Schopnost poznat pravdivou informaci

Tato otázka dosáhla nejnižšího skóre v celém šetření. Žáci vykazují výraznou nejistotu a omezenou schopnost pracovat s informacemi.

Mnozí respondenti uvedli, že „nevědí“ nebo „spíše nepoznají“ rozdíl mezi pravdou a dezinformací, což je v současném digitálním světě závažné zjištění.

Závěr k otázce č. 5:

→ Hypotéza H5 (*„Schopnost rozlišit pravdivé a nepravdivé informace je slabší“*) je potvrzena.

5.4.6 Uvědomění si důsledků online chování

Výzkumná otázka č. 6:

Uvědomuje si žák důsledky svého chování v online prostředí, včetně možných právních dopadů?

Otázka:

- Q12: Vím, že nevhodné chování na internetu může mít následky v reálném životě.

Průměrné hodnoty odpovědí:

- Q12: Průměr odpovědi: 0.2

Rozložení odpovědí mezi třídami:

	Q12
6. třída:	-0,43
7. třída:	-0,14
8. třída:	0,27
9. třída:	0,38

Tabulka 7 Rozložení tříd – Uvědomění si důsledků online chování

Průměrné výsledky jsou pozitivní – většina žáků si alespoň obecně uvědomuje, že jejich online chování může mít důsledky. Starší žáci dosahují vyšších hodnot, ale i mladší většinou odpovídali „spíše ano“.

Závěr k otázce č. 6:

→ Hypotéza H6 (*„Žáci si nejsou vědomi důsledků“*) je vyvrácena – většina žáků důsledky chápe.

5.4.7 Rozdíly podle věku a pohlaví

Výzkumná otázka č. 7:

Liší se úroveň znalostí podle pohlaví a věku respondentů?

Tato otázka byla zpracována pomocí celkového skóre z jednotlivých odpovědí, přičemž skóre bylo normalizováno a zohledňovalo i korekci u inverzně skórovaných položek.

Výsledky:

- Průměrné skóre narůstá s věkem – žáci 9. třídy měli jednoznačně nejlepší výsledky, naopak žáci 6. a 7. třídy zaostávali.

- Dívky v průměru dosahovaly mírně lepšího skóre než chlapci, ale rozdíl nebyl dramatický.

Závěr k otázce č. 7:

→ Hypotéza H7 (*„Existují rozdíly mezi věkem a pohlavím“*) je potvrzena – hlavně věk má významný vliv.

5.5 Celková zhodnocení výzkumu

Výzkumná část této práce se zaměřuje na úroveň připravenosti žáků druhého stupně základní školy v oblasti digitální bezpečnosti. Cílem bylo zjistit, jak žáci vnímají a zvládají požadavky kladené RVP ZV v tematickém okruhu digitální gramotnosti, konkrétně v oblasti bezpečnosti.

Pro sběr dat byl využit dotazník s 14 otázkami, které pokrývaly hlavní oblasti digitální bezpečnosti: znalost pojmu osobní údaje, bezpečné heslo, rozpoznání rizikového chování, adekvátní reakce na online ohrožení, schopnost rozlišovat pravdivé informace a uvědomění si důsledků vlastního online chování. Odpovědi byly kvantifikovány na pětibodové škále a následně statisticky analyzovány.

Na základě odpovědí 62 respondentů bylo možné vytvořit ucelený obraz o aktuálním stavu digitální gramotnosti v bezpečnostní rovině mezi žáky ve věku 11–15 let.

Zhodnocení hypotéz

Výzkumné hypotézy:

- H1: Většina žáků chápe, co jsou osobní údaje, a ví, co je bezpečné sdílet online.
- H2: Žáci znají pojem bezpečné heslo, ale ve větší míře používají stejné heslo na více účtech.
- H3: Žáci dokáží rozpoznat rizikové chování na internetu.
- H4: Žáci vědí, jak se zachovat při setkání s nevhodným chováním na internetu.
- H5: Schopnost rozlišit pravdivé a nepravdivé informace na internetu je u žáků slabší.
- H6: Žáci si nejsou vědomi právních a jiných důsledků nevhodného online chování.
- H7: Existují statisticky významné rozdíly v úrovni znalostí mezi různými ročníky a mezi pohlavími.

Hypotéza	Výsledek	Komentář
H1: Znalost osobních údajů	Nebyla plně potvrzena	Pojem známý, ale praktická aplikace kolísavá
H2: Bezpečné heslo	Potvrzena	Znalost ano, chování ne
H3: Rizikové chování	Částečně potvrzena	Starší žáci lepší, mladší důvěřivější
H4: Reakce na nevhodné chování	Potvrzena	Většina ví, co dělat
H5: Ověření informací	Potvrzena	Slabá stránka napříč věkem
H6: Uvědomění důsledků	Vyvrácena	Žáci si důsledky uvědomují
H7: Rozdíly věk/pohlaví	Potvrzena	Věk rozhoduje, pohlaví méně výrazně ale převládá znalost žen

Tabulka 8 Zhodnocení hypotéz

Na základě výsledků výzkumného šetření lze formulovat několik konkrétních doporučení pro školní praxi. Největší nedostatky v oblasti digitální bezpečnosti byly zaznamenány u žáků 6. a 7. ročníku, proto je vhodné zaměřit se na tyto mladší ročníky intenzivněji. Výuka by měla být více praktická – efektivní je například práce s modelovými situacemi, nácvik vytváření bezpečných hesel nebo rozpoznávání falešných zpráv.

Dále se ukázalo, že žáci sice mnohdy znají pojmy teoreticky, ale neumí je aplikovat v praxi. Proto je důležité podporovat přechod od teorie k reálným dovednostem. Význam má také rozvoj mediální gramotnosti, tedy schopnosti ověřovat informace a rozpoznat manipulaci.

5.6 Shrnutí

Výzkumné šetření ukázalo, že žáci druhého stupně základních škol mají základní orientaci v oblasti digitální bezpečnosti, avšak jejich znalosti a praktické dovednosti jsou často nevyrovnané. Největší rezervy se objevují zejména v oblasti ověřování informací, porozumění osobním údajům a tvorbě bezpečných hesel. Přestože většina žáků deklaruje, že ví, co je bezpečné sdílet, konkrétní odpovědi ukazují spíše nejistotu nebo nedostatečné praktické návyky.

Data rovněž ukazují jasnou souvislost mezi věkem a mírou zvládnutí digitální bezpečnosti. Starší žáci (zejména 9. třída) dosahují lepších výsledků ve většině sledovaných oblastí, zatímco mladší žáci (6. a 7. třída) častěji vykazují nízké skóre. Tento trend je z pedagogického hlediska pozitivní – naznačuje, že školní výuka v oblasti digitální bezpečnosti přináší postupný efekt. Současně však poukazuje na potřebu začít s výukou těchto témat co nejdříve, aby se předešlo zažití nevhodných návyků a podcenění rizik v online prostředí.

Celkově výzkum potvrzuje význam systematického a věkově diferencovaného přístupu k digitální bezpečnosti na základních školách. Vyučování by se nemělo zaměřovat pouze na technické dovednosti, ale také na formování postojů a rozvoj kritického myšlení, které žákům pomůže samostatně se rozhodovat v digitálním světě.

Závěr

Bezpečnost v digitálním světě je oblastí, která ve vzdělávání nabývá stále většího významu. Digitální technologie se staly běžnou součástí života, ale schopnost zacházet s nimi bezpečně a odpovědně není samozřejmostí. V této bakalářské práci jsem se proto zaměřila na jednu z klíčových složek digitální gramotnosti – bezpečnost – a její úroveň u žáků druhého stupně základních škol.

Teoretická část práce ukázala, že bezpečnost v digitálním prostředí nelze chápat pouze jako technický problém. Jde především o kombinaci dovedností, postojů a kritického myšlení, které jsou nezbytné pro ochranu sebe i druhých v online prostředí. Byly popsány aktuální hrozby, které na děti číhají od phishingu, přes manipulaci až po sexuální zneužívání. Dále bylo vymezeno i to, jak na ně vzdělávací systém reaguje.

Výzkumné šetření přineslo odpověď na otázku, jak si v těchto oblastech digitální bezpečnosti stojí žáci. Data ukázala, že ačkoliv základní povědomí o pojmech, jako jsou osobní údaje nebo bezpečná hesla, žáci většinou mají, praktické dovednosti jim často chybí. Výsledky ukazují výrazné rezervy zejména v oblasti ověřování informací, odpovědného sdílení a schopnosti reagovat na rizikové situace. U některých otázek převažovala spíše nejistota nebo pasivita než jisté a uvědomělé chování.

Zároveň se ukázalo, že věk respondentů hraje v úrovni zvládnutí digitální bezpečnosti důležitou roli. Starší žáci – především deváťáci – vykazovali celkově lepší orientaci i odpovědnější přístup. To může být vnímáno pozitivně, protože naznačuje, že výuka digitální bezpečnosti má dopad. Zároveň ale ukazuje, jak zásadní je začínat s těmito tématy co nejdříve, ideálně už na prvním stupni. Čím dříve děti pochopí základní principy bezpečného online chování, tím lépe je dokážou začlenit do svého běžného fungování.

Přestože žáci často vnímají technologie jako přirozenou součást světa, neznamená to, že se v digitálním prostředí automaticky umí chovat bezpečně. Právě v tom je role školy a pedagogů nezastupitelná – výuka by měla být praktická, věkově přiměřená a opakovaná. Nestačí žákům jednorázově říct, co nedělat. Je třeba s nimi téma dlouhodobě a systematicky otevírat, vytvářet bezpečné prostředí pro diskusi a učit je samostatně přemýšlet nad tím, co dělají.

K tomu je však třeba aby i učitelé měli přehled a vyznali se v tématech bezpečnosti na sítích a sami se vzdělávali ať už samostudiem nebo rekvalifikačními kurzy.

Závěrem bych chtěla zdůraznit, že děti nejsou pouze pasivními příjemci informací. Pokud je dobře připravíme, mohou se samy stát důležitými nositeli digitální osvěty – nejen

mezi vrstevníky, ale často i v rodinách, kde jejich rodiče nebo prarodiče s technologiemi teprve bojují. V tomto směru má školní výchova obrovský potenciál ovlivnit nejen samotné žáky, ale i jejich okolí.

Věřím, že výsledky této práce mohou být inspirací pro pedagogy, rodiče i tvůrce vzdělávacích obsahů. Také pevně věřím, že tato práce bude přínosem pro všechny, kteří se chtějí o tomto tématu něco dozvědět. Digitální bezpečnost by neměla být jen tématem informatiky – měla by se stát běžnou součástí přemýšlení o tom, jak se pohybujeme v online světě a jak jej ovlivňujeme svým každodenním chováním.

Seznam použitých zdrojů

Literatura

Joint Research Centre. (2022). *The Digital Competence Framework 2.2: DigComp 2.2 – The Digital Competence Framework for Citizens* (Y. Punie, C. Vuorikari, & S. Carretero, Eds.). Publications Office of the European Union. https://doi.org/10.2760/115376

Kopecký, K., Szotkowski, R., Kubala, L., & Schweiner, P. (2023). *Kyberakademie pro pracovníky obcí, obecních policií a další cílové skupiny ve školním prostředí* (Verze 1.0). Centrum prevence rizikové virtuální komunikace, Univerzita Palackého v Olomouci.

Ministerstvo školství, mládeže a tělovýchovy. (2023). *Rámcový vzdělávací program pro základní vzdělávání* (verze červen 2023). Praha: MŠMT. Dostupné z: https://www.edu.cz/rvp-zv/

Průcha, J., Walterová, E., & Mareš, J. (2009). *Pedagogický slovník* (6. vyd.). Portál.

Sedlák, P., Konečný, M., & kol. (2021). *Kybernetická (ne)bezpečnost: Problematika bezpečnosti v kyberprostoru* (1. vyd.). Brno: CERM.

Elektronické zdroje

Klusák, V., & Chalupová, B. (Režiséři). (2020). *V síti* [Dokumentární film]. Hypermarket Film

Česká bankovní asociace. (2025, 29. ledna). *Banky loni klientům zachránily téměř 8 miliard korun.* https://www.cbaonline.cz/clanky/banky-loni-klientum-zachranily-temer-8-miliard-korun-kyberutoku-mezirocne-pribylo-o-ctvrtinu

Digitální vzdělávání zvyšuje bezpečnost dětí i kariérní vyhlídky. (2024, 4. prosinec). Dvojklik.cz. https://www.dvojklik.cz/saferkidsonline/digitalni-vzdelavani-zvysuje-bezpecnost-deti-i-karierni-vyhlidky/

ESET. (n.d.). *Co je ransomware a jak se mu bránit?* ESET. Staženo 16. června 2025 z https://www.eset.com/cz/ransomware/

Humpálová, J., & Skalický, M. (2024, 19. března). *Muž, který nenávidí ženy? Případ Andrewa Tatea a "nebezpečí pro mladou generaci"*. iRozhlas.

https://www.irozhlas.cz/zpravy-svet/muz-ktery-nenavidi-zeny-pripad-andrewa-tatea-a-nebezpeci-pro-mladou-generaci_2403190600_cen

Kopecký, K. (2019, 15. května). *Mýtus o pedofilech zneužívajících děti opět rezonuje internetem*. E-Bezpečí, 4(1), 120–123. Dostupné z https://www.e-bezpeci.cz/journal/articles/1551.html

Kopecký, K. (2022, 2. listopadu). *Co je to vlastně ten hoax, dezinformace, misinformace nebo třeba fake news? Čím se tyto termíny liší a co mají společného*. E-Bezpečí. https://www.e-bezpeci.cz/index.php/clanky-komentare/2864-co-je-to-vlastne-ten-hoax-dezinformace-misinformace-nebo-treba-fake-news-cim-se-tyto-terminy-lisi-a-co-maji-spolecneho

Kopecký, K. (2025, 16. června). *Manosféra: Když internet učí chlapce nenávidět ženy*. E-Bezpečí. https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/socialni-site/4563-manosfera-kdyz-internet-uci-chlapce-nenavidet-zeny

Krejčí, V., & Kopecký, K. (2010, 4. února). *Kyberšikana u českých dětí – závěry z výzkumného šetření projektu E-Bezpečí a Centra PRVoK 2009* [Výzkumná zpráva]. Centrum prevence rizikové virtuální komunikace (PRVoK), Pedagogická fakulta Univerzity Palackého v Olomouci & projekt E-Bezpečí. https://www.e-bezpeci.cz/index.php/pohledem-vedy/43-247?utm

Národní ústav pro vzdělávání. (2011). *Stručné vymezení digitální gramotnosti a informatického myšlení*. From: https://archiv-nuv.npi.cz/t/strucne-vymezeni-digitalni-gramotnosti-a-informatickeho.html

(Národní ústav pro vzdělávání, 2011)

Národní úřad pro kybernetickou a informační bezpečnost. (2015). *Phishing – stále aktuální hrozba*. https://nukib.gov.cz/cs/infoservis/doporuceni/1494-phishing-stale-aktualni-hrozba/

(NÚKIB, 2015)

O2 Chytrá škola. (n.d.). *Phishing, viry a sociální inženýrství: Phishing, viry a sociální inženýrství* [článek]. Staženo 16. června 2025 z https://vyuka.o2chytraskola.cz/clanek/9/phishing-viry-a-socialni-inzenyrstvi/14398

Policie České republiky. (bez data). *Zneužívání dětí na internetu*. Policie České republiky. Staženo 16. června 2025 z https://policie.gov.cz/clanek/zneuzivani-deti-na-internetu.aspx

Zoner software. (n.d.). *Sociální inženýrství*. Internetem bezpečně. Staženo 16. června 2025 z https://www.internetembezpecne.cz/internetem-bezpecne/podvodne-praktiky/socialni-inzenyrstvi/

Sedláčková, V., & Čihák, O. (2021, 17. března). *Přibývá lidí, kteří nevěří vědě, ale žvástům o placaté Zemi, všímá si Jiří Grygar*. Český Rozhlas Plus. https://plus.rozhlas.cz/pribyva-lidi-kteri-neveri-vede-ale-zvastum-o-placate-zemi-vsima-si-jiri-grygar-7170230

Kvalifikační práce

Burďák, A. (2016). *Digitální gramotnost žáků základních škol na 2. stupni* (Diplomová práce). Univerzita Palackého v Olomouci, Pedagogická fakulta.

Polák, O. (2022). *Rozvoj digitální gramotnosti v oblasti Člověk a svět práce pomocí malých programovatelných robotů* (Diplomová práce) Západočeská univerzita v Plzni, Fakulta pedagogická.

Seznam obrázků

Seznam grafů

Seznam tabulek

Seznam příloh

Příloha 1 – Dotazník

1. Jakou třídu základní školy navštěvuješ:
   6. třída
   7. třída
   8. třída
   9. třída
2. Uveď pohlaví
   Muž
   Žena
   Jiné
3. Vím co jsou osobní údaje.
   ( ) Ne
   ( ) Spíše ne
   ( ) Nevím
   ( ) Spíše ano
   ( ) Ano
4. Vím jaké údaje je bezpečné sdílet online.
   ( ) Ne
   ( ) Spíše ne
   ( ) Nevím
   ( ) Spíše ano
   ( ) Ano
5. Na sociálních sítích a hrách si hlídám, co o sobě sdílím
   ( ) Ne
   ( ) Spíše ne
   ( ) Nevím
   ( ) Spíše ano
   ( ) Ano
6. Vím, co znamená pojem bezpečné heslo.
   ( ) Ne
   ( ) Spíše ne
   ( ) Nevím
   ( ) Spíše ano
   ( ) Ano
7. Používám stejné heslo k více účtům nebo her (například u e-mailu, her nebo školních aplikací).
   ( ) Ne
   ( ) Spíše ne
   ( ) Nevím

( ) Spíše ano
( ) Ano

8. Poznám, když se někdo chová na internetu podezřele
   ( ) Ne
   ( ) Spíše ne
   ( ) Nevím
   ( ) Spíše ano
   ( ) Určitě ano
9. Psát si na internetu s cizími lidmi považuji za bezpečné.
   ( ) Ne
   ( ) Spíše ne
   ( ) Nevím
   ( ) Spíše ano
   ( ) Ano
10. Vím, co dělat, pokud mě někdo nebo něco online ohrožuje.
    ( ) Ne
    ( ) Spíše ne
    ( ) Nevím
    ( ) Spíše ano
    ( ) Ano
11. Rozpoznám pravdivou a nepravdivou informaci na internetu.
    ( ) Vůbec ne
    ( ) Spíše ne
    ( ) Nevím
    ( ) Spíše ano
    ( ) Určitě ano
12. Vím, že nevhodné chování na internetu může mít následky v reálném životě.
    ( ) Ne
    ( ) Spíše ne
    ( ) Nevím
    ( ) Spíše ano
    ( ) Ano
13. Pravidelně aktualizuji svůj počítač, tablet nebo mobil.
    ( ) Ne
    ( ) Spíše ne
    ( ) Nevím
    ( ) Spíše ano
    ( ) Ano
14. Stahuji neznámé soubory z internetu.
    ( ) Ne
    ( ) Spíše ne

( ) Nevím
( ) Spíše ano
( ) Ano

1. Anotace

Jméno a příjmení:	Jana Nejezchlebová
Katedra:	Katedra technické a informační výchovy
Vedoucí práce:	prof. Ing. Čestmír Serafín, Dr.
Rok obhajoby:	2025

Název práce:	Bezpečnost v digitální gramotnosti
Název v angličtině:	Security in Digital Literacy
Anotace práce:	Práce se věnuje bezpečnosti v digitální gramotnosti u žáků druhého stupně ZŠ. Teoretická část popisuje digitální kompetence a rizika v online prostředí. Praktická část obsahuje výzkumné šetření, jehož cílem bylo zjistit, jak žáci vnímají a zvládají vybrané bezpečnostní oblasti z RVP ZV. Výsledky ukazují nedostatky zejména v oblasti kritického myšlení a ochrany osobních údajů.
Klíčová slova:	digitální gramotnost, bezpečnost, žáci, kritické myšlení, digitální rizika
Anotace v angličtině:	The thesis focuses on digital security within digital literacy among lower secondary school pupils. The theoretical part describes digital competencies and online risks. The practical part presents a research survey aimed at determining how pupils perceive and manage selected security areas defined by the Czech national curriculum (RVP ZV). The results reveal shortcomings particularly in critical thinking and personal data protection.

Klíčová slova v angličtině:	digital literacy, digital security, pupils, critical thinking, online risks
Přílohy vázané v práci:	Dotazník
Rozsah práce:	32 normostran
Jazyk práce:	čeština