FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

# Zadání bakalářské práce

| | |
|---|---|
| **Název:** | Informační bezpečnost pro učitele základních škol, školní mládež a studenty |
| **Student:** | Kateřina Šebestová |
| **Vedoucí:** | Ing. David Pešek |
| **Studijní program:** | Informatika |
| **Obor / specializace:** | Informační systémy a management |
| **Katedra:** | Katedra softwarového inženýrství |
| **Platnost zadání:** | do konce letního semestru 2023/2024 |

## Pokyny pro vypracování

1. Proveďte analýzu informačně bezpečnostních rizik pro děti navštěvujících základní školu.
2. Proveďte analýzu stávajících preventivních řešení na konkrétní základní škole.
3. Na základě zjištěných informací navrhněte soubor metod vhodných pro předcházení zvolených rizik.
4. Zhodnoťte přínosy navrhovaných řešení a proveďte analýzu jejich nákladů.

*Elektronicky schválil/a Ing. David Buchtela, Ph.D. dne 10. října 2022 v Praze.*

Bakalářská práce

# INFORMAČNÍ BEZPEČNOST PRO UČITELE ZÁKLADNÍCH ŠKOL, ŠKOLNÍ MLÁDEŽ A STUDENTY

**Kateřina Šebestová**

Fakulta informačních technologií
Katedra softwarového inženýrství
Vedoucí: Ing. David Pešek
10. května 2023

# Obsah

# Seznam obrázků



# Seznam tabulek

*Ráda bych zde poděkovala všem, kteří se podíleli na tvorbě této bakalářské práce. Zejména děkuji mému vedoucímu Ing. Davidu Peškovi za jeho odborné vedení, podporu a vstřícnost při konzultacích. Děkuji také všem vyučujícím Fakulty informačních technologií na ČVUT za jejich ochotu a cenné rady během mého studia.*

*Též bych ráda poděkovala Mgr. Petře Sobkové a všem z NÚKIB za jejich pomoc a nasměrování při vzniku bakalářské práce.*

*Za pomoc při tvorbě dotazníkového šetření patří mé hluboké poděkování Mgr. Tomáši Houdkovi, Ph.D. a Mgr. et Mgr. Jakubovi Šenovskému, Ph.D.*

*Mé poděkování patří paní ředitelce Mgr. Evě Čulíkové za umožnění spolupráce se základní školou Písnická v Praze 12 a všem jejím pedagogům. Obzvláště ráda bych vyjádřila poděkování Mgr. Lence Hanyšové a Mgr. Janě Vlkové, jejichž věcné připomínky a zpětná vazba byly neocenitelné.*

*Ráda bych vyjádřila své poděkování i ostatním ředitelům a pedagogům základních škol, díky kterým bylo možné provést dotazníkové šetření. Jsem jim velice vděčná, že nalezli čas dát svým žákům dotazník vyplnit.*

*Tímto bych ráda poděkovala i všem žákům, kteří dotazník zodpověděli a věnovali mu pozornost.*

*V neposlední řadě bych ráda poděkovala svým přátelům a především rodině, která mi byla oporou během celého mého dosavadního studia. Máte mé díky.*

# Prohlášení

Prohlašuji, že jsem předloženou práci vypracovala samostatně a že jsem uvedla veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 2373 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou a veškeré jejich dokumentace (dále souhrnně jen „Dílo“), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla, avšak pouze k nevýdělečným účelům. Toto oprávnění je časově, teritoriálně i množstevně neomezené.

V Praze dne 10. května 2023 Kateřina Šebestová

# Abstrakt

Tato bakalářská práce se zabývá informační bezpečností a analýzou informačně bezpečnostních rizik pro žáky základních škol. V rámci práce bylo provedeno dotazníkové šetření na několika školách, jehož cílem bylo zjistit současný stav povědomí o informační bezpečnosti ve vybraných oblastech. Na základě výsledků dotazníku a analýzy preventivních opatření konkrétní základní školy, byly vypracovány návrhy preventivních aktivit, které mohou školy učinit pro podporu výuky informační bezpečnosti.



**Klíčová slova** informační bezpečnost, přihlašovací údaje, sociální inženýrství, základní školy, informatika na základních školách, dotazníkové šetření



# Abstract

This bachelor thesis deals with information security and the analysis of information security risks for grammar school students. Within the thesis a questionnaire survey was conducted at several schools, the aim of which was to determine the current state of awareness of information security in selected areas. Based on the results of the questionnaire and the analysis of the preventive measures of the specific grammar school, proposals have been developed for preventive activities that schools can employ to support teaching of information security.



**Keywords** information security, login data, social engineering, grammar schools, computer science class at grammar schools, questionnaire survey

# Seznam zkratek

| | |
|---|---|
| DNS | Domain Name System |
| HTTPS | Hypertext Transfer Protocol Secure |
| ICT | Informační a komunikační technologie |
| IP adresa | Internet Protocol address |
| MŠMT | Ministerstvo školství, mládeže a tělovýchovy |
| NÚKIB | Národní úřad pro kybernetickou a informační bezpečnost |
| RVP | Rámcový vzdělávací program |
| RVP ZV | Rámcový vzdělávací program pro základní vzdělávání |
| SSO | Single Sign-On – Jednotné přihlášení |
| ŠVP | Školní vzdělávací program |
| URL | Uniform Resource Locator – webová adresa |

# Úvod

*„Jakákoliv dostatečně vyspělá technologie je k nerozeznání od magie.“*

*Arthur C. Clarke*

Žijeme v digitálním věku. Od prvních počítačů sálových velikostí jsme se dostali k dotykovým zařízením, které se vejdou do kapsy a průměrný uživatel na nich tráví čím dál více času. Díky tomuto pokroku, rozvoji informačních technologií, jsme propojenější více, než kdy dříve.

Už nejsme nuceni spoléhat na poštovní systém, potřebujeme-li poslat zprávu příteli v jiné zemi. Není potřeba trpělivosti při čekání na odpověď, která by navíc v době, kdy ji obdržíme, nemusela mít aktuální vypovídající hodnotu. Chceme-li poslat zprávu, jediné co potřebujeme udělat, je zmáčknout „odeslat“ a náš přítel si jí může přečíst téměř okamžitě. Nejsme ale ani z daleka omezeni na komunikaci pouze pomocí zpráv. Stačí se pomocí několika málo kliknutí připojit, skrze jednu z mnoha aplikací, online a můžeme si užít schůzku klidně z pohodlí domova. Není od nás nadále vyžadováno podnikat složité a dlouhé cesty, abychom se fyzicky dostavili na místo setkání. Již nejsme limitováni prostorem, neboť pokud máme k dispozici naše chytrá zařízení a internet, je prostor snadno překonán. Nejsložitější částí plánování mezikontinentálních schůzek se tak stává určení vhodného časového slotu.

Svět, ve kterém žijeme je jiný než svět ve kterém žili a vyrůstali naši rodiče a prarodiče. Stal se rychlejším, hektičtějším, vyžadujícím okamžité reakce a chrlícím na nás stále více informací, které se navíc stále rychleji stávají irelevantními. Mezi těmito informacemi musí jedinec rozlišit podstatné a méně podstatné zprávy, ty zavádějící či zcela fiktivní. Život neprožíváme skrze své smysly, ale skrze naše zařízení, kterým ochotně svěřujeme ty nejdůvěrnější informace.

Dne 10. března 2020 vydalo ministerstvo zdravotnictví mimořádné nařízení, kterým zakázalo žákům a studentům na základních, středních a vyšších odborných školách osobní přítomnost ve školách a školských zařízení. V důsledku toho byla postupně zavedena distanční výuka, vyžadující pro své fungování práci s výpočetní technologií, jako jsou mobilní zařízení, stolní počítače či notebooky. Ze dne na den tak bylo nutné, aby se žáci i učitelé naučili pracovat s novými nástroji. Tato potřeba porozumění technologiím se již netýkala pouze učitelů vyučujících informatické předměty, ale očekávala se například i od učitelů prvního a druhého stupně základních škol. Ať už učitelé se svými žáky komunikovali pomocí e-mailových zpráv, v nichž zasílali látku k samostudiu, či se scházeli na jedné z moha platforem pro videohovory, stala se práce v digitálním prostředí součástí každodenního života většiny populace.

Digitální svět však skrývá své vlastní nástrahy, o kterých je nutné uživatele poučit a naučit ho, jak se pohybovat v tomto prostředí bez rizika. Dle průzkumu EU Kids Online z roku 2020 přistupovalo k internetu pomocí mobilního telefonu přes 80 % dětí ve věku od 9 do 16 let. [1] Jelikož děti jsou jedním z nejzranitelnějších cílů na internetu, domnívám se, že je obzvláště důležité pracovat na jejich osvětě, už co nejdříve. Aby takové snahy byly úspěšné, je potřeba, aby i učitelé byli v konsensu s těmito cíli a měli k dispozici vhodné materiály, z nichž mohou při výuce a vlastním vzdělávání čerpat.

# Cíle

Cílem bakalářské práce je podpořit učitele při výuce informatické bezpečnosti na českých školách pomocí navrhnutí možných preventivních aktivit.

Tato práce si klade za úkol provést analýzu informačně bezpečnostních rizik se kterými se mohou setkávat žáci základních škol. V rámci analýzy těchto rizik bude provedeno dotazníkové šetření na několika školách s cílem zjistit současný stav informovanosti o vybrané výseči informační bezpečnosti.

Následně bude provedena analýza způsobu, jakým přistupuje konkrétní škola k výuce informační bezpečnosti a prevenci bezpečnostně informačních rizik. V závislosti na informacích získaných pomocí vyhodnocení dotazníkového šetření a analýzy školy dojde k výběru výseči informačně bezpečnostních rizik pro něž bude vypracováno několik návrhů jak podpořit jejich výuku. Pro tyto návrh bude zhodnocena jejich přínosnost a provedena analýza jejich nákladů.

Práce je dělena na tří části a to teoretickou, analytickou a praktickou. V teoretické části dochází k definování potřebných pojmů, problému a shrnutí současných poznatků v oblasti prevence informatických bezpečnostních rizik. V rámci analytické části je provedena analýza rizik a analýza preventivních opatřeních těchto rizik na konkrétní základní škole. V praktické části dochází k návrhu možných preventivních řešení v reakci na zjištěné poznatky v analytické části. Následně budou zhodnoceny přínosy každé varianty a bude provedena analýza jejich nákladů.

# Kapitola 1
# Informační bezpečnost

Tato kapitola a její podkapitoly čerpají primárně z [2], [3] a [4].

Informační bezpečnost se zabývá ochranou informace po celou dobu její životnosti bez ohledu na médium, které informaci nese. Informací se rozumí každý znakový pojem, který má smysl pro komunikátora i příjemce.

Pod informační bezpečnost zahrnujeme ochranu důvěrnosti, integrity a dostupnosti informací. Mohou být zahrnuty i další vlastnosti jako je autenticita, odpovědnost, nepopiratelnost a spolehlivost. [5] Informační bezpečnost se zaměřuje na prevenci, detekci a reakci na útoky na informační systémy, ochranu citlivých informací před zneužitím a zabezpečení informačních systémů. Mezi hrozby s nimiž se informační bezpečnost potýká jsou útoky na přihlašovací údaje, viry a jiný škodlivý software, phishingové útoky a další. [6]

Informatickou bezpečnost lze vnímat v tandemu s kybernetickou bezpečností, tou se rozumí souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru. Zabývá se zajištění důvěrnosti, integrity a dostupnosti informací v kybernetickém prostoru. Kybernetická bezpečnost se zahrnuje technické opatření jakými jsou firewall, antivirový software, šifrování a další nástroje, které pomáhají chránit počítačové sítě a systémy před neoprávněným přístupem a útoky.

Jedním z pilířů informační bezpečnosti je snaha zabránit přístupu neautorizovaných osob k zařízení či účtům. K tomu slouží vhodné přihlašovací údaje.

## 1.1 Přihlašovací údaje

Přihlašovací údaje je uspořádaná množina informací, které je nutné zadat pro přístup do jinak nepřístupného či omezeného systému. Pro přihlášení je vždy nutné zadat správně celou množinu těchto informací. S přihlašovacími údaji se nejčastěji setkáme jako s dvojicí uživatelského jména (také známé jako username) a hesla.

Uživatelské jméno je jednoznačným identifikátorem uživatele. Zpravidla se jedná o pro daný systém unikátní řetězec znaků, nejčastěji o kombinaci písmen a znaků. Uživatelským jménem může být telefonní číslo, e-mailová adresa či libovolné seskupení znaků, které splňuje podmínky daného systému. V některých případech je dána uživateli možnost si toto uživatelské jméno zvolit – setkáváme se s tím nejčastěji při zakládání účtů na sociálních sítích či jiných podobných platformách. V pracovním či školním prostředí pak bývá zvykem, že je uživatelské jméno uživateli přiděleno správcem systému či jinou pověřenou osobou. [7]

Znalost přihlašovacích údajů by měla být omezena na oprávněné uživatele. Obvykle jde pouze o jednoho jedince a to vlastníka účtu k nimž přihlašovací údaje patří. V mimořádných případech se může jednat i o skupinu lidí, jako je rodina či společná domácnost – například hesla

k streamovacím službám, Wi-Fi síti…

Přihlašovací údaje jsou oblíbeným cílem kybernetických útoků. [8]

### 1.1.1 Bezpečnost hesel

Bezpečnost hesel je jednou z klíčových oblastí kybernetické bezpečnosti. Za heslo považujeme řetězec znaků sloužící k ověření identity či oprávněného přístupu.

Základními předpoklady pro bezpečné heslo je dodržení následujících zásad:

**Složitost** heslo by mělo být dostatečně složité, tedy obsahovat variabilitu znaků (číslice, velká a malá písmena, speciální znaky) a být vhodné délky.

**Unikátnost** heslo by mělo být pro každý účet unikátním, nemělo by tedy docházet k recyklovaní hesel či využívání dlouhých částí znaků z jiných hesel – například přidáním přípony odlišující konkrétní službu (-Fb, -Gmail, -Insta…) na konec či začátek hesla.

**Nesdílet** znalost hesla by měl mít pouze oprávněný uživatel. Nemělo by docházet ke sdílení hesla a to ani v rámci pracovního či osobního prostředí.

**Nepsat** uživatel by si neměl heslo nikam zapisovat, bez ohledu na nosič záznamu (Excelovská tabulka, sešit, poznámka, textové soubory…). V případě potřeby by uživatel měl použít pro vybraná hesla vhodné programy – takzvané správce hesel.

**Žádné osobní údaje** uživatel by při volbě bezpečného hesla neměl používat osobních údajů či informací, které jsou k němu zjistitelné. Mezi takovéto údaje například patří:

- Jména rodinných příslušníků
- Jména mazlíčků
- Důležitá data (svatba, narození…)
- Adresy
- Jména či názvy pozpátku (Divad, Koobecaf…)
- Názvy služeb (Instagram, Facebook)

**Nepoužívat triviální hesla** každoroční průzkumy vykazují jaká hesla uživatelé nejčastěji používají. Použitím hesla na takovémto seznamu se uživatel vystavuje riziku, že jeho heslo bude bez větších problémů prolomeno. Hesla objevující se na seznamu nejpoužívanějších hesel zahrnují například slovo „heslo“ v libovolném jazyce a variacích či 123456, 123456789, qwerty…

[9]

#### 1.1.1.1 Složitost hesla

Při požadavku na složitost hesla mluvíme především o využívání velkých a malých písmen, číslic a speciálních znaků (čárka, vykřičník, zavináč…) v hesle. Anglická abeceda využívá 26 písmen. Jelikož rozlišujeme zda jsou písmena velká či malá, máme k dispozici celkem 52 znaků. Česká abeceda zvyšuje počet na 42 písmen, je nutné však z tohoto počtu odebrat písmeno „ch“, které bývá v digitálních zařízení zapisováno pomocí dvou znaků a to znaku „c“ a znaku „h“. Tímto způsobem při využití jak malých tak velkých písmen máme k dispozici 82 znaků. Přidáním číslic zvyšujeme číslo o 10 znaků. V případě použití speciálních znaků dojde k dalšímu nárůstu – každý systém si zde může zvolit zda, případně jaké, speciální znaky pro použití v hesle povolí. Množinu těchto znaků nazveme abecedou.

Počet různých hesel, které je možné sestavit je roven $V(k,n) = n^k$ přičemž $n$ označuje počet znaků abecedy a $k$ délku hesla. Ze vzorce lze poznat, že dochází k exponenciálnímu růstu v závislosti na počtu znaků, které v heslu použijeme.

**Tabulka 1.1** Počet možných kombinací hesla v závislosti na délce hesla a počtu možností pro každý znak v hesle – anglická abeceda, vlastní dílo

| **Délka hesla k** | **Malá písmena** $V(k,26)=n^k$ | **Malá a velká písmena** $V(k,52)=n^k$ | **Malá, velká písmena a číslice** $V(k,62)=n^k$ |
|---|---|---|---|
| 1 | 26 | 52 | 62 |
| 2 | 676 | 2 704 | 3,844 |
| 3 | 17,576 | 140 608 | 238 328 |
| 4 | 456 976 | 7 311 616 | 14 776 336 |
| 5 | 11 881 376 | 380 204 032 | 916,132 832 |
| 6 | 308 915 776 | 19 770 609 664 | 56 800 235 584 |
| 7 | 8 031 810 176 | 1 028 071 702 528 | 3 521 614 606 208 |
| 8 | 208 827 064 576 | 53 459 728 531 456 | 218 340 105 584 896 |
| 12 | 95 428 956 661 682 176 | 390 877 006 486 250 192 896 | 3 226 266 762 397 899 821 056 |
| 16 | 43 608 742 899 428 874 059 776 | 2 857 942 574 656 970 690 381 479 936 | 47 672 401 706 823 533 450 263 330 816 |

### 1.1.1.2 Síla hesla

Síla hesla udává stupeň obtížnosti s kterou neautorizovaná osoba zvládne prolomit heslo hrubou silou. Sílu hesla ovlivňuje mnoho faktorů, viz 1.1.1, jeho složitost či preferenční pozice určitých znaků (například číslice na konci).

V rámci snahy vynutit používání bezpečných hesel mnohé služby zavedly na hesla následující požadavky: heslo o minimální délce 8 znaků, minimálně jedno malé a velké písmeno a alespoň jedna číslice. V reakci na tento požadavek si mnozí uživatelé volili hesla začínající velkým písmenem a končící libovolnou číslicí. Pokud vezme útočník v úvahu tuto skutečnost a bude zkoušet kombinace hesel vyhovující pouze tomuto vzoru dojde ke značné redukci počtu možných kombinacích. Tento počet lze vyjádřit následujícím vzorcem: $V(k,n,m) = m \cdot n^{k-2} \cdot 10$ přičemž $m$ označuje počet velkých písmen abecedy, $n$ označuje celkový počet znaků abecedy a $k$ délku hesla.

**Tabulka 1.2** Počet možných kombinací hesla s prvním znakem velkým a číslicí na konci v závislosti na délce hesla v porovnání s heslem bez preferencí znaků na pozici – anglická abeceda, vlastní dílo

| **Délka hesla k** | **heslo s prvním znakem velkým a číslicí na konci** $V(k,26,62)=m\cdot n^{k-2}\cdot 10$ | **Heslo bez preferencí znaků na pozici** $V(k,62)=n^k$ | **rozdíl** |
|---|---|---|---|
| 8 | 14 768 061 251 840 | 218 340 105 584 896 | $203 \cdot 10^{12}$ |
| 9 | 915 619 797 614 080 | 13 537 086 546 263 552 | $12 \cdot 10^{15}$ |
| 10 | 56 768 427 452 072 960 | 839 299 365 868 340 224 | $782 \cdot 10^{15}$ |
| 11 | 3 519 642 502 028 523 520 | 52 036 560 683 837 093 888 | $48 \cdot 10^{18}$ |
| 12 | 218 217 835 125 768 458 240 | 3 226 266 762 397 899 821 056 | $3 \cdot 10^{21}$ |
| 16 | 3 224 460 053 010 956 997 156 208 640 | 47 672 401 706 823 533 450 263 330 816 | $44 \cdot 10^{27}$ |

Tyto výpočty předpokládají, že útočník bude zkoušet uhodnout hesla pomocí takzvané metody útoků hrubou silou (viz subsection 1.1.6 Útok hrubou silou). Podobným způsobem dochází k snížení možných kombinací v případě, že útočník předpokládá využití slov ze slovníku (viz subsection 1.1.6 Slovníkový útok) a hledá tedy jejich alternace. Mezi uživateli je oblíbenou strategií pro vytvoření složitějšího hesla záměna vzhledově podobných znaků jako jsou například „E“ za „3“, „O“ za „0“ či „a“ za „@“. [10] Příkladem takovéhoto hesla je heslo doménového administrátora DigiNotar „Pr0d@dm1n“, které uniklo díky íránskému hackerovi. [11] V současné době útočníci s touto strategií při svém útoku často počítají.

Silné heslo je takové heslo, které splňuje základní požadavky bezpečného hesla. Příkladem takovéhoto hesla může být „0lk*3OvfQ63A!vrSA“ či „%2!4q2*ns$7@tqy&4#1B“.

### 1.1.1.3 Bezpečnostní otázky

Při vytváření účtu některé služby poskytují možnost zvolení takzvané bezpečností otázky. Jedná se o otázku, kterou má uživatel zodpovědět v případě zapomenutí části přihlašovacích údajů k účtu. Tyto otázky se obvykle týkají osobních údajů jako je: jméno sourozence, město narození

či oblíbený předmět na základní škole. Takovýto typ informací však porušuje jednu ze zásad bezpečného hesla a to – neuvádění osobních informací. Odpovědi na tyto otázky lze v případě potřeby často dohledat, tipnout, získat pomocí sociálního inženýrství či se uživatel může stát obětí hackera, který na ně již odpověď zná. [12, 13]

### 1.1.2 Správa přihlašovacích údajů

Důležitou součástí práce s přihlašovacími údaji je kromě jejich tvorby i jejich uchovávání. Optimálním případem je, pakliže si uživatel pamatuje přihlašovací údaje k dané službě. S množstvím služeb k nimž je uživatel nucen se přihlašovat, ale často dochází k potřebě zaznamenání si přihlašovacích údajů pro danou službu. Mezi způsoby správy hesel patří:

**Uložení hesla v prohlížeči** mnohé prohlížeče umožňují zapamatování si hesel. O této metodě více 1.1.2.1.

**Správce hesel** využití pro uložení hesel specializovaného programu, takzvaných správců hesel. O této metodě více 1.1.2.2.

**Externí úložiště** používání externích zařízení, jakožto správců přístupových údajů či klíčů. V takovémto případě hrozí riziko odcizení externího zařízení.

**Sešit s hesly** je metoda při níž si uživatel zapisuje přihlašovací údaje do sešitu. Nevýhodou tohoto postupu je možné odcizení sešitu či případné neoprávněné nahlédnutí do něj, při němž může dojít k odcizení přihlašovacích údajů.

**Poznámky** je metoda využívající zapsání si hesla na lísteček. Takovýto lísteček bývá následně umístěn na, pro uživatele, pohodlném místě. Může se jednat o vylepení hesla na monitor počítače či jejich vylepení z druhé strany klávesnice. V obou případech se uživatel vystavuje riziku, že kdokoliv pobývající se v okolí zařízení může přihlašovací údaje odpozorovat. Jakákoliv poznámka může být navíc ztracena či odcizena.

Příkladem, kdy se tato metoda vymstila, je fotografie zveřejněná slovenskou ministryní informatiky, která takto zveřejnila heslo k počítači. [14]

**Zápis do souborů** může se jednat o textový soubor, Excelovou tabulku či poznámky v mobilním telefonu. V případě, že se útočník zmocní přístupu do daného zařízení dochází k možnosti zneužití těchto přihlašovacích údajů. Obzvláště rizikovou je tato metoda v okamžiku, kdy je zařízení ponecháno bez dozoru a odemčené.

**Paměť** Optimálním řešením je, aby si uživatel své přihlašovací údaje pamatoval. S větším množstvím hesel, které dodržují pravidla pro bezpečné přihlašovací údaje, nabývá tento úkon na složitosti a často vede k zjednodušování či recyklaci hesel na úkor jejich bezpečnosti.

[12, 10, 15, 9]

#### 1.1.2.1 Ukládání hesel do prohlížečů

Při vyplňování přihlašovacích formulářů internetové prohlížeče obvykle nabídnou možnost „zapamatovat si heslo“ či jinou významově podobnou zprávu. Pokud uživatel tuto možnost uložení hesla v prohlížeči zvolí, rozlišujeme mezi dvěma variantami okolností přihlášení.

**Uživatel je přihlášen k svému účtu v rámci prohlížeče** (účet Google na Chromu, Mozilla Firefox účet...) V tomto případě dojde k uložení hesla v rámci uživatelského účtu. To umožňuje uživateli k takto uloženým heslům přístup z jakéhokoliv zařízení, na které se přihlásí účtem k prohlížeči. Pokud uživatel pracuje na veřejně přístupném zařízení musí dbát na to, aby se před opuštěním pracoviště odhlásil ze svého uživatelského účtu, neboť by jinak ohrozil své přístupové údaje.

**Uživatel není přihlášen k svému účtu v rámci prohlížeče** Dochází k uložení hesla na zařízení, skrze které uživatel k službě přistupuje. V případě, že se uživatel přihlašuje z veřejně přístupného počítače a zvolí možnost uložení hesla, umožňuje tím přístup k přihlašovacím údajům neznámým a neautorizovaným osobám.

Jelikož si prohlížeč tímto způsobem uloží přihlašovací údaje a bude-li uživatel příště vyzván k jejich vyplnění, prohlížeč je automaticky vyplní a usnadní tak proces přihlašování. [9]

Hesla jsou v prohlížeči uložena v šifrovací podobě. V případě, že si je chce uživatel zobrazit, nikoliv pouze použít k automatickému vyplnění formuláře, bývá vyzván k přihlášení pomocí hesla do zařízení. V případě, že jsou přihlašovací údaje k zařízení kompromitovaná, útočník se díky přístupu k zařízení také může zmocnit veškerých takto uložených hesel. [12]

#### 1.1.2.2 Správce hesel

Správce hesel, častěji známý jako Password Manager, je program jehož cílem je zapamatovávání si hesel namísto uživatele. Přihlašovací údaje uživatele ukládá v šifrovaném digitálním sejfu. Uživatel si je nucen pro přístup pamatovat pouze jedno heslo.

Správce hesel lze rozdělit do dvou kategorií podle jejich řešení a to cloudových a lokálních. Výhodou cloudových správců hesel je možnost přístupu k heslům z více zařízení. Obvykle mají k dispozici i plugin do prohlížečů, který umožňuje automatický vyplnění přihlašovacího formuláře. Nevýhodou je, že vyžadují od uživatele důvěru v cloudové úložiště. Pokud uživatel důvěru postrádá, může v takovém případě uživatel zvolit lokální variantu správce hesel, která ukládá hesla přímo v zařízení. Tímto zařízením nemusí být pouze počítač či mobilní telefon, ale například flash disk. Nevýhodou tohoto řešení je neumožnění využití automatické synchronizace napříč více zařízeními a riziko ztráty dat v případě poškození zařízení na němž se správce hesel nachází.

Zřejmou nevýhodou správce hesel je akumulace hesel na jednom místě. V případě zvolení nedostatečně bezpečného hesla pro přístup k správci se uživatel vystavuje nebezpečí zneužití jeho přihlašovacích údajů. Dochází k nebezpečí i ze strany poskytovatele služby správce hesel, u něhož hrozí riziko, že útočníci objeví v programech zranitelnosti, kterých využijí k prolomení zabezpečení programu. [16]

Do správce hesel by tak uživatel neměl svěřovat nejdůležitější hesla, jako jsou například hesla k internetovému bankovnictví.

### 1.1.3 Jednotné přihlašování

Jednotné přihlašování (Single Sign-On, zkráceně SSO) je metoda umožňující uživatelům přihlašovat se ke službám a aplikacím pouze pomocí jediných přihlašovacích údajů. Díky tomuto uživatel nemusí vytvářet nové přihlašovací údaje pro každou službu.

Existuje mnoho různých služeb a technologií, které podporují jednotné přihlašování. Některé z nejčastěji používaných jsou například Google SSO, Facebook SSO, Microsoft SSO, OAuth a OpenID Connect.

Využívání SSO snižuje zátěž na uživatele, který si nemusí pamatovat další přihlašovací údaje. Tím snižuje riziko zapomenutí hesla. Avšak je nutné, aby uživatel pro SSO volil dostatečně vhodné přihlašovací údaje, protože v případě úniku či prolomení těchto přihlašovacích údajů, ztrácí uživatel kontrolu i nad službami na ně vázanými. Používáním SSO také uživatel prohlubuje svou závislost na poskytovateli služby – například používá-li Facebook SSO je pro uživatele výrazně obtížnější si Facebookový účet zrušit, neboť na něj má navázaný právě další služby.

Služby používané pro SSO mají díky uživatelově aktivitě informace o dalších službách, kterým uživatel věnuje svůj čas a díky tomu mohou lépe sledovat zájmy uživatelů. [17]

#### 1.1.3.1 eduID

Česká akademická federace identit eduID.cz je projekt, jehož cílem je poskytnout členům rámec pro vzájemné využívání identit při přístupech k síťovým službám, které spravuje sdružení CESNET.

Uživatelé jejichž organizace je členem, mohou čerpat následující výhody:

- jedny přihlašovací údaje pro přístup k více aplikacím
- správci aplikace neudržují autentizační data uživatelů, ani autentizaci neprovádí
- autorizace probíhá v kontextu domovské organizace
- federační infrastruktura poskytuje bezpečný způsob výměny informací o uživatelích
- je možné využít hostované infrastruktury o jejíž technickou realizaci a správu poskytovatele identit spravuje CESNET

[18]

#### 1.1.3.2 MojeID

MojeID je česká služba sloužící k autentizaci uživatele na různých webových službách. Provozovatelem MojeID je sdružení CZ.NIC.

CZ.NIC je zájmové sdružení právnických osob založené roku 1998. Hlavní náplní sdružení je provoz registru jmen domén registrovaných pod doménou CZ a zabezpečování provozu domény .CZ. Sdružení se dále zabývá osvětou v oblasti internetové bezpečnosti. [19]

CZ.NIC uchovává data za bezpečnostních standardů, se kterými přistupuje k zabezpečení registru národních domén. Pro přihlášení skrze MojeID se uživatel nepřihlašuje do dané služby, ale přihlašuje se přímo do služby MojeID, díky tomuto opatření koncová služba nemá k dispozici přihlašovací údaje uživatele. MojeID umožňuje uživateli zobrazit jaké údaje koncová služba z profilu požaduje a dovoluje uživateli rozhodnout se, zda je službě chce předat. Pro registraci do služby je nutné vyplnit formulář a ověřit identitu pomocí kódů, které jsou zaslány na telefoní číslo a e-mailovou adresu.

MojeID nabízí dvě ze tří úrovní záruky prostředků pro přístup ke službám veřejné správy a to úrovně „značná“ a „vysoká“. Obě úrovně vyžadují ověření totožnosti.

Úroveň „značná“ umožňuje přístup k většině elektronických služeb veřejné správy jako jsou portály zdravotních pojišťoven, Portál občana či ePortál České správy sociálního zabezpečení. Pro tuto úroveň je potřeba zabezpečit účet buď mobilní aplikací MojeID Klíč, USB/NFC/Bluetooth klíč s úrovní certifikace min. L1 či systémový klíč Windows Hello nebo Android.

Úroveň „vysoká“ umožňuje navíc například online nákup státních dluhopisů. [20]

### 1.1.4 Vícefaktorová autentizace

Vícefaktorová autentizace, také známá jako dvojfázové ověřování, je metoda používaná k zvýšení bezpečnosti při přihlašování uživatele k účtu. Metoda je rozložena na dvě části. V první části zadává uživatel přihlašovací údaje jako jsou přihlašovací jméno a heslo. Následně je po ověření zadání správných údajů vyzván k potvrzení přihlášení. V ten okamžik vstupuje do druhé části autentizace. Ta může probíhat několika způsoby, dle služby k níž se přihlašuje. Následují nejběžnější způsoby druhé části autentizace:

- Uživatel obdrží e-mailovou zprávu na svůj e-mailový účet, který zvolil pro komunikaci se službou. Je vyzván k zadání obdrženého kódu v rámci časového intervalu.
- Uživatel obdrží SMS na telefonní číslo, které zvolil pro komunikaci se službou. Následně postupuje jako v předešlém případě.

- Uživatel je vyzván, aby potvrdil přihlášení skrze mobilní aplikaci.

[21]

### 1.1.5 Odemykaní mobilních zařízení

V České republice k roku 2021 používalo mobilní telefon přes 98 % osob starších 16 let. Z toho v 76 % případech se jednalo o takzvaný chytrý telefon (smartphone). [22] Pro přístup do zařízení je uživateli umožněno zvolit si metodu odemykání mobilní obrazovky. Uživatel si může zvolit i nevybrat žádnou z metod a nechat tak zařízení volně přístupné. Základní metody odemykání mobilního zařízení jsou následující:

**PIN** je metoda využívající kombinace číslic. Pro bezpečný PIN je doporučená minimální délka 6 znaků a požadavek na netriviální kombinaci těchto znaků (příklad triviálních sekvencí 111111, 123456 či 654321). Jedná se o snadno zapamatovatelnou metodu, která lze hůře odpozorovat a není závislá na okolních světelných podmínkách.

**Heslo** je metoda využívající kombinaci znaků abecedy, platí doporučení popsaná v 1.1.1.

**Gesto** je metoda při níž uživatel přejede po obrazovce v určitém vzoru, obvykle uživatel vytváří vzor spojením několika z devíti bodů na mobilní obrazovce. Tato metoda zabezpečení je snadno odpozorovatelná a lze uhodnout i z mastnoty displeje. Většina uživatelů navíc zvolí jako vybraný vzor libovolné písmeno. Počet kombinací, kterými lze pohodlně znak vytvořit je taktéž omezený.

**Rozpoznání obličeje** je metoda využívající kameru pro nasnímání obličeje. U starších zařízení je riziko, že mobilní telefon se odemkne i v případě, že se bude jednat o fotografii. V současné době dochází k nástupu 3D skenerů s infračerveným senzorem. Ten vytváří hloubkovou mapu obličeje a následně provádí výpočty zda dochází ke schodě s dříve naskenovaným obličejem. Díky tomuto postupu dochází k zvýšené toleranci odlišných světelných podmínek.

**Otisk prstu** je metoda při níž uživatel naskenuje otisk svého prstu pro přístup k zařízení. Tato metoda mnohdy vyžaduje opakované pokusy pro přihlášení a je závislá na více faktorech jako jsou čistota prstů. U starších zařízení bylo možné tuto metodu obejít například využitím voskového odlitku prstu. Současné pokročilé skenery si uchovávají informaci elektrického náboje otisku a na jeho základě provádějí výpočty zda se jedná o otisk uživatele.

Jak rozpoznávání obličeje, tak otisk prstu je náchylný k zneužití, jestliže se uživatel nachází ve spánku či bezvědomí. Obě tyto metody navíc často vyžadují zvolení záložní metody pro přístup k zařízení, kterými jsou buď PIN, heslo či gesto. V případě nevhodně zvoleného přístupového údaje sekundární metody, lze skrze ně snadno obejít bezpečnostní opatření dané biometrické metody .

### 1.1.6 Útoky na přihlašovací údaje

**Útok hrubou silou** lépe známý jako brute force attack, je metoda používaná k zajišťování přihlašovacích údajů. Útočník zkouší jako možné heslo všechny existující kombinace znaků, dokud nezjistí skutečné heslo. Tento způsob je časově velmi náročný. Jeho úspěšnost je závislá na délce hesla, složitosti hesla a výpočetním výkonu použitého počítače.

Webové stránky se proti těmto pokusům mohou chránit omezením pokusů přihlášení doprovázenými časovými limity na opětovné přihlášení. Dále zablokováním účtu v případě neúspěchu po vyčerpání předem stanovených počtů pokusů, pro jehož odblokování je pak uživatel nucen učinit další kroky. Další metodou může být využití CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart). [23] CAPTCHA je test, který se

používá ve snaze automaticky odlišit skutečného uživatele od robotů, například při vkládání komentářů, při registraci…Test spočívá v zobrazení obrázku s deformovaným textem, který má uživatel přepsat do příslušného vstupního políčka. Předpokladem tohoto testu je schopnost uživatele rozeznat i deformovaný text a robotova neschopnost rozeznání.

**Reverzní brute-force** takto se nazývá situace, kdy hacker oplývá znalostí hesla a k danému heslu se snaží přiřadit správný účet.

**Slovníkový útok** je druh útoku před kterým si útočník připraví databázi slov – slovník – jimiž bude útočit na uživatele. V rámci tohoto útoku jsou často využívány seznamy často používaných hesel. Jedná se o poměrně rychlou metodu, úspěch záleží na velikosti slovníku a na tom, zda oběť používá heslo, které lze pomocí slovníku odhadnout.

Slovník vytvořený pro potřeby slovníkového útoku je často založen na mateřském jazyce cíle a může obsahovat mimo celá slova také jejich zkrácené varianty, oblíbené části písní, pořekadel…

**Hybridní útok** je druh útoku využívající kombinace předchozích technik. Dochází k využívání základních znalostí o cílovém uživateli, jako je jeho jméno, rok narození či jiné dohledatelné osobní informace.

**Credential stuffing** je útok využívající dat z databází jiných služeb. Útočník má tedy k dispozici kompletní přihlašovací údaje a hlavními cíli se stávají uživatelé využívající stejné či podobné přihlašovací údaje pro více služeb. [24]

**Sniffing** je metoda pro získávání informací pomocí sniffer programů. S těmito programy se jedinec může setkat například při práci na veřejné nezabezpečené Wi-Fi síti.

Sniffer je program umožňující odposlouchávání všech protokolů, které počítač přímá či odesílá. Využívá se například pro odposlouchávání přístupových jmen a hesel, čísel kreditních karet…

Obětí útoku nemusí být vždy koncový uživatel, ale mohou se jí stát přímo služby, které mají k dispozici databázi s přihlašovacími údaji. Mluvíme pak o úniku přihlašovacích údajů a vejde-li takováto událost ve známost, měl by uživatel reagovat okamžitou změna hesla k inkriminované službě. Jelikož mnoho uživatelů používá stejná přihlašovací údaje k více službám, může v důsledku tohoto úniku dojít k bezpečnostnímu ohrožení dalších účtů.

Aby služby předcházely ohrožení svých uživatelů, neměly by hesla uchovávat v podobě v jaké je uživatel zadává, ale měli by ukládat jejich zahashovanou podobu, která vzniká použitím hashovací funkce. Princip hashovacích funkcí je snadný přechod z hesla do hash klíče a snaha znemožnit z hash klíče získání hesla. Ne všechny hashovací funkce jsou vhodné a mnohé již zastaraly a tudíž ani v případě jejich užití službou není při úniku uživatel v bezpečí před zneužitím jeho účtu.

NÚKIB v souvislosti s uchováváním hesel vydává minimální požadavky na kryptografické algoritmy. Tyto požadavky jsou povinné pro subjekty, kterých se týká zákon č. 181/2014 Sb. – o kybernetické bezpečnosti. Pro ostatní subjekty se jedná o doporučení.

## 1.2 Sociální inženýrství

*„Sociální inženýrství obchází všechny technologie, včetně firewallů.“*

*Kevin Mitnick*

Následující kapitola a její podkapitoly primárně čerpají z [25], [26] a [27].

Sociálním inženýrstvím označujeme soubor metod a technik, jejichž cílem je manipulovat s lidským chováním a názory. Tato technika běžně nalezne uplatnění v oblastech marketingu, politiky, vzdělávání, psychologie…Zde je několik příkladů legálního použití sociálního inženýrství:

- snaha ovlivnit názor konzumenta na určitý produkt v rámci marketingové kampaně

- snaha vytvořit určitý obraz značky či produktové řady
- časově omezené nabídky a slevy za účelem vyvolání pocitu naléhavosti
- věrnostní programy s odměnami a slevami se snahou přimět zákazníka k opakovaným nákupům
- apelování na názory voličů během kampaní
- snaha rodiče vychovat svého potomka

V následujícím textu budeme pracovat s pojmem sociálního inženýrství v rámci kontextu informační bezpečnosti. Pro tyto účely budeme sociální inženýrství definovat následovně:

▶ **Definice 1.1** (Sociální inženýrství)**.** *Účelová manipulace osob s cílem přimět je k provedení určité akce nebo k vyzrazení důvěrné informace.*

Sociální inženýrství je jednou z nejjednodušších a zároveň nejúčinějších metod. Cílí na uživatele, jakožto na nejslabší článek bezpečnostního systému. Člověk na rozdíl od stroje má emoce a ty lze zneužít. Útočník tak často využívá strachu, nepozornosti a jiných lidských vlastností za účelem vlastního obohacení.

Policie považuje za velmi závažné použití sociálního inženýrství na dětech. Může docházet k podvodnému lákání intimních materiálů či záběrů z webových kamer s nimiž následně může být obchodováno. V takovýchto případech je mnohdy samotná oběť výrobcem a distributorem dětské pornografie.

### 1.2.1 Útok pomocí sociálního inženýrství

Útočník provádějící útok pomocí sociálního inženýrství využívá následujících tří způsobů a jejich kombinací:

**Sběr volně dostupných informací** Klíčovým předpokladem úspěchu sociálního inženýrství je dostatek informací o zvoleném cíli útoku. Z toho důvodu dochází před samotným útokem k průzkumu informací, které lze o oběti dohledat. V této fázi může útočník prohledávat webové stránky společnosti a další veřejně přístupné rejstříky, ze kterých lze zjistit například telefonní čísla, jména a bydliště osob. Dobrým zdrojem informací jsou sociální sítě, na kterých uživatelé často sdílí osobní údaje, včetně informací o současné poloze, finanční situaci a politických názorech.

Další technikou, kterou útočník využívá k získávání informací jsou podvodné webové služby. Zde se může jednat o podvržení stránek společností, do kterých se uživatel přihlásí a tímto způsobem se útočník dostane k přihlašovacím údajům. V takovém případě jsou uživatelé využívající stejné přihlašovací údaje k více službám obzvláště zranitelní. Útočník může využívat také aplikací, které si uživatel nainstaluje na své mobilní zařízení a povolí jim přistupovat k důvěrným informacím – například aplikace kalkulačky přistupující ke kontaktům, GPS či souborům.

**Fyzický útok** Útočník se vydává například za pracovníka servisové agentury (servis tiskáren, pracovník údržby…), policejního příslušníka, zaměstnance plynárny, bankovního poradce…Cílem je získat informace zevnitř, k tomu může docházet i pomocí prohledávání odpadků.

**Psychologický útok** Pro psychologický útok je důležité budování vztahů a důvěry. To je časově náročná operace a může docházet k opakované komunikaci. Útočník cílí na lidské slabiny jimiž je například pocit strachu. Zde může docházet k využívání obav o finanční situaci či politických událostí.

Příkladem psychologického útoku je útočník představující se jako pracovník banky, který informuje o napadení uživatelského účtu. Snahou je následně vyvolat v oběti paniku a vytvořit stresovou situaci, která vyžaduje okamžitou akci – tedy nedat možnost oběti o situaci dostatečně přemýšlet. V takovýchto případech útočník může oběť vyzvat, aby převedla své finanční prostředky na jiný, bezpečný, účet, který je právě pod správou útočníka.

## 1.2.2 Výběr technik sociálního inženýrství

### 1.2.2.1 Phishing

Phishing – překládán jako „rybaření“, „rhybaření“, „házení Phishing udic“ – je metoda jejímž účelem je zcizení digitální identity uživatele – jeho přihlašovacích údajů, čísel bankovních karet a účtů…– za účelem jejich zneužití. Zprávy jsou šířeny převážně elektronickou poštou a jsou maskovány za důvěryhodného odesílatele. Může se jednat o padělané dotazy od banky s žádostí o zaslání přihlašovacích údajů nebo přímo přihlášení k falešné stránce.

Phishingové útoky často cílí na velké skupiny, například příjemcem e-mailové zprávy může být 10 000 uživatelů a vycházejí z předpokladu, že i malé procento uživatelů, které se na danou zprávu chytí, bude v množství dostatečné – 1 % z 10 000 uživatelů je stále 1 000 uživatelů, často tyto procenta bývají vyšší.

Phishingový útok probíhá v následujících krocích:

**Plánování útoku** Během této fáze dochází k výběru cílové skupiny a metody, která bude k útoku použita. Jsou vyhodnocována rizika s útokem spojená.

**Vytváření vhodných podmínek** Během této fáze je vytvářeno technické řešení phishingového útoku.

**Vlastní útok** Během této fáze je e-mail doručen uživatelům. Úspěšnost útočníka je závislá na zpracování e-mailu a dalších faktorech jimiž je například uživatelova zkušenost a informovanost.

Útočník se často vydává za banku informující uživatele o možnosti zneužití jejich přihlašovacích údajů a nabízející možnost zabezpečení účtu, tím že se na něj přihlásí. Odkaz, který má uživatele přesměrovat na stránku internetového bankovnictví však vede na podvodnou stránku, která vzhledově odpovídá očekávané stránce a proto uživatel své přihlašovací údaje zadá.

**Sběr dat** Dochází k sbírání dat, které oběti chycené na phisihingový útok útočníkovi sdělí.

**Profit z útoku** Dochází k zneužití získaných dat. Pomocí nich útočník přistupuje k účtům a převádí finační prostředky na vlastní účet.

Rozlišujeme mezi několika dalšími druhy phishingu, jako jsou:

**Spear Phishing** je cílenou formou phishingového útoku. Na rozdíl od plošného phishingu Spear Phishing má přesně zvolený cíl svého útoku.

Za účelem co největší uvěřitelnosti útočník provede průzkum, aby získal co nejvíce informací o svém cíli – struktura organizace, jména pracovníků…– a následně vytvoří e-mailovou zprávu, která působí jako by byla odeslána legitimním zaměstnancem, zaměstnavatelem, obchodním partnerem. To vše má vyvolat co nejméně podezření ze strany oběti, která bude tímto způsobem ochotnější stáhnout požadovaný program či provést jiný úkon (například proplatit fakturu). Cílovou skupinou jsou často ekonomové, účetní a další skupiny pracující s peněžními obnosy.

**Vishing** je forma phishigu, který probíhá v podobě telefonického hovoru. Během hovoru se útočník snaží z uživatele vylákat citlivé informace. Útočník často falšuje svou identitu a vydává se za skutečné osoby. V současné době jsou útočníci schopni přepsat i číslo příchozího hovoru, které se uživateli zobrazí, když hovor zvedá. K tomu dochází skrze takzvaný spoofing, který umožňuje napodobit legitimní číslo a tím prohloubit iluzi, že útočník je tím, za koho se vydává. Hovor se tak může tvářit, že je například skutečně volán z telefonního čísla policejního příslušníka či bankovního poradce. Uživatel by měl proto zavěsit a zavolat na číslo osoby, které si dohledá na důvěryhodném zdroji. Neměl by použit funkce telefonu „zavolat zpět".

**Smishing** je formou phishingu probíhající pomocí SMS zpráv. Hlavním cílem bývá snaha donutit uživatele aby proplatil peněžní částku – například zavoláním na placenou linku – či klikl na URL odkaz.

**Homografový útok** je formou phishingu, v rámci kterého dochází k zaměnění vzhledově podobných znaků za znaky jiné, například z jiné znakové abecedy (například využitím řecké abecedy, cyrilice…). K útoku dochází pomocí na první pohled k nerozeznatelným URL odkazů, na které když uživatel, klikne dostane se na podvodnou webovou stránku.

#### 1.2.2.2 Pharming

Pharming – též překládán jako „rhybaření" – je metoda používaná na internetu s cílem získání citlivých osobních údajů. Principem této metody je napadení DNS serveru a přepsání IP adresy, což způsobí přesměrování uživatele na falešnou internetovou stránku – internetové bankovnictví, e-mail, sociální síť…– i přes zadání správné URL adresy do prohlížeče. Jedná se o phishingu příbuznou techniku.

K webovým stránkám uživatel přistupuje pomocí doménových jmen, které následně přesměrují uživatele na příslušnou IP adresu, například *seznam.cz* → 77.75.77.222 či *google.com* → 172.253.63.100. Tyto doménová jména jsou uchovávána na DNS serverech. Pharming je právě útokem na tyto DNS servery, na které místo původní IP adresy vloží svou vlastní. Tímto způsobem dochází k přesměrování uživatele přistupujícího k webové stránce pomocí doménového jména na stránku podvodnou, často velmi věrně imitující originál.

Dalším způsobem pharmingu je napadení zařízení uživatele pomocí malwere, který má za cíl odklonit přenos souborů na falešnou webovou stránku.

#### 1.2.2.3 Baiting

Baiting je technika cílící na zvědavost oběti. Dochází k využívání především fyzických médií jimiž jsou například USB disky, CD či DVD, které uživatelé nacházejí ve veřejných prostorech jako je knihovny, schody, výtahy…Může se také jednat o soubory dostupné na internetu, například filmy, PC hry, hudbení soubory…

Cílem Baitingu je apelovat na uživatelovu zvědavost, která ho přiměje, aby zařízení použil či stáhl. Jsou infikovány totiž škodlivým software, který se snaží infikovat uživatelovo zařízení a případně systémy, k nimž je takové zařízení připojeno.

#### 1.2.2.4 Blagging

Blagging je metoda při níž se útočník vydává za oběti známou osobu – může jít například o partnera, blízkého přítele, kolegu z práce či nadřízeného. Útočník často využívá identit reálných osob, čímž činí svůj čin uvěřitelnějším. Blagging často vyvolává pocit časové tísně a mnohdy cílí na soucit či přátelství. Cílem útoku je přimět oběť k převodu finančního obnosu na účet útočníka. Obvyklou metodou zde bývá zpravidla poutavý a naléhavý příběh. [28]

Příkladem může být naléhavá situace, při níž blízký přítel potřebuje okamžitou peněžní pomoc. Jedinec zde jedná v dobré víře, že pomáhá svému blízkému a tuto částku poskytne. Dalším

příkladem může být žádost o uhrazení akutního platebního příkazu, který obdrží účetní od svého nadřízeného.

#### 1.2.2.5 Pretexting

Pretexting je druhem sociálního inženýrství, při němž dochází k vytváření smyšleného scénáře za účelem přesvědčit oběť, aby učinila určitou akci či sdělila potřebné informace. Během útoku dochází k smíšení lží s dříve získanými pravdivými informacemi.

Útočník se snaží během útoku vydávat za jinou osobu, zde je pak obzvláště důležitý jazyk, který útočník používá. Pakliže nezná vhodné výrazy či se chová nepřesvědčivě a nedisponuje příslušnými rekvizitami, hrozí, že vyvolá ve své oběti pochybnosti o své totožnosti.

#### 1.2.2.6 Quid pro quo

Quid pro quo neboli „něco za něco“ je technika, která se zaměřuje na výměnu služby za protislužbu. Může se jednat o pomoc s problémem či odměnu v jiné podobě – sladkost, finanční odměna…

Obvyklou taktikou je útok podvodníka vystupujícího jako IT technik. Ten kontaktuje zaměstnance určité společnosti a zatímco řeší jejich problém, přesvědčí je ke stažení programu, díky kterému dojde k infikaci koncového zařízení.

Lidé jsou navíc ochotni prozradit důvěrné informace o svých přihlašovacích údajích – například, že obsahují datum narození, jméno mazlíčka…– což jsou informace, které lze následně dohledat.

#### 1.2.2.7 Shoulder Surfing

Shoulder Surfing je taktika, během níž dochází k odpozorování důležitých informací z displeje uživatelova zařízení – tedy pomocí „koukání přes rameno“. Tímto způsobem může uživatel přijít o své přihlašovací údaje, nejen k samotnému zařízení, ale například k internetovému bankovnictví.

Uživatel by si měl být vědom svého okolí, tedy například zda za ním nikdo nestojí právě když se přihlašuje či nestojí zády k oknu. V případě volby dostatečně silného hesla navíc může uživatel předcházet jeho odpozorování, právě z důvodu jeho složitosti.

#### 1.2.2.8 Tailgating

Tailgating je metoda využívaná především ve velkých organizacích, kde se mezi sebou všichni zaměstnanci nutně neznají. Díky tomu je možné pro útočníka předstírat, že je legitimním zaměstnancem a využít tuto lež k přístupu do omezených prostor – například předstíráním, že útočník ztratil svou legitimační průkazku a žádá o pomoc při vstupu do budovy. Díky tomu může dojít například k odcizení dat či nainstalování škodlivého kódu do zařízení na pracovišti.

#### 1.2.2.9 Trashing

Trashing je metoda využívající důvěrných informací, které skončí v koši. Trashing vychází z anglického slova „trash“, což znamená „odpadky“ či „smetí“. Využívá nepozornosti uživatelů, kteří důvěrné informace hodí do koše bez toho, aby je skartovali či jinak omezili jejich čitelnost.

### 1.2.3 SPAM

SPAM je hromadné šíření nevyžádaného sdělení často reklamního charakteru, obecněji jde o veškeré nevyžádané zprávy, tedy například i o zprávy obsahující viry.

SPAM získal své jméno po produktu Spam společnosti Hormel Foods, přičemž se jednalo o masovou konzervu. Spam se proslavil během 2. světové války a po ní, neboť nahrazoval maso

a měl dlouhou dobu trvanlivosti. Britská skupina Monthy Python použila produkt Spam ve svém skeči o objednávání jídla. Právě zde byl poprvé použit pro označení nevyžádaného produktu, což se následně přeneslo právě do informatiky.

Spam může například obsahovat:

- obchodní/reklamní sdělení
- edukativní sdělení (pozvánky na lekce, kurzy…)
- hoax (řetězové zprávy, uvádějící zkreslené, nepravdivé či zavádějící informace)
- kriminální (obsahující malware či odkazující na podvodné stránky či stránky se škodlivým kódem)

#### 1.2.3.1 Scam

SPAM obsahující kriminální či jiný podvodný obsah je nazýván scam (v překladu „podvod“). Mezi scam lze zařadit například phishing, hoax, podvodné loterie a nabídky…

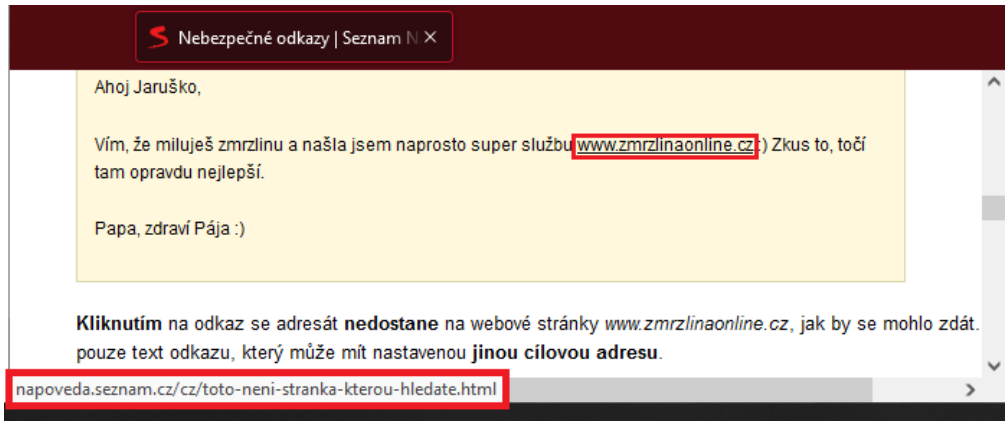
Jedním z nejznámějších scamů je scam 419, známí také jako Nigerijské dopisy. Tento druh podvodného jednání vznikl již před nástupem internetu, ale právě ten umožnil scamu masově se rozšířit. Cílem je vylákat z uživatele peníze či bankovní údaje za účelem zcizení peněžní částky. Nejznámější podoba scamu 419 je oslovení uživatele ohledně zdědění velkého peněžního obnosu, od jehož získání dělí jedince pouze několik jednoduchých kroků.

### 1.2.4 Rozpoznání technik sociálního inženýrství

**Překlady** Zprávy jsou často překládány do češtiny z jiného jazyka. To se projevuje v nedokonalém překladu, chybné větné skladbě, skloňování a jiných jazykových nedostatcích.

**Překlepy** Uživatel musí dbát na detaily. Častou taktikou je záměna vzhledově podobných písmen například v adrese odesílatele e-mailové zprávy.

**Odkazy** Adresy odkazů mohou často připomínat cílovou adresu, ale jsou doplněné o překlepy či znaky jiné abecedy, které jsou vzhledově podobné. Vzhled adresy v e-mailu také nemusí odpovídat adrese na kterou bude uživatel skutečně přesměrován. Jestliže uživatel přejede myší přes odkaz, webové prohlížeče v levém dolním rohu zobrazí adresu, díky tomu si může ověřit, zda se odkazy schodují či odkaz vede na jinou adresu.




**Obrázek 1.1** Náhled na odkazy, screenshot stránky [29].

**Akce** Důležité je uvědomit si, zda by služba dané informace měla vyžadovat. Při přihlašování do internetového bankovnictví by měl uživatel zbystřit pokud je po něm například požadován PIN kód spolu s číslem kreditní karty či jinými údaji.

## 1.3 Software

Software je sada programů, které zpracovávají data či vykonávají konkrétní úlohu. Software lze rozdělit na:

- systémový software – vstupně/výstupní systémy, operační systémy, grafické operační systémy…
- aplikační software – aplikace, jednoduché utility, komplexní programové systémy…
- firmware – programy ovládající hardware

### 1.3.1 Malware

Malware je složenina anglických slov „malicious software“, což je překládáno jako „škodlivý software“ či „škodlivý kód“. Jedná se o označení pro software, který se využívá k narušení činnosti informačních systémů, zisku informací či využití přístupu k informačnímu systému. Malware je schopen vykonávat více činností zároveň, může se tedy současně šířit a zároveň získávat informace z napadeného systému.

Malware se může šířit mnoha způsoby. Například pomocí přenosového paměťového média (CD, DVD, USB disk…) dojde k infikování zařízení v okamžiku, kdy uživatel médium připojí. Jednou z nejčastějších metod šíření malware je stažení spustitelného souboru z internetu a následné spuštění staženého souboru. Tyto soubory se mohou maskovat za nespustitelné soubory jako jsou obrázky (jpeg, png), textové soubory, audiovizuální soubor (film, seriál) či jiné programy. Malware se také může nacházet v příloze e-mailové zprávy, přímo v těle e-mailu či na webové stránce samotné.

Falešným antivirem nazveme program vydávající se za antivirus v rámci předstírání legitimního fungování, provede útok na zařízení a objeví jeho zranitelnosti.

Malware má mnoho druhů, které jsou pojmenovány podle činnosti, kterou provádějí:

**Adware** Jedná se o zkratku „advertising supported software“, tedy „software podporující reklamu“. Adware zobrazuje reklamy například formou pop-up okna. Adware může být spojen i se spywarem, tedy kromě obtěžujících vyskakujících oken na obrazovce i sledovat činnosti uživatele.

**Spyware** Je zkratka „spy“ a „software“ tedy „špehující software“. Pomocí spyware jsou získávána data o provozu informačního systému a to bez vědomí a souhlasu uživatele. Součástí dat mohou být osobní a důvěrné informace o uživatelných či společnosti, stejně jako informace o chování uživatele.

Spyware může být i součástí jiných volně šířených programů (například zakoupených her), v takových případech je činnost spyware ošetřena ve smluvních podmínkách a uživatel tak souhlasí s monitorováním jeho aktivit.

**Vir** je program či závadný kód, který sám sebe připojuje k existujícímu spustitelnému souboru. Virus se šíří v momentě, kdy dojde ke spuštění tohoto souboru.

Projevy viru jsou různé, může se jednat o vyhrávání melodie, zahlcení systému, změnu či zničení dat. Je možné viry rozlišovat podle způsobu, kterým se projevují či toho jaké soubory viry napadají.

**Červ** je program podobný viru, který nepotřebuje žádný spustitelný soubor, neboť je šířen samostatně. Napadený systém je schopen odeslat další kopie sami sebe k dalším uživatelům pomocí síťové komunikace. Červi jsou navíc schopny analyzovat bezpečnostní slabiny napadeného systému a z tohoto důvodu jsou využívaný k hledání bezpečnostních mezer.

**Trojský kůň** je počítačový program obsahující skryté funkce s nimiž uživatel nesouhlasí či o nich neví. Bývá připojen k jinému programu, bezpečnému programu či aplikaci či se sami za neškodný program vydávají. Trojský kůň není schopen samostatného šíření. Aktivovaný trojský kůň je možné využít k mazání, upravování, blokaci či ničení dat, nebo například k narušení běhu systému.

Backdoor (v překladu „zadní vrátka“) je druhem trojského koně, který slouží k napadení a případnému ovládnutí napadeného počítače na dálku.

RAT (Remote Access Trojan) je druh trojského koně, který umožňuje útočníkovi převzít kontrolu nad zařízením. Obvykle dá o sobě útočník vědět tím, že pošle oběti z vlastního e--mailového účtu zprávu, ve které vysvětluje, že získal kontrolu nad přihlašovacími údaji a má přístup i k webkameře. Následně často dochází k vydírání na základě toho, že díky webkameře získal intimní záběry, které zveřejní nedojde-li k platbě.

**Rootkit** je pojem označující technologie sloužící k maskování přítomnosti malware v napadeném systému. Samy o sobě nejsou složité, ale mění chování operačního systému či jeho částí tak, aby uživatel nevěděl o existenci škodlivých programů v zařízení.

Rootkit může cíleně napadat i specializované programy, zejména antiviry. V takovém případě pak dochází k prodloužení doby, než je škodlivý program v systému odhalen.

**Keylogger** je program pro detekci stisknutí kláves na uživatelově počítači. V případě, že program zaznamená stisknutí klávesy, zapíše záznam o jejím stisknutím nejčastěji do textového souboru. Tímto způsobem program sleduje chování uživatele. Jelikož zaznamenává veškeré stisknutí klávesnic, může dojít k situaci, kdy se uživatel na daném počítači přihlašuje k účtu a jsou zaznamenány i jeho přihlašovací údaje. V takovém případě se jedná o spyware a uživatel se proti takovémuto druhu programu může chránit antispywarovými programy. [30]

**Ransomware** je malware, který omezuje či brání uživateli v používání systému do doby, než je zaplacena požadovaná peněžní částka. Chová se tedy jako vyděrač, který drží uživatelova data jako rukojmí.

Rozlišujeme dva druhy ransomware. První typ omezí funkčnost celého počítačového systému a neumožní uživateli ho jakkoliv používat. Druhý typ (crypto-ransomware) ponechá počítačový systém funkční, ale uzamkne či jinak znepřístupní data uživatele. Data jsou zašifrována a uživatel je vyzván k provedení platby, obvykle v podobě virtuální měny jako je například Bitcoin. Platby mívají stanovený časový rámec. Zde mohou zasáhnout prostřednici (mediátoři), kteří s útočníkem mohou případně vyjednat snížení požadované částky.

### 1.3.2 Makra

Makra jsou pokročilé sady pravidel z balíčku Microsoft Office a mohou je obsahovat soubory vytvořené například v Excelu, Wordu či PowerPointu. Právě makra v případě, že uživatel povolí jejich spuštěný, jsou schopny napáchat mnoho škod. V případě, že se je útočník rozhodne použít, může pomocí nich nainstalovat škodlivý soubor či vykonat jiné úkony. Z tohoto důvodu jsou ve výchozím nastavení veškerá makra Microsoftem vypnuta a uživatel je musí sám povolit. To by měl dělat pouze v případě, že je dobře obeznámen se souborem, který makra vyžaduje.

Přípona souboru podporující makra končí na „m“, například „.docm“, „.xlsm“, „.pptm“ …[31]

### 1.3.3 Ochranné opatření

Obecnými doporučeními pro ochranu zařízení a dat na zařízeními jsou:

**Antivirové programy** Antivirové programy, známé také jako antiviry, slouží k vyhledávání virů (jednou nebo více různými technikami), jejich odstranění a léčení napadených souborů. Antivirové programy mohou také zálohovat a obnovovat systémové oblasti na disku, ukládat kontrolní informace o souborech, poskytovat informace o virech…

Důležitou součástí využívání antivirových programů je jejich aktualizace, vždy pokud možno co nejdříve. Nedochází-li k takovéto aktualizaci, není antivirový program vybaven k rozeznání a práci s nově se objevivšími viry.

**Aktualizace** Aktualizace obecně slouží k vylepšení stávajícího programu. Toto vylepšení může být například přidáním nové funkce či grafiky. Důležitou částí aktualizací je však oprava bezpečnostních děr a chyb v programu. Jelikož dochází na poli informatiky k neustálému vývoji, je nutné náležitě reagovat a opravovat bezpečnostní opatření (vylepšovat zastaralé bezpečnostní opatření, předcházet zranitelnosti antiviru).

**Firewall** Firewall slouží k zabezpečení síťového provozu mezi sítěmi. Slouží jako kontrolní bod rozhodující se podle nastavených pravidel, který rozhoduje, co pustí dovnitř zařízení a co ven tak, aby zařízení zůstalo v bezpečí.

**Zálohy** Pro předcházení ztráty důležitých dat je vhodné soubory zálohovat. Pro tyto účely může uživatel použít například USB flash disk či cloudové uložiště. Je vhodné, aby uživatel dbal na bezpečnost a zvolil důvěryhodné řešení, případně data například zašifroval.

**Stahování** Uživatel by měl dbát na to z jakých zdrojů stahuje obsah do svého zařízení. V případě, že stahuje a instaluje software, měl by využívat oficiálních zdrojů (oficiální stránka produktu, obchod s aplikacemi…).

V případě, že uživatel stahuje aplikace do telefonu, měl by využívat služeb obchodů s aplikacemi jako je například Google Play, Galaxy Store či App Store. Aplikace v nabídce obchodů prošly bezpečnostní kontrolou, která však není bezchybná. Škodlivé aplikace je tak možné stáhnout i jejich prostřednictvím. Při jejich výběru by tedy měl uživatel kontrolovat recenze dalších uživatelů a podezřelé hodnocení aplikace.

**Oprávnění aplikací** Uživatel by si měl uvědomovat jaké oprávnění nainstalovaným aplikacím povoluje. Aplikace bez patřičných oprávnění nemůže částečně či zcela fungovat. Je důležité, aby zde uživatel vyhodnotil zda daná aplikace má k daným datům přistupovat. Například navigace ke svému fungování potřebuje polohu, ale například kalkulačka vyžadující přístup ke kontaktům a zprávám, by měla uživatele zarazit a donutit ke zvážení.

Doporučení v zájmu bezpečného připojení k internetu a internetovou komunikaci jsou:

**Veřejné Wi-Fi sítě** Uživatel by měl být při práci s veřejnými Wi-Fi sítěmi opatrný, protože komunikace na dané síti lze odposlouchávat. Útočník tak může vytvořit vlastní Wi-Fi nebo se na nějakou otevřenou Wi-Fi síť připojit a odposlouchávat komunikaci na ní provozovanou. Tímto způsobem může dojít k odposlechnutí například přihlašovacích údajů.

**HTTPS** Protokol HTTPS (Hypertext Transfer Protocol Secure) slouží k zabezpečené komunikaci přes síť, obzvláště pak na Inetenetu. Komunikace mezi stránkou opatřenou HTTPS a webovým prohlížečem je šifrovaná. To má za cíl chránit jednání uživatele na dané webové stránce před odposlechnutím.

**Mobilní data, hotspot** internet od standardních mobilních operátorů nabízí bezpečnou alternativu k přístupu na internet. Výhodou mobilního připojení je možnost toto připojení sdílet pomocí hotspotu s dalšími zařízeními. Je vhodné dodržovat zásady bezpečných přihlašovacích údajů a heslo pro hotspot zvolit vhodně.

**VPN** VPN (virtual private network) je zkratka označující šifrované připojení k jinému sytému. Jedná se o službu jejíž cílem je zajistit maximálně soukromé připojení k internetu. Vše co uživatel v rámci internetu dělá prochází přes VPN a ta to činí pro útočníky nečitelným.

VPN původně vznikla k vzdálenému přístupu k pracovním diskům či systémům. Umožňuje připojit se uživateli z domova do pracovní sítě a chovat se jako kdyby byl se zařízením přímo na pracovišti.

**Koncové šifrování** Koncové či end-to-end šifrování slouží pro zabezpečení komunikace mezi uživateli. Jeho cílem je zajistit přenos dat proti odposlechu – tedy aby útočník neměl možnost odposlechnout zprávy v jejich nešifrované podobě a dostat se tak k důvěrným informacím. Klasické SMS koncové šifrovaní nepoužívají, stejně jako většina e-mailových služeb. Ani komunikační aplikace (messengery) end-to-end nutně nevyužívají – například u Facebook Messenegeru je nutné end-to-end šifrování zapnout a zahájit takzvanou „tajnou konverzaci“, což lze pouze v rámci mobilní aplikace.

| Komunikátor | Provozovatel | Státní jurisdikce | End-to-end šifrování | End-to-end šifrování pro skupinové konverzace | Podpora češtiny | Nevyžaduje osobní údaje, e-mail a/nebo telefonní číslo | Zdarma | Lze nastavit, aby se zprávy po čase smazaly | Aplikace a/nebo provozovatel nespojen s bezpečnostními incidenty** | Multiplatformní (iOS, Mac, PC, Android) |
|---|---|---|---|---|---|---|---|---|---|---|
| Threema | Threema GmbH | Švýcarsko | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ |
| Signal | Signal Technology Foundation | USA | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ |
| Telegram | Telegram Messenger Inc. | Velká Británie/ UAE | —* | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ |
| WhatsApp | Meta (dříve Facebook) | USA | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ |
| Messenger | Meta (dříve Facebook) | USA | —* | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ |
| Google messages | Google | USA | —* | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ |
| Apple iMessages | Apple | USA | —* | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ | ✗ |

**Obrázek 1.2** Porovnání komunikačních aplikací, převzato z [32].

**Soukromí** Aplikace a sociální sítě sledují chování uživatele v rámci své služby. Získané data pak používají například pro cílenou reklamu. Tyto informace se dají dále zneužít, jak se ukázalo, například v rámci skandálu s Cambride Analytica, která data získaná od Facebooku využila v rámci volebních kampaní.

NÚKIB vydal 8. března tohoto roku varování před aplikací TikTok vlastněnou čínskou společností ByteDance. Varování zakazuje instalaci a používání aplikace na pracovních zařízeních všem osobám spadajícím pod zákon o kybernetické bezpečnosti. [33]

Uživatel by si měl být vědom těchto skutečností a dle toho pečlivě zvažovat svůj postoj k daným službám.

# Kapitola 2
# Český školský systém

*„Každý má právo na vzdělání. Vzdělání nechť je bezplatné, alespoň v počátečních a základních stupních. Základní vzdělání je povinné. Technické a odborné vzdělání budiž všeobecně přístupné a rovněž vyšší vzdělání má být stejně přístupné všem podle schopností.“*

*Všeobecná deklarace lidských práv, článek 26*

## 2.1 Vývoj základního školství v Českých zemích

Tato kapitola primárně čerpá z [34], [35] a [36].

V roce 1774 byl Marií Terezií vydán císařský výnos Všeobecný školní řád, který reformoval školství na území Habsburské říše a zaváděl šestiletou výuku pro děti od 6 do 12 let v rámci níž měli být žáci vyučováni v psaní, čtení a počtech. Přechod na povinnou školní docházku nebyl okamžitý. Bylo nutné vybudovat dostatečné množství škol a vyučit učitele, kteří by pokryli výuku. Směrem k povinné docházce pak pobízely dekrety vyžadující úspěšné vychození školy k získání učňovských míst. [37] Teprve o necelých sto let později, roku 1869, byl vydán říšský zákon rozšiřující výuku o další předměty jako jsou dějepis či zeměpis a zavádějící osmiletou povinnou školní docházku, jejíž nedodržení je sankcionováno.

Dne 28. 10. 1918 došlo k vyhlášení Československého státu a v listopadu toho roku bylo založeno ministerstvo školství. V následujících letech české školství prošlo reorganizací a bylo těžce zasaženo německou okupací. V roce 1948 byl schválen zákon o základní úpravě jednotného školství (školský zákon), který poprvé stanovuje povinnou školní docházku na devět let (od 6 do 15 roku dítěte) a rozděluje základní školu na dva stupně, první a druhý, přičemž první stupeň má pět ročníků a druhý čtyři. [38]

S nástupem komunistické strany došlo ve školství ke změnám a v průběhu let se měnila délka povinné školní docházky nejprve na 8 let [39], v roce 1960 na 9 let [40] a následně na 10 let. [41] Po pádu komunistického režimu došlo k obnově českého školství a v roce 1990 byla novelizací zákona z roku 1984 opět zavedena devítiletá povinná školní docházka.

V průběhu celých 70. let došlo k zahájení výuky informačních oborů na technických vysokých školách. V 80. letech pak k zavedení do škol osmibitových mikropočítačů, na kterých probíhá výuka programování – na základních školách formou kroužků. V roce 1990 byl na gymnáziích k zaveden předmět Informatika a výpočetní technika z něhož bylo umožněno složit maturitní zkoušku. Na základních školách došlo v průběhu 90. let k vyučování informatiky v rámci třech různých vyučovacích předmětu během nichž bylo vyučováno ovládání počítače, práce s počítačem a algoritmizace.

## 2.2 Rámcový vzdělávací plán

V roce 2004 byl schválen zákon o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), který vstoupil v platnost 1.1.2005 a rušil předchozí zákon z roku 1984 a jeho novely. Tímto zákonem byly zavedeny Rámcové vzdělávací programy (dále RVP) tvořící podklad Školních vzdělávacích programů (dále ŠVP), které vychází z Národního programu rozvoje vzdělávání v České republice – Bílé knihy z roku 2001.

RVP určují závazný rámec pro školy při jejich tvorbě ŠVP. Skrze RVP tedy dochází k vynucování změn ve školství na celostátní úrovni. RVP rozlišuje mezi třemi etapami vzdělávání a to předškolním, základním a středním vzděláním. Rámcový vzdělávací plán pro základní školu (dále RVP ZV) je rozdělen na jednotlivé vzdělávací oblasti, přičemž jednou z nich je Informační a komunikační technologie, od roku 2021 Informatika, které se budou následující podkapitoly věnovat.

### 2.2.1 RVP ZV 2005 a 2017

Vzdělávací oblast Informační a komunikační technologie dle RVP ZV z roku 2005 se zaměřuje na rozvoj následujících kompetencí žáka:

- využívání moderních informačních a komunikačních technologií
- porozumění informacím po celou dobu jejich životnosti včetně médiích na kterých se informace vyskytuje
- podpora algoritmického myšlení a logických formulací
- práce s informacemi a jejich zdroji
- duševní vlastnictví v oblasti informatiky

Výuku stanovuje jak pro první tak pro druhý stupeň. Oba stupně mají stanovenou minimální časovou dotaci 1 hodiny týdně. Minimální časová dotace stanovuje kolik hodin v rámci daného stupně musí týdně škola minimálně oblasti věnovat. 1 hodina týdně tedy představuje jeden ročník s 1 hodinou věnovanou předmětu zabývající se oblastí Informační a komunikační technologie.

Očekávané výstupy prvního stupně jsou:

- základy práce s počítačem
  - využívání standardních funkcí
  - bezpečnost práce
  - ochrana dat
  - seznámení s formáty souborů
  - multimediální využití
- vyhledávání informací
  - vhodné způsoby vyhledávání – jakým způsobem zadávat hesla do vyhledávačů
  - komunikace skrze informační technologie
- zpracovávaní informací
  - práce s textem a obrázkem

V rámci druhého stupně pak jsou očekávané výstupy následující:

- práce s informací a její ověřování
- zpracovávání a využití informací
  - práce s textovými, grafickými a tabulkovými editory
  - typografie
  - duševní vlastnictví

[42]

Oproti RVP ZV z roku 2005 nedochází v oblasti Informační a komunikační technologie k výrazným změnám. Tento program je v současné době pro školy dobíhající. [43]

### 2.2.2 RVP ZV 2021

Školy mohou začít vyučovat podle ŠVP vypracovaných na základě RVP ZV z roku 2021 od 1. září 2021. Nejpozději musí s touto výukou začít do 1. září 2023 u všech ročníků prvního stupně. Výuku všech ročníků druhého stupně je nutné začít nejpozději 1. září 2024. V současné době tedy existují školy podle RVP ZV 2021 vyučující a školy u kterých tomu tak není.

Zásadní změnou je přejmenování oblasti z Informační a komunikační technologií na Informatiku a navýšení minimální časové dotace na 2 hodiny v rámci 1. stupně a 4 hodiny na 2. stupni.

Cílovým zaměřením oblasti Informatika je:

- systémový přístup k analýze situací a jevů světa
- nacházení a výběr vhodných řešení
- týmová práce
- kódování informací a organizace informací
- rozhodování na základě dat a jejich interpretace
- komunikace formou formálního jazyka srozumitelného strojům

RVP ZV 2021 klade požadavky na výuku v 2. období 1 stupně tedy v rámci 4 a 5 třídy. Očekávaným výstupem je:

- data, informace a modelování
  - rozhodování na základě dat
  - schopnost porozumět modelovým situacím (zjednodušeným, znázorněným pomocí schémat, tabulek, diagramů…) a vyčíst z modelu informace
- algoritmizace a programování
  - sestavení a testování symbolických zápisů algoritmů
  - popis problémů a návrh jeho řešení
  - blokově orientované programovací jazyky
- práce se strukturovanými daty
- digitální technologie
  - práce s aplikacemi
  - propojení digitálních zařízení a rizika s tímto spojená

- bezpečnostní pravidla pro práci s digitálními technologiemi
- bezpečnost přístupových údajů

V rámci druhého stupně jsou očekávány výstupy:

- data, informace a modelování
  - získávání dat, jejich interpretace a odhalování chyb
  - kódování dat
  - modelování situací pomocí grafů či schémat
- algoritmizace a programování
  - porozumění algoritmu
  - tvorba algoritmu v blokově orientovaném jazyce
- Informační systémy
  - porozumění informačním systémům
  - práce s daty v tabulkách
  - evidence dat
- digitální technologie
  - funkčnost hardwaru a softwaru
  - správa dat
  - připojování zařízení
  - závady a chybové stavy počítače
  - bezpečná práce s daty

[44]

Kapitola 3

# Analýza informačně bezpečnostních rizik pro žáky základních škol

Dnešní doba je charakterizována vysokou mírou digitalizace a informačních technologií. Elektronika a zejména internet se tak stávají běžnou součástí každodenního života a děti se s nimi setkávají stále mladší. Vzhledem k množství útoků, kterým je každý uživatel internetu nevyhnutelně vystaven, je třeba, aby si děti osvojily základní principy počítačové bezpečnosti.

Jednou z nejdůležitějších zásad je práce s přihlašovacími údaji, které je třeba vhodně tvořit a dále spravovat. Jelikož už několik let v řadě jsou mezi nejčastěji používanými hesly na internetu tyto hesla: „123456“, „password“, „123456789“, „heslo“, nebo „qwerty“, je obzvláště důležité už od dětství budovat povědomí o rizicích s hesly a jejich nevhodnými tvary. Problematice bezpečných přihlašovacích údajů se věnuje kapitola 1.1.

S tím, jak se vystavujeme technologiím přichází mnoho rizik, kterým je třeba předcházet. K tomu je potřeba, aby byly děti o rizicích informovány a poučeny o vhodných způsobech ochrany. Je nutné děti naučit jakým způsobem správně instalovat software a aktualizovat ho. Právě aktualizace pomáhají software uchránit před nalezenými bezpečnostními riziky, které by jinak mohl útočník zneužít. Je potřeba děti poučit o vhodných zdrojích softwaru a o nebezpečí malwaru, proti kterému se lze bránit antivirem. Rizikovým oblastem práce se software se věnuje kapitola 1.3.

Děti jsou zranitelným cílem často právě díky jejich nezkušenosti. Z toho důvodu je důležité dětem vysvětlit jednotlivé techniky sociálního inženýrství. Díky pochopení modelových situací a rizikových oblastí, tak mohou děti vhodně reagovat, odvrátit pokusy o zneužití jejich důvěry či jiné podvodné pokusy. Sociálnímu inženýrství a jeho rizikům se věnuje kapitola 1.2.

V této práci se věnuji těmto třem oblastem, tedy práci s přihlašovacími údaji, softwaru a sociálnímu inženýrství.

## 3.1 Dotazníkové šetření

V rámci této bakalářské práce bylo provedeno dotazníkové šetření, jehož cílem bylo zjistit současný stav obeznámenosti žáků základních škol s vymezenými tématy Informační bezpečnosti. Dotazníkové šetření bylo zaměřeno na studenty prvního a druhého stupně základních škol, kteří již v rámci své školní docházky absolvovali či právě absolvují hodiny vyučující informatiku.

### 3.1.1 Metodologie

Dotazníkové šetření probíhalo formou anonymního online dotazníku, zaslaným čtyřem základním školám v Praze a ve Středočeském kraji. V těchto školách pak proběhl sběr samotných dat. Dotazník byl vypracován v Google Forms, formulářích od společnosti Google. Sběr dat na školách proběhl v průběhu jednoho týdne od 27. 3. 2023 do 31. 3. 2023. Po tomto termínu bylo přijato dalších 12 odpovědí.

Pro dotazníkové šetření byla zvolena forma kvantitativního výzkumu. Na základě informací získaných během průzkumu a prostudování podobných dotazníkových šetření byl vytvořen dotazník. Podoba dotazníku a formulace otázek byla konzultována s Mgr. Tomášem Houdkem, Ph.D. a Mgr. et Mgr. Jakubem Šenovským, Ph.D. Dotazník byl také zkušebně vyplněn 10 žáky, kteří byli instruováni, aby případně zaznamenali jakékoliv nejasnosti, které u kterékoliv otázky mají. Tyto poznámky byli zapracovýny do současné podoby dotazníku. Pro tyto účely byla u každé z uzavřených otázek povolena možnost „jiné“, která k tomuto účelu sloužila. Došlo k vyplnění zkušebního dotazníku alespoň jedním žákem 3. až 9. třídy. Žáci byli instruováni, že jejich odpovědi jsou anonymní a slouží pouze jako zpětná vazba pro tvorbu dotazníku, jejich odpovědi tak nejsou zahrnuty ve vyhodnocení dotazníkového šetření.

Dotazník obsahuje celkem 21 otázek, přičemž poslední otázka byla dobrovolná a umožňovala tedy žákovi zanechat vzkaz. Zbylých 20 otázek bylo pro odeslání dotazníku povinných. Otázky byly uzavřené a v závislosti na otázce bylo možné zvolit jednu či více odpovědí. Celý dotazník v jeho pdf podobě se nachází v příloze A.

### 3.1.2 Limitace

Dotazník byl vypracován tak, aby ho žáci mohli vypracovat samostatně. Jelikož dochází k autoevaluaci mohou být výsledky zkresleny žákovým pochopením otázky či jinými vlivy.

Vzhledem k rozdílům mezi RVP ZV 2017 a RVP ZV 2021 může navíc docházet k rozdílům mezi žáky škol, které již vyučují podle nových RVP ZV 2021.

Výsledné hodnoty mohou být ovlivněny i pandemií covidu 19, která v rámci distanční výuky vedla k větší práci s digitálními technologiemi a to nad rámec jejich běžného zapojení do výuky. Žáci tak mohou být s zacházením s těmito nástroji lépe seznámeni, než by tomu tak bylo u stejné věkové skupiny před pandemií.

### 3.1.3 Respondenti

Dotazníkové šetření vyplnilo celkem 470 žáků základních škol. Školy byly požádány, aby dotazník nechaly vyplnit studenty ročníků u kterých už výuka informatiky proběhla, nebo právě probíhá.

**Tabulka 3.1** Rozložení respondentů napříč ročníky, vytvořeno na základě dotazníkových odpovědí

| Ročník | Počet respondentů | Procentuální zastoupení |
|---|---|---|
| 3 | 3 | 0,64 % |
| 4 | 73 | 15,53 % |
| 5 | 114 | 24,26 % |
| 6 | 74 | 15,74 % |
| 7 | 106 | 22,55 % |
| 8 | 60 | 12,77 % |
| 9 | 40 | 8,51 % |
| **celkem**: | **470** | **100 %** |

Jelikož vyplňování dotazníku probíhalo ve třídách a odpovědi žáků třetího ročníku byly mezi odpovědmi získanými v daném časovém úseku od žáků čtvrtých a pátých ročníků, lze předpokládat, že 3 žáci, kteří uvedli, že navštěvují třetí ročník, ve skutečnosti navštěvují ročník jiný.

### 3.1.4 Analýza a interpretace dat

V následující kapitole jsou výsledky v tabulkách udávány v procentech. Jednotlivé sloupce znázorňují ročníky základních škol. V rámci sloupce za daný ročník je za 100 % považováno celkový počet respondentů, kteří uvedli, že daný ročník navštěvují. V rámci sloupce „celkem“ je za 100 % považováno všech 470 respondentů.

**Otázka č. 1** – V jakém ročníku studuješ?
Výsledky této otázky jsou zpracovány v tabulce 3.1.

**Otázka č. 2** – Které heslo je podle Tebe nejbezpečnější?
Tato otázka má za účel ověřit základní pochopení bezpečných hesel. Žák by měl být schopen vyloučit zřetelně nevhodná hesla. V dotazníku byly nabídnuty následující možnosti:

- **123456** – jedná se o jedno z nejčastěji používaných hesel a z tohoto důvodu není bezpečné.
- **heslo** – jde o jedno z nejpoužívanějších hesel v Česku a proto není bezpečné.
- **passw0rd** – variace hesla „password“. Současné útoky umí cílit i na variace tohoto hesla a to obzvláště dojde-li ke změně z „o“ na „0“ či jiné často zaměňované znaky, jako v tomto případě.
- **Sk8kPes,P5esOves** – přepis věty „Skákal pes, přes oves“ do podoby hesla. Jedná se o metodu tvorby hesla z vět či slovních spojení, která slouží k usnadnění si zapamatování hesla, které tímto způsobem nabírá na délce. V tomto případě došlo k nahrazení písmen s čárkami a háčky za jejich číselnou variantu na klávesnici. Každé slovo také začíná velkým písmenem. Výsledné heslo je dlouhé, zapamatovatelné a obsahuje malé i velké písmena, speciální znaky a číslice.
- **Kralicek12** – délkou vhodné heslo, ale obsahuje potenciálně osobní informace, nemělo by docházet k použití domácích mazlíčků v heslech. Heslo má na začátku velké písmeno a na konci číslice, což činí využití těchto prvků v hesle nedostatečnými, neboť útoky s tímto rozložením počítají.
- **BatManJede!** – dostatečně dlouhé heslo obsahující velká a malá písmena a speciální znak.

**Tabulka 3.2** Které heslo je podle Tebe nejbezpečnější? Vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| 123456 | 33,33 % | 6,85 % | 2,63 % | 2,7 % | 1,89 % | 1,67 % | 7,5 % | 3,62 % |
| heslo | 0 % | 8,22 % | 8,77 % | 1,35 % | 0 % | 0 % | 5 % | 4,04 % |
| passw0rd | 0 % | 9,59 % | 2,63 % | 1,35 % | 0,94 % | 3,33 % | 0 % | 2,98 % |
| Sk8kPes,P5esOves | 0 % | 65,75 % | 74,56 % | 91,89 % | 88,68 % | 90 % | 75 % | 80,64 % |
| BatManJede! | 66,67 % | 1,37 % | 5,26 % | 1,35 % | 5,66 % | 5 % | 10 % | 4,89 % |
| Kralicek12 | 0 % | 8,22 % | 6,14 % | 1,35 % | 2,83 % | 0 % | 2,5 % | 3,83 % |

Z výsledku dotazníku se lze domnívat, že většina žáků umí rozpoznat základní prvky bezpečného hesla, jimiž jsou délka a variabilita znaků v hesle. Také lze předpokládat, že určité procent žáků zvolilo své odpovědi záměrně chybně, například je možné si povšimnout, že v 7. a 8. ročníku nikdo z respondentů za nejbezpečnější heslo nezvolil odpověď „heslo“, kdežto v 9. ročníku tuto odpověď zvolilo 5 %.

**Otázka č. 3** – Co děláš pro zapamatování hesla? (Více možných odpovědí)

Záměrem této otázky je zmapovat postoje žáků ke správě hesel. V dotazníku byly nabídnuté následující možnosti:

- **Uložím si ho do prohlížeče** – nevýhodou ukládání hesel v prohlížeči je nutnost důvěřovat způsobu, jakým je prohlížeč ukládá. V případě, že dojde ke kompromitaci zařízení či účtu k prohlížeči, může dojít i ke zneužití takto uložených přihlašovacích údajů.
- **Zapíšu si ho do sešitu ve kterém mám další hesla** – je důležité, aby uživatel nenechával takovýto sešit bez dohledu, neboť v případě, že by se ho zmocnil útočník, získá tak všechny zapsané přihlašovací údaje.
- **Napíšu si ho na lístek, který mám hned na očích** – nebezpečí spočívá v možném odpozorování takto zapsaných hesel, případném úniku například v rámci fotografie svého pracovního prostředí.
- **Použiji PasswordManager** – správce hesel je důležité používat s vhodně zvoleným heslem, který slouží k přístupu k přihlašovacím údajům v něm uloženým. Je nutné, aby uživatel uvážlivě vybíral vhodného správce hesel a udržoval si přehled o nebezpečích s ním spojených – například únicích, po nichž by měl okamžitě změnit své přihlašovací údaje uložené ve správci hesel.
- **Použiji hardwarový klíč** – výhodou je anulování rizika, že útočník autentizační prostředek zkopíruje. Uživatel se vystavuje riziku v okamžiku, kdy hardwarový klíč je odcizen.
- **Mám jedno heslo pro všechno a to si pamatuji** – pokud má žák více než jeden účet pro který takto využívá stejného hesla, vystavuje se riziku, že dojde-li ke kompromitaci přihlašovacích údajů k jednomu účtu, ztrácí tak kontrolu i nad účty se stejnými přihlašovacími údaji.
- **Uložím si heslo do textového souboru** – nezabezpečené textové soubory jsou nebezpečné pokud se útočník zmocní zařízení, kde se takovýto soubor nachází. V takovém případě se útočník dostává k důvěrným informacím, které může zneužít.
- **Svoje hesla si pamatuji** – v ideálním případě by si uživatel všechny svá hesla měl pamatovat. Spolu s požadavkem na jejich složitost a unikátnost je to však u většího počtu hesel problematické.
- **Hesla mi spravuje rodina** – tato odpověď se snaží zohlednit žáky, kterým spravuje jejich rodina hesla a tudíž sami nevolí, případně ani neví, jakou formou jsou hesla spravována.

**Tabulka 3.3** Co děláš pro zapamatování hesla? Vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Uložím do prohlížeče | 33,33 % | 10,96 % | 10,53 % | 6,76 % | 16,98 % | 13,33 % | 27,5 % | 13,4 % |
| Zapíšu do sešitu | 33,33 % | 21,92 % | 30,7 % | 35,14 % | 41,51 % | 30 % | 30 % | 32,34 % |
| Napíšu na lístek | 0 % | 15,07 % | 25,44 % | 12,16 % | 12,26 % | 15 % | 20 % | 16,81 % |
| Použiji správce hesel | 0 % | 15,07 % | 15,79 % | 14,86 % | 24,53 % | 21,67 % | 17,5 % | 18,3 % |
| Použiji hardwarový klíč | 0 % | 2,74 % | 3,51 % | 5,41 % | 7,55 % | 6,67 % | 2,5 % | 4,89 % |
| Mám jedno heslo | 33,33 % | 20,55 % | 25,44 % | 21,62 % | 18,87 % | 23,33 % | 25 % | 22,34 % |
| Uložím do souboru | 0 % | 15,07 % | 10,53 % | 12,16 % | 14,15 % | 15 % | 20 % | 13,62 % |
| Hesla si pamatuji | 0 % | 61,64 % | 62,28 % | 54,05 % | 65,09 % | 66,67 % | 7 % | 62,34 % |
| Hesla spravuje rodina | 66,67 % | 13,7 % | 9,65 % | 9,46 % | 11,32 % | 15 % | 2,5 % | 11,06 % |

Dle dat většina žáků spoléhá na paměť. Další nejpoužívanější metodou je zápis hesel do sešitu. Skoro čtvrtina dotazovaných však uvedla, že používají pouze jedno heslo, což je zásadní bezpečnostní riziko.

**Otázka č. 4** – Máš vlastní mobil?

Tato otázka slouží pro určení kontextu následujících otázek, jejichž vypovídající hodnota se může v závislosti na vlastnictví mobilního telefonu lišit.

**Tabulka 3.4** Máš vlastní mobil? Vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Ne | 33,33 % | 6,85 % | 2,63 % | 0 % | 0 % | 0 % | 0 % | 1,91 % |
| Ano | 33,33 % | 89,04 % | 83,33 % | 83,78 % | 92,45 % | 88,33 % | 97,5 % | 87,87 % |
| Sdílím ho se sourozenci | 33,33 % | 1,37 % | 0 % | 0 % | 0 % | 0 % | 0 % | 0,43 % |
| Mám víc mobilů | 0 % | 2,74 % | 14,04 % | 16,22 % | 7,55 % | 11,67 % | 2,5 % | 9,79 % |

Z dat vyplývá, že více než 95 % žáků má alespoň jeden vlastní mobilní telefon.

**Otázka č. 5** – Kdo všechno umí odemknout Tvůj mobil? (Více možných odpovědí)

Cílem otázky je prozkoumat jakým způsobem se žáci chovají k přihlašovacím údajům k vlastnímu mobilnímu zařízení. Tato otázka se zaměřuje na sdílení přihlašovacích údajů k zařízení. Měli na výběr z následujících možností:

- **Jen já**
- **Moji rodiče** – přihlašovací údaje k zařízení potomka umožňují rodičům lépe sledovat jeho aktivitu na daném zařízení a předcházet tak některým potenciálním rizikům.
- **Moji sourozenci** – dovoluje přístup k zařízení i sourozencům. V případě starších sourozenců může docházet k pomoci s prevencí rizik práce s daným zařízením.
- **Jiný rodinný příslušník**
- **Někteří moji kamarádi** – může dojít k případnému úniku či zneužití přihlašovacích údajů. Přihlašovací údaje by měli znát pouze oprávněné osoby (pro určité věkové kategorie dětí může být oprávněnou osobou i rodinný příslušník či jiný opatrovník) .
- **Nemám heslo** – odpověď pro žáky, kteří nevyužívají žádné formy hesla ke svému mobilnímu telefonu. V takovémto případě, kdokoliv kdo se zařízení zmocní, má k němu plný přístup.
- **Nemám mobil** – odpověď pro ty žáky, kteří nemají vlastní mobilní telefon.

Z dat zpracovaných pro tuto otázku byly vyjmuty odpovědi respondentů, kteří ve 4. otázce uvedli, že nemají vlastní mobilní telefon. Lze pozorovat, že určité procento respondentů zvolilo odpověď „Nemám mobil“ ačkoliv v předchozí otázce uvedli, že vlastní vlastní mobilní telefon či jich mají dokonce více.

**Tabulka 3.5** Kdo všechno umí odemknout Tvůj mobil? Vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Jen já | 33,33 % | 75,34 % | 62,28 % | 70,27 % | 71,7 % | 68,33 % | 77,5 % | 69,57 % |
| Moji rodiče | 0 % | 65,75 % | 69,3 % | 40,54 % | 39,62 % | 23,33 % | 15 % | 46,6 % |
| Moji sourozenci | 0 % | 23,29 % | 28,07 % | 10,81 % | 21,7 % | 11,67 % | 5 % | 18,94 % |
| Jiný rodinný příslušník | 33,33 % | 4,11 % | 5,26 % | 0 % | 2,83 % | 0 % | 5 % | 3,19 % |
| Někteří moji kamarádi | 0 % | 10,96 % | 14,91 % | 18,92 % | 26,42 % | 25 % | 30 % | 20 % |
| Nemám heslo | 0 % | 4,11 % | 2,63 % | 1,35 % | 4,72 % | 1,67 % | 2,5 % | 2,98 % |
| Nemám mobil | 66,67 % | 0 % | 0 % | 0 % | 0,94 % | 0 % | 2,5 % | 0,85 % |

Z tabulky je zřetelný klesající trend sdílení přihlašovacích údajů s rodinnými příslušníky, přičemž nejvíce sdílí s rodinou hesla žáci 4. a 5. ročníku. Naopak s přibývajícím věkem lze pozorovat, že roste sdílení přihlašovacích údajů s přáteli, kdy u 9. třídy je to 30 %.

Část žáků si při zodpovídání této otázky přála vyjádřit možnost, že přístup k jejich mobilnímu telefonu mají oni a někdo jiný (rodiče, sourozenci…). Pro znázornění této odpovědi tedy zvolili odpověď „Jen já“ a zároveň další možnosti. Tabulku 3.5 lze zpracovat podle tří typů odpovědí:

1. žáci, kteří zvolili možnost „Jen já“ spolu s další možností – tabulka 3.6
2. žáci, kteří zvolili pouze možnost „Jen já“ – tabulka 3.7
3. žáci, kteří nezvolili možnost „Jen já“ – tabulka 3.8

**Tabulka 3.6** Rozložení žáků kteří zvolili odpověď „Jen já“ spolu s další odpovědí, vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Jen já | 66,67 % | 72,6 % | 43,86 % | 21,62 % | 40,57 % | 11,67 % | 22,5 % | 38,3 % |
| Moji rodiče | 0 % | 68,49 % | 69,3 % | 40,54 % | 39,62 % | 23,33 % | 15 % | 47,02 % |
| Moji sourozenci | 0 % | 23,29 % | 28,07 % | 10,81 % | 21,7 % | 11,67 % | 5 % | 18,94 % |
| Jiný rodinný příslušník | 33,33 % | 4,11 % | 5,26 % | 0 % | 2,83 % | 0 % | 5 % | 3,19 % |
| Někteří moji kamarádi | 0 % | 10,96 % | 14,91 % | 18,92 % | 26,42 % | 25 % | 30 % | 20 % |
| Nemám heslo | 0 % | 5,48 % | 3,51 % | 1,35 % | 4,72 % | 1,67 % | 2,5 % | 3,4 % |
| Nemám mobil | 66,67 % | 4,11 % | 1,75 % | 0 % | 0,94 % | 0 % | 2,5 % | 0 % |

**Tabulka 3.7** Rozložení žáků kteří zvolili pouze odpověď „Jen já“, vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Jen já | 0 % | 17,81 % | 20,18 % | 48,65 % | 38,68 % | 56,67 % | 55 % | 35,96 % |

**Tabulka 3.8** Rozložení žáků kteří zvolili nezvolili odpověď „Jen já“, vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Jen já | 0 % | 0 % | 0 % | 0 % | 0 % | 0 % | 0 % | 0 % |
| Moji rodiče | 0 % | 12,33 % | 31,58 % | 22,97 % | 18,87 % | 13,33 % | 5 % | 19,57 % |
| Moji sourozenci | 0 % | 1,37 % | 14,91 % | 5,41 % | 9,43 % | 8,33 % | 2,5 % | 8,09 % |
| Jiný rodinný příslušník | 0 % | 1,37 % | 3,51 % | 0 % | 0,94 % | 0 % | 2,5 % | 1,49 % |
| Někteří moji kamarádi | 0 % | 1,37 % | 9,65 % | 13,51 % | 10,38 % | 21,67 % | 15 % | 11,06 % |
| Nemám heslo | 0 % | 2,74 % | 0,88 % | 1,35 % | 3,77 % | 1,67 % | 0 % | 1,91 % |
| Nemám mobil | 33,33 % | 0 % | 0 % | 0 % | 0 % | 0 % | 0 % | 0 % |

**Otázka č. 6** – Jaký máš zámek na mobilní telefon?

Tato otázka navazuje na předchozí otázku a zkoumá volbu zámku na mobilní telefon. Bylo možné zvolit následující odpovědi:

- **Heslo** – mělo by být zvolené vhodné heslo, tedy takové heslo, které není snadno uhodnutelné a odpozorovatelné. Uživatel by měl volit heslo dle pravidel pro bezpečné přihlašovací údaje.
- **Gesto** – jedná se o nejsnadněji odpozorovatelné heslo. Gesta mají omezený počet příjemně zadavatelných kombinací a často je lze odkoukat z mastnoty obrazovky.
- **PIN kód** – pro bezpečné použití je doporučován PIN kód o alespoň 6 znacích. PIN kód by dále neměl být triviální – například „123456“ či „000000“.
- **Biometrické údaje** – jedná se o poměrně bezpečnou metodu přihlašování, která je zneužitelná především v bezvědomí uživatele. Je nutné ji však kombinovat s vhodně zvolenou sekundární metodou přihlašování.

- **Žádný** – v tomto případě nemá mobilní telefon zámek a tudíž kdokoliv může získat přístup do zařízení.

**Tabulka 3.9** Jaký máš zámek na mobilní telefon? Vytvořeno na základě dotazníkových odpovědí[1]

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Biometrické údaje a heslo | 0 % | 16,44 % | 11,4 % | 14,86 % | 16,04 % | 25 % | 20 % | 16,17 % |
| Biometrické údaje a PIN | 0 % | 6,85 % | 14,91 % | 27,03 % | 27,36 % | 30 % | 25 % | 21,06 % |
| Biometrické údaje a gesto | 0 % | 4,11 % | 7,02 % | 10,81 % | 6,6 % | 8,33 % | 12,5 % | 7,66 % |
| Gesto | 0 % | 16,44 % | 14,91 % | 12,16 % | 12,26 % | 6,67 % | 5 % | 12,13 % |
| Heslo | 33,33 % | 17,81 % | 16,67 % | 6,76 % | 11,32 % | 11,67 % | 22,5 % | 14,04 % |
| Nemám mobil | 0 % | 0 % | 0 % | 0 % | 0 % | 1,67 % | 0 % | 0,21 % |
| PIN kód | 33,33 % | 26,03 % | 26,32 % | 27,03 % | 21,7 % | 15 % | 15 % | 22,98 % |
| Žádné | 0 % | 5,48 % | 6,14 % | 1,35 % | 4,72 % | 1,67 % | 0 % | 3,83 % |

Z tabulky je viditelné, že nejčastější formou zámku je biometricky údaj v kombinaci buď s heslem, PIN kódem či gestem. Nejčastějším tradičním zámkem je pak PIN kód.

**Otázka č. 7** – Používáš jiné heslo pro každý účet?

Neopakování hesel napříč službami je standardní bezpečnostní praktika. Cílem této otázky bylo zmapovat její dodržovaní.

**Tabulka 3.10** Používáš jiné heslo pro každý účet? Vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Ne | 0 % | 23,29 % | 22,81 % | 16,22 % | 15,09 % | 16,67 % | 17,5 % | 18,72 % |
| Ano | 66,67 % | 46,58 % | 45,61 % | 55,41 % | 54,72 % | 45 % | 57,5 % | 50,43 % |
| Ano, ty důležité | 0 % | 15,07 % | 18,42 % | 17,57 % | 22,64 % | 3 % | 22,5 % | 20,43 % |
| Řeší to za mě rodina | 33,33 % | 15,07 % | 13,16 % | 10,81 % | 7,55 % | 8,33 % | 2,5 % | 10,43 % |

**Otázka č. 8** – Aktualizuješ pravidelně software?

Aktualizace software je důležitou obranou proti malware. Uživatel by proto měl aplikace a jiný software aktualizovat,

**Tabulka 3.11** Aktualizuješ pravidelně software? Vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Ne | 0 % | 23,29 % | 22,81 % | 16,22 % | 15,09 % | 16,67 % | 17,5 % | 18,72 % |
| Ano | 66,67 % | 46,58 % | 45,61 % | 55,41 % | 54,72 % | 45 % | 57,5 % | 50,43 % |
| Ano, ty důležité | 0 % | 15,07 % | 18,42 % | 17,57 % | 22,64 % | 3 % | 22,5 % | 20,42 % |
| Řeší to za mě rodina | 33,33 % | 15,07 % | 13,16 % | 10,81 % | 7,55 % | 8,33 % | 2,5 % | 10,43 % |

Polovina žáků odpověděla, že pravidelně aktualizují software, přičemž 20 % pouze ten, který považuje za důležitý.

**Otázka č. 9** – Setkal ses někdy s útokem na svůj účet?

Cílem této otázky je prozkoumat, zda se žáci setkali s útokem na svůj účet, případně, zda ví jak útok odhalit.

20 % žáků uvádí, že se setkali s útokem na svůj účet, přičemž méně než 8 % žáků byl účet ukraden. Jelikož je možné, že určité procento útoků zůstalo nepovšimnuté, je tedy nutné těchto 20 % interpretovat jako spodní hranici. Přes 10 % žáků pak neví, zda k útoku došlo a přes 7 % si není vědomo, jak útok na účet poznat. Útok na účet lze nejčastěji odhalit ztrátou kontroly nad

[1] Z dat byli vyjmuty odpovědi respondentů, kteří v 4. otázce uvedli, že nemají vlastní mobilní telefon.

**Tabulka 3.12** Setkal ses někdy s útokem na svůj účet? Vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Ne | 0 % | 71,23 % | 54,39 % | 63,51 % | 65,09 % | 55 % | 52,5 % | 60,43 % |
| Ano, ale nebyl ukraden | 33,33 % | 6,85 % | 9,65 % | 13,51 % | 14,15 % | 20 % | 17,5 % | 12,98 % |
| Ano, byl ukraden | 33,33 % | 2,74 % | 5,26 % | 5,41 % | 8,49 % | 10 % | 20 % | 7,66 % |
| Nevím | 0 % | 10,96 % | 16,67 % | 9,46 % | 8,49 % | 13,33 % | 10 % | 11,7 % |
| Nevím, jak to poznat | 33,33 % | 8,22 % | 14,04 % | 8,11 % | 3,77 % | 1,67 % | 0 % | 7,23 % |

účtem nebo pomocí notifikací o pokusech o přihlášení. Tyto notifikace jsou často vyslány, pokouší-li se někdo přihlásit k účtu například z cizí země. Ochranou před napadením účtu a metodou na odhalení napadení je nastavení dvoufázového ověření.

**Otázka č. 10** – Používáš na všech zařízeních antivirový programy?

Používání antivirových programů je důležitou součástí bezpečného používání zařízení. Antivirové programy, lépe známé jako antiviry, jsou schopny detekovat a odstranit malware ze zařízení. Mít nainstalovaný antivirový program však nestačí, aby správně fungoval, musí mu uživatel umožnit aktualizaci, vždy když si to program vyžádá. Jelikož dochází k neustálému vývoji ze strany útočníků, právě aktualizace umožňuje programu reagovat na stále nové hrozby.

**Tabulka 3.13** Používáš na všech zařízeních antivirový programy? Vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Ne | 0 % | 26,03 % | 21,93 % | 18,92 % | 18,87 % | 16,67 % | 27,5 % | 21,06 % |
| Ano, mám antivirové programy | 33,33 % | 23,29 % | 21,93 % | 36,49 % | 32,08 % | 43,33 % | 40 % | 31,06 % |
| Myslím si, že ano | 33,33 % | 24,66 % | 35,09 % | 32,43 % | 39,62 % | 25 % | 27,5 % | 32,13 % |
| Řeší to rodina | 33,33 % | 26,03 % | 21,05 % | 12,16 % | 9,43 % | 15 % | 5 % | 15,74 % |

Pouze 31 % dotázaných má na všech zařízeních nainstalovaný antivirus. Dalších 32 % se domnívá, že tomu tak je. Zařízení v současné době často již obsahují nějaký základní antivirový program, který jestliže je náležitě udržován a povolen v zařízení, je často dostačující. Příkladem předinstalovaných antivirových programů je Windows Defender od společnosti Microsoft, který se nachází na každém zařízení s operačním systémem Windows 8 a vyšším.

**Otázka č. 11** – Kontroluješ oprávnění aplikací?

Aby aplikace mohla správně fungovat, potřebuje oprávnění k přístupu k určitým funkcím. Tyto oprávnění musí uživatel pro správné fungování udělit. Uživatel však musí být při udělování oprávnění na pozoru, neboť některé podvodné aplikace mohou tyto přístupové oprávnění zneužit. Podvodné aplikace se často vydávají za neškodné aplikace, například kalkulačku, ale požadují oprávnění k přístupu nad rámec potřeb obyčejné kalkulačky – například poloha či kontakty.

Vždy, když aplikace žádá o přístup, měl by se uživatel zamyslet, zda chce, aby společnost za danou aplikací měla k dané funkci přístup.

**Tabulka 3.14** Kontroluješ oprávnění aplikací? Vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Ne | 33,33 % | 17,81 % | 15,79 % | 17,57 % | 14,15 % | 18,33 % | 27,5 % | 17,45 % |
| Ano, jednou za čas | 33,33 % | 30,14 % | 28,07 % | 31,08 % | 26,42 % | 23,33 % | 35 % | 28,51 % |
| Ano, při stažení | 33,33 % | 32,88 % | 42,11 % | 45,95 % | 58,49 % | 58,33 % | 37,5 % | 46,6 % |
| Řeší to za mě rodina | 0 % | 19,18 % | 14,04 % | 5,41 % | 0,94 % | 0 % | 0 % | 7,45 % |

V tabulce si lze všimnout rostoucího trendu u odpovědi „Ne“, které je doprovázené klesající mírou rodinného zapojení.

**Otázka č. 12** – Jak si vybíráš, kterou aplikaci si nainstaluješ? (Více možných odpovědí)

Záměrem této otázky je zmapovat vlivy, které vedou k nainstalovaní aplikace. Následování zavádějících doporučení a klamavých reklam na aplikace, může vést ke zvýšení bezpečnostních rizik, protože mohou sloužit k nalákání uživatele k instalaci podvodné či jinak rizikové aplikace. Uživatel by si měl tyto skutečnosti uvědomovat a věnovat pozornost zdroji doporučení. Proto by si měl před instalací aplikace provést alespoň minimální rešerši, například četbou recenzí.

Z dat vyplývá, že přes 32 % respondentů vybírá aplikaci dle reklamy.

**Tabulka 3.15** Jak si vybíráš, kterou aplikaci si nainstaluješ? Vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Doporučení | 33,33 % | 65,75 % | 70,18 % | 58,11 % | 63,21 % | 68,33 % | 65 % | 65,11 % |
| Reklama v jiné hře | 0 % | 17,81 % | 18,42 % | 27,03 % | 24,53 % | 18,33 % | 35 % | 22,34 % |
| Reklama jinde | 0 % | 10,96 % | 13,16 % | 16,22 % | 17,92 % | 26,67 % | 37,5 % | 18,09 % |
| Náhodné nalezení | 33,33 % | 43,84 % | 43,86 % | 47,3 % | 41,51 % | 41,67 % | 57,5 % | 44,68 % |
| Recenze | 66,67 % | 27,4 % | 34,21 % | 32,43 % | 44,34 % | 45 % | 27,5 % | 36,17 % |
| Přijde mi zprávou | 33,33 % | 1,37 % | 3,51 % | 6,76 % | 1,89 % | 1,67 % | 5 % | 3,4 % |

**Otázka č. 13** – Ptáš se před stažením aplikace rodinného příslušníka?

Tato otázka má za cíl zmapovat, kdy dochází k omezování konzultování stahování aplikací a žáci začínají tyto záležitosti řešit samostatně. Hlavně v nižších ročnících bývá žádoucí, aby existovala kontrola nad stahováním aplikací žákem. Důvodem k tomuto opatření je především nezkušenost žáka a s tím související potřeba dohledu nad postupně se rozvíjejícími schopnosti žáka v oblasti informační bezpečnosti.

**Tabulka 3.16** Ptáš se před stažením aplikace rodinného příslušníka? Vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Ne | 33,33 % | 15,07 % | 28,95 % | 45,95 % | 63,21 % | 78,33 % | 82,5 % | 48,09 % |
| Ano | 66,67 % | 49,32 % | 35,09 % | 18,92 % | 12,26 % | 5 % | 10 % | 23,83 % |
| Ano, ale někoho jiného | 0 % | 1,37 % | 2,63 % | 0 % | 1,89 % | 0 % | 2,5 % | 1,49 % |
| Občas | 0 % | 34,25 % | 33,33 % | 35,14 % | 22,64 % | 16,67 % | 5 % | 26,6 % |

Z tabulky lze vysledovat, že konzultování s rodinnými příslušníky výrazně klesá mezi 5 a 6 ročníkem studia žáka, ale udržuje se alespoň formou občasných konzultací. V 9. třídě už přes 80 % žáků stahuje aplikace samostatně a bez dozoru.

**Otázka č. 14** – Kontroluje rodina jakým způsobem využíváš výpočetní techniku? (Více možných odpovědí)

Navazující otázka na otázku č.13 si klade za cíl zmapovat, jakým způsobem dochází ke kontrole nad žákovým přístupem k výpočetním technologiím.

**Tabulka 3.17** Kontroluje rodina jakým způsobem využíváš výpočetní techniku? Vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Hlídají obsah | 66,67 % | 28,77 % | 35,09 % | 17,57 % | 15,09 % | 11,67 % | 0 % | 21,06 % |
| Hlídají čas | 33,33 % | 52,05 % | 41,23 % | 35,14 % | 33,02 % | 21,67 % | 5 % | 34,47 % |
| Občas se zeptají | 66,67 % | 36,99 % | 31,58 % | 37,84 % | 45,28 % | 43,33 % | 37,5 % | 38,72 % |
| Nekontrolují vůbec | 33,33 % | 10,96 % | 18,42 % | 22,97 % | 31,13 % | 33,33 % | 55 % | 25,96 % |
| Občas upozorní na nebezpečí | 66,67 % | 28,77 % | 24,56 % | 35,14 % | 22,64 % | 33,33 % | 20 % | 27,45 % |

Z tabulky lze vysledovat klesající trend dohledu nad žákovým přístupem k výpočetním technologiím. Nejčastěji rodinní příslušníci volí metodu občasných dotazů. Druhou nejčastější metodou je kontrola času stráveného na zařízení. Nejméně častou metodou je hlídání obsahu, který žák na zařízení konzumuje. Jen 13 % žáků uvedlo, že jejich rodina hlídá obsah i čas strávený u výpočetní techniky (ve čtvrtém ročníku 19,18 %, v pátém 22,81 %, v šestém 10,81 %, v sedmém 10,38 % a osmém ročníku 6,67%). Přitom právě kontrola obsahu je žádoucí, obzvláště u nižších ročníků, a to především protože žák může být vystavován nežádoucím a nebezpečným vlivům (například nebezpečné výzvy na Tiktoku, které sledujícího navádějí k vzájemnému škrcení, polykání mleté skořice či jiným životu nebezpečným aktivitám). [45] Nebezpečí spojená s internetem a komunikací přes něj se věnuje řada průzkumů a dokumentů, například dokument V síti zabývající se zneužíváním dětí.

**Otázka č. 15** – V případě potřeby založení účtu využiješ možnost přihlášení pomocí jiného již existujícího účtu?

Jednotné přihlašování (SSO) je metoda, při níž se uživatel přihlašuje skrze jiný již existující účet. Díky tomu osoba ovládající účet, který poskytuje identitu, získá přístup ke všem navázaným uživatelským účtům; napadení takového účtu má proto závažnější důsledky.

**Tabulka 3.18** V případě potřeby založení účtu využiješ možnost přihlášení pomocí jiného již existujícího účtu? Vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Ano, většinou využiji | 0 % | 15,07 % | 23,68 % | 33,78 % | 49,06 % | 51,67 % | 57,5 % | 39,96 % |
| Ano, vždy využiji | 33,33 % | 9,59 % | 26,32 % | 31,08 % | 25,47 % | 30 % | 42,5 % | 26,17 % |
| Ne, vždy zakládám nový účet | 33,33 % | 15,07 % | 11,4 % | 16,22 % | 15,09 % | 15 % | 0 % | 13,19 % |
| Nikdy se sám/sama neregistruji | 33,33 % | 38,36 % | 21,93 % | 14,86 % | 6,6 % | 1,67 % | 0 % | 15,53 % |
| Účty mi spravuje rodina | 0 % | 21,92 % | 16,67 % | 4,05 % | 3,77 % | 1,67 % | 0 % | 9,15 % |

Je možné si v tabulce všimnout rostoucí tendence spojenou s využíváním SSO. Ta bude pravděpodobně spojená se zvyšujícím se množství účtů, které si žák zakládá a proto je nucen častěji vytvářet nové přihlašovací údaje – vzhledem k narůstající četnosti, pak žák zřejmě volí právě metodu jednotného přihlašování, díky které není nucen tyto nové přihlašovací údaje vytvářet.

**Otázka č. 16** – Jaké chatovací aplikace používáš pro osobní komunikaci? (Více možných odpovědí) Různé chatovací služby přistupují k soukromí zpráv odlišně, ať už jde o podporu koncového šifrování či celkovou politiku týkající se soukromých zpráv. Z tohoto důvodu je pro uživatele vhodné, aby si byl vědom co všechno obnáší smluvní podmínky služby. Webová stránka Terms of Service; Didn't Read[2] je projekt, zabývající se analýzou a známkováním smluvních podmínek služeb. Na této stránce tak lze nalézt základní informace o službách, které uživatel využívá.

V závislosti na službě skrze kterou jsou zprávy, fotografie či jiné dokumenty zaslány, získává služba práva na data. Některé služby také zpracovávají soukromé zprávy mezi uživateli, například pro reklamní účely. Uživatel by si měl tyto skutečnosti uvědomovat a dbát na ně během jakéhokoliv takovéhoto sdílení informací.

V této otázce bylo možné zvolit více odpovědí a i vlastní odpovědi přidat. Respondenty zapsané odpovědi jsou v tabulce zahrnuty pod nadpisem „Jiné". Zmíněná je i sociální síť bývalého amerického prezidenta Donalda Trumpa Truth Social.

Nejpoužívanější aplikací je WhatsApp od americké společnosti Meta, která vlastní i Facebook Messenger a Instagram. WhatsApp má automaticky zapnuté koncové šifrování (end-to-end šifrování) pro všechny konverzace a klíč je uložen v zařízení a s každou zprávou se mění. [46] Druhou

[2] Dostupné skrz `https://tosdr.org/`

nejpoužívanější metodou jsou SMS zprávy, které koncové šifrování neumožňují. Instagram obsadil třetí pozici. Ten stejně jako Facebook Messenger umožňuje zahájit šifrovanou konverzaci. [47] Facebook Messenger jí umožňuje pouze v rámci své mobilní aplikace. Na čtvrtém místě je sociální platforma pro krátká videa TikTok od čínské společnosti ByteDance. TikTok v současné době nepodporuje komunikaci s koncovým šifrování. [48] Mnohé další aplikace nabízí možnost zapnout koncové šifrování a to převážně pouze pro vybranou konverzaci, nikoliv tedy globálně pro všechny současné a budoucí konverzace. Například Snapchat pak používá koncové šifrování pro fotky skrze službu zasílané, pro soukromé či skupinové chaty ho však neumožňuje.

**Tabulka 3.19** Jaké chatovací aplikace používáš pro osobní komunikaci? Vytvořeno na základě dotazníkových odpovědí

| **Aplikace**: | | **celkem:** |
|---|---|---|
| | WhatsApp | 88,72 % |
| | SMS | 63,4 % |
| | Instagram | 45,74 % |
| | TikTok | 36,81 % |
| | Discord | 31,28 % |
| | Snapchat | 31,06 % |
| | Microsoft Teams | 24,26 % |
| | Facebook Messenger | 22,13 % |
| | Telegram | 17,02 % |
| | Viber | 16,38 % |
| | Apple iMessages | 9,79 % |
| | Skype | 9,79 % |
| | Google Messages | 7,23 % |
| | Signal | 3,83 % |
| | Vkontakte | 3,19 % |
| | WeChat | 2,34 % |
| | Google Hangouts | 1,91 % |
| | Wire | 1,06 % |
| | Line | 0,85 % |
| | Slack | 0,85 % |
| | Olvid | 0,63 % |
| | Kik | 0,63 % |
| **Jiné:** | E-mail | 1,28 % |
| | Telefon | 1,28 % |
| | Hry | 0,85 % |
| | Youtube | 0,64 % |
| | Omegle | 0,21 % |
| | InfoWars | 0,21 % |
| | Truth Social | 0,21 % |
| | Zalo | 0,21 % |

**Otázka č. 17** – Posíláš osobní fotografie pomocí chatovacích aplikací? (Více možných odpovědí)

Cílem této otázky je zjistit jakým způsobem žáci přistupují ke sdílení osobních fotografií. Jednalo se o otázku, kde bylo možné vybrat více odpovědí. Zasílání osobních fotografií může vést například ke kyberšikaně či zjištění osobních informací o jedinci. Z fotografií lze často vyčíst, na kterém místě se uživatel nachází, kde bydlí a další informace, které mohou být využity například za účelem krádeže.

Automatické mazaní zpráv často nezaručí, že fotografie po daném úseku opravdu přestane existovat. Často jí lze před vypršením časového limitu stáhnout či vytvořit její screenshot.

V tabulce lze vidět, že značná část žáků sdílí fotografie s rodinnými příslušníky. Přičemž přes 22 % žáků pouze s rodinnými příslušníky.

**Tabulka 3.20** Posíláš osobní fotografie pomocí chatovacích aplikací? Vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Rodině | 66,67 % | 58,9 % | 57,89 % | 44,59 % | 55,66 % | 41,67 % | 35 % | 51,49 % |
| Kamarádům | 33,33 % | 39,73 % | 28,95 % | 18,92 % | 39,62 % | 48,33 % | 57,5 % | 36,38 % |
| Důvěryhodným osobám | 0 % | 0 % | 0 % | 0 % | 0 % | 0 % | 0 % | 0 % |
| Pouze zašifrovanou komunikací | 0 % | 2,74 % | 4,39 % | 2,7 % | 4,72 % | 5 % | 5 % | 4,04 % |
| Ano, ale zprávy se automaticky mažou | 33,33 % | 1,37 % | 1,75 % | 2,7 % | 2,83 % | 5 % | 2,5 % | 2,77 % |
| Nikomu | 66,67 % | 19,18 % | 30,7 % | 35,14 % | 26,42 % | 23,33 % | 20 % | 27,02 % |

**Tabulka 3.21** Otázka č. 17 žáci, kteří posílají osobní fotografie pouze rodině[3], vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Pouze rodině | 0 % | 24,66 % | 33,33 % | 28,38 % | 21,7 % | 6,67 % | 5 % | 22,55 % |

**Otázka č. 18** – Sdílíš na sociálních sítích své osobní údaje? (Více možných odpovědí)

Cílem této otázky je zmapovat jakým způsobem přistupují žáci ke sdílení osobních informací prostřednictvím sociálních sítí. Skrze sociální sítě lze o uživateli získat mnoho informací a to obzvlášť nejsou-li vhodně nastavené oprávnění na zobrazení obsahu. Tímto způsobem jde často zjistit životní styl uživatele, jeho zvyky a návyky, včetně informací o tom kde bydlí, jaké místa často navštěvuje a s kým se přátelí. Tyto informace je pak útočník schopen využít a zneužít při svém útoku.

Příkladem demonstrující nebezpečí sdílení osobních informací na sociálních sítí je video vytvořené Febelfin, Belgickou bankou, kde jsou pomocí sociálního inženýrství schopni zjistit i číslo kreditní karty, video s názvem Amazing mind reader reveals his 'gift'[4] je dostupné na Youtube.

**Tabulka 3.22** Sdílíš na sociálních sítích své osobní údaje? Vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Osobní fotografie | 66,67 % | 12,33 % | 20,18 % | 27,03 % | 34,91 % | 36,67 % | 37,5 % | 27,23 % |
| Uvedené bydliště | 33,33 % | 4,11 % | 1,75 % | 1,35 % | 2,83 % | 5 % | 2,5 % | 2,98 % |
| Uvedená škola | 33,33 % | 2,74 % | 2,63 % | 1,35 % | 0,94 % | 3,33 % | 2,5 % | 2,34 % |
| Fotografie z pravidelně navštěvovaného místa | 33,33 % | 4,11 % | 1,75 % | 2,7 % | 7,55 % | 13,33 % | 5 % | 5,53 % |
| Uvedení současné polohy | 0 % | 5,48 % | 4,39 % | 9,46 % | 17,92 % | 18,33 % | 20 % | 11,49 % |
| Uvedený rodinní příslušníci | 33,33 % | 4,11 % | 3,51 % | 5,41 % | 6,6 % | 5 % | 2,5 % | 4,89 % |
| Myslím si, že neuvádím | 0 % | 6,85 % | 15,79 % | 17,57 % | 21,7 % | 26,67 % | 12,5 % | 17,02 % |
| Ne | 66,67 % | 75,34 % | 64,91 % | 58,11 % | 43,4 % | 36,67 % | 40 % | 54,89 % |

Z tabulky lze vyčíst rostoucí trend sdílení své osobní fotografie na sociálních sítích. Roste taktéž míra sdílení polohy, kde se žák v danou chvíli nachází. Více než polovina respondentů udává, že osobní informace na sociálních sítích nesdílí.

**Otázka č. 19** – Komu řekneš heslo na Wi-Fi u sebe doma? (Více možných odpovědí)

Tato otázka se zabývá přístupem k sdílení hesla od domácí Wi-Fi sítě. Pomocí hesla k Wi-Fi síti se zařízení dostává do domácí sítě a v závislosti na jejím nastavením je možné ovlivňovat

[3] V tabulce jsou zpracovány data uživatelů, kteří v otázce zvolili možnost „Ano, rodině" a nevybrali ani jednu z možností „Ano, kamarádům", „Ano, pouze důvěryhodným osobám" a „Ne, nikomu". Celkový počet těchto respondentů byl 106.

[4] Dostupné skrz `https://www.youtube.com/watch?v=F7pYHN9iC9I`

další připojená zařízení. Například dojde-li k připojení infikovaného zařízení do domácí sítě, může toto zařízení infikovat další připojená zařízení (například i Wi-Fi router). Dalším příkladem, kdy nemusí být žádoucí udělit přístupové údaje uživatelům mimo domácnost, je, jsou-li k síti připojené bezpečnostní kamery.

Útočník může přístup k domácí Wi-Fi síti využít k infikaci zařízení nežádoucím malware.

**Tabulka 3.23** Komu řekneš heslo na Wi-Fi u sebe doma? Vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Členům domácnosti | 0 % | 58,9 % | 63,16 % | 70,27 % | 75,47 % | 76,67 % | 70 % | 68,3 % |
| Kamarádům | 33,33 % | 32,88 % | 48,25 % | 51,35 % | 64,15 % | 73,33 % | 65 % | 54,47 % |
| Příbuzným | 33,33 % | 39,73 % | 42,11 % | 45,95 % | 55,66 % | 68,33 % | 47,5 % | 49,15 % |
| Přítel/Přítelkyně | 33,33 % | 4,11 % | 22,81 % | 20,27 % | 32,08 % | 45 % | 45 % | 26,38 % |
| Návštěvě | 0 % | 21,92 % | 30,7 % | 29,73 % | 33,96 % | 51,67 % | 30 % | 32,34 % |
| Komukoliv | 33,33 % | 0 % | 4,39 % | 9,46 % | 3,77 % | 13,33 % | 2 % | 7,02 % |
| Řeší to rodina | 0 % | 42,47 % | 29,82 % | 21,62 % | 13,21 % | 13,33 % | 5 % | 22,34 % |

Z tabulky je viditelné, že žáci nejčastěji heslo od Wi-Fi sdílí s členy domácnosti a kamarády. Pouze s členy domácnosti sdílí heslo pouze 10 % respondentů.

**Otázka č. 20** – Co rozhoduje, zda klikneš na odkaz, který ti někdo pošle? (Více možných odpovědí)

Sociální inženýrství často využívá ochoty uživatele kliknout na odkaz. Tyto odkazy často vedou na podvodné stránky či na stránky nakažené malwarem. Z toho důvodu je důležité, aby uživatel před kliknutím na odkaz byl obezřetný. Obecnou zásadou je neklikat na odkazy z neznámých zdrojů.

**Tabulka 3.24** Co rozhoduje, zda klikneš na odkaz, který ti někdo pošle? Vytvořeno na základě dotazníkových odpovědí

| Ročník | 3 | 4 | 5 | 6 | 7 | 8 | 9 | celkem: |
|---|---|---|---|---|---|---|---|---|
| Kdo ho poslal | 33,33 % | 73,97 % | 74,56 % | 62,16 % | 75,47 % | 83,33 % | 82,5 % | 74,26 % |
| Jak vypadá | 0 % | 41,1 % | 35,09 % | 40,54 % | 65,09 % | 5 % | 42,5 % | 45,96 % |
| Kam skutečně vede | 100 % | 36,99 % | 31,58 % | 32,43 % | 35,85 % | 50 % | 40 % | 37,02 % |
| Zda jsem ho očekával | 0 % | 17,81 % | 29,82 % | 28,38 % | 30,19 % | 46,67 % | 57,5 % | 32,13 % |
| Obsah zprávy s odkazem | 33,33 % | 10,96 % | 13,16 % | 18,92 % | 31,13 % | 30 % | 35 % | 21,91 % |
| Platforma | 0 % | 24,66 % | 18,42 % | 24,32 % | 34,91 % | 45 % | 35 % | 28,72 % |

19 % respondentů (převážně z nižších ročníků) uvedlo, že se rozhoduje pouze na základě toho, kdo odkaz odeslal. 9 % respondentů bere v úvahu odesílatele a vzhled odkazu. Vzhled odkazu, však často lze přepsat, takže může být zavádějící. Skoro 5 % respondentů vyhodnocuje všechny uvedené možnosti, než na odkaz klikne.

**Otázka č. 21** – Vzkazy

Poslední otázka dotazníku umožňovala zanechat vzkaz. Bylo zde zanecháno několik doplňujících informací k dotazníku.

- Dva žáci sdělili, že mají pouze tlačítkový telefon.
- Jeden žák zmínil, že jeho rodina využívá Family Link ke kontrole využívání výpočetní techniky. Family Link je služba umožňující rodičům vytvořit účet pro své dítě a takto spravovat jeho používání mobilního zařízení. Rodiče mohou nastavit omezení pro používání aplikací a webových stránek, stanovit čas, který může dítě na zařízení strávit a sledovat polohu.
- Jeden žák upozornil, že ne všichni znají heslo od své domácí Wi-Fi sítě.

- Jeden žák uvedl, že kliká na odkazy, když „*tam není takové písmo, které znám moc dobře*“.
- Jeden žák uvedl, „*na stránkách a aplikacích mám svoje telefonní číslo a používám svůj hlas*“.
- Jeden žák uvedl, že neinstaluje žádný program.
- Jeden žák sdělil, že nemá sociální sítě, pouze WhatsApp a Youtube.
- Jeden žák si přeje, aby se informovalo o nebezpečí spojené s klikáním na odkazy, které mohou zablokovat i zničit telefon.
- Jeden žák informuje, že Apple si umí zapamatovat heslo a pomocí iTouch nebo použitím PIN kódu zobrazí hesla k účtům.
- Jeden žák upřesňuje, že problematiku řeší s rodiči a bratrem.

## 3.2 Analýza prevence na ZŠ Písnická v Praze 12

Tato kapitola čerpá z [49] a materiálů na webu zveřejněných.

Základní škola se nachází v hlavním městě Praha a je otevřena od roku 1980. Zřizovatelem školy je Úřad městské části Praha 12. Jedná se o školu poskytující všeobecné základní vzdělání s prvním až devátým postupným ročníkem, která vzdělává zhruba 480 žáků. Ročníky jsou vyučovány ve dvou paralelních třídách s průměrně 25 žáky.

Ve škole stabilně pracuje kolem 55 pedagogických pracovníků a to včetně vychovatelů školní družiny a asistentů pedagoga. Ve škole působí dva výchovní poradci, pro první a pro druhý stupeň, metodik prevence sociálně patologických jevů a školní psycholog.

### 3.2.1 ŠVP

Na základní škole vznikl nový školní vzdělávací plán z RVP ZV 2021, který je platný od 1. 9. 2022. Podle nového programu byla ve školním roce 2022/2023 zahájena výuka ve všech třídách s výjimkou 8. a 9. ročníku v nichž doběhne výuka dle předchozích ŠVP.

Škola si v oblasti Informatiky klade za cíl rozvíjet následující digitální kompetence:

- ovládání běžně používaných digitálních zařízení, aplikací a služeb
- vyhledávání, získávání a kritické posuzování informací a digitálního obsahu
- tvorba vlastního digitálního obsahu
- používání digitálních zařízení s cílem usnadnění a zkvalitnění práce
- prevence bezpečnostních rizik

Škola podporuje používání digitálních zařízení i v rámci výuky napříč předměty. Žáci mohou na vyzvání pedagoga pracovat s digitálními zařízeními například za účelem vyhledávání informací.

Dle nového ŠVP je předmět Informatiky na škole vyučován jednou týdně od 4. ročníku do 9. ročníku. To je změna oproti předcházejícímu ŠVP, které stanovovalo výuku Informatiky na 5. a 6. ročník. Dle obou ŠVP je v 9. ročníku jednou týdně vyučován i předmět Mediální výchova.

Výuka předmětu Informatika je vedena ve specializované počítačové učebně vybavené počítači a tiskárnou.

**4. ročník** Ve čtvrtém ročníku jsou vyučovány základní dovednosti v oblasti práce s počítači, tak aby došlo k sjednocení znalostí napříč žactvem. Mezi tyto základní znalosti patří:

- práce s vstupními (myš, klávesnice…) a výstupními (monitor, sluchátka…) periferiemi
- propojení technologií
- práce s internetem
- elektronická pošta
- práce s daty – úložiště, sdílení, cloud, mazání dat, koš
- bezpečnostní pravidla pro práci – ergonomie, ochrana digitálního zařízení a zdraví uživatele

V rámci předmětu jsou vyučovány základy algoritmizace a šifrování.

**5. ročník** V současné chvíli dochází k výuce 5. ročníku podobně jako v ročníku 4. neboť v předchozím ŠVP byl předmět Informatiky vyučován na prvním stupni pouze v 5. ročníku.

**6. ročník** V šestém ročníku jsou dále prohlubovány znalosti žáků v oblasti algoritmizace především formou blokově orientovaných programovacích jazyků. Dále je prohlubovaná i znalost šifer a přenosu dat – žáci jsou vedeni k vyzkoušení šifrování a dešifrování vlastních zpráv.

V rámci předmětu se žáci mimo jiné věnují běžným uživatelským a základním administrativním činnostem, jako například:

- práce s daty v grafu a tabulce
- práce s bitmapovou a vektorovou grafikou
- instalace a aktualizace aplikací a programů
- fungování a služby internetu
- přístup k datům a metody jejich zabezpečení

**7. ročník** V sedmém ročníku je vyučována především algoritmizace. Žáci jsou vedeni k analýze problémů a tvorbě vlastního řešení. Jsou vyučovány základy práce s grafy a ohodnocenými grafy. Jsou představeny základní programovací praktiky jako je práce s proměnnými, funkcemi…

**8. ročník** V osmém ročníku není tento školní rok předmět Informatiky vyučován, neboť současní žáci 8. ročníku studují dle předcházejících ŠVP.

Dle nových ŠVP bude výuka navazovat a dále prohlubovat znalosti algoritmizace a programování. Výuka se zaměří i na audiovizuální tvorbu – tvorba zvuku, animace…Pokračuje výuka práce s daty a tabulkami. Žák je vzděláván v oblasti hardwaru a operačního systému.

**9. ročník** V devátém ročníku není tento školní rok předmět Informatiky vyučován. Devátý ročník je vyučován dle předchozích ŠVP. V rámci předmětu Pracovní činnosti jsou vyučovány dvě oblasti a to příprava pokrmů a informatika. Žáci jsou rozděleny na dvě skupiny, kdy mají jedno pololetí zaměřené na přípravu pokrmů a v druhém se věnují informatice.

V rámci tématu informatika pracují žáci s Microsoft Powerpoint, kde tvoří vlastní prezentace. Dále je vyučována grafika, úprava fotografií a práce s Microsoft Excel. Žáci jsou poučeni o tiskárnách a moderních technologiích (CD-ROM, DVD, USB, Dokumety Google…)

Dle nových ŠVP je výuka zaměřena na práci se soubory a fungování technologií (internet věcí, umělá inteligence, virtuální realita…). Žák by měl po absolvování předmětu umět pracovat v online prostředí, rozumět fungování sítí a základních pojmů s tím spojených.

V rámci předmětu Multimediální výchova je vyučována práce s informací a její ověřování. Jsou probírány klady a zápory mobilních zařízení, jejich funkcionalita a práce s nimi. V rámci předmětu tvoří žáci v týmech prezentace na téma Nebezpečí sociálních sítí a internetu.

### 3.2.2 Primární prevence rizikového chování

Primární prevence rizikového chování (dále pouze PPRCH) je snaha předcházet vzniku rizikového chování u osob u kterých se toto chování ještě nevyskytovalo.

Ve škole dochází k reakcím na aktuální problémy. Učitelé s žáky diskutují nově objevující se problematiku – například podvodné e-maily, hoaxy šířené ve spojení se zpoplatněním aplikace WhatsApp a další. Výuka a další aktivity školy jsou podpořeny projektem PPRCH. Na žádost vyučujících metodička prevence podle potřeby zařazuje bloky prevence věnující se aktuálně se vyskytujícím útokům.

## 3.3 Vyhodnocení a shrnutí kapitoly

Z výsledků dotazníků je zřetelné, že většina žáků si uvědomuje, jak by mělo bezpečné heslo vypadat. Naopak je poněkud zneklidňujících 22 % žáků, kteří odpověděli, že používají pouze jedno heslo. Velkému nebezpečí se vystavují i žáci, kteří si hesla zapisují na lístek, který mají hned na očích, neboť takový zvyk může v pozdějších letech v pracovním prostředí způsobit značné škody. Proto je potřeba žákům představit nebezpečí s hesly spojená a prezentovat jim všechny možné varianty správy hesel, přičemž některé z těchto řešení značně usnadňují používání různých hesel pro každý účet.

Metoda jednotného přihlašování je mezi respondenty oblíbená, využívá ji přes 66 % žáků. Existuje několik druhů SSO, přičemž by si měl být uživatel vědom výhod a rizik s nimi spojených. Například, navazuje-li účty pravidelně na Facebook SSO, bude pro uživatele výrazně obtížnější Facebookový účet zrušit.

V současné době přichází čím dál mladší děti do kontaktu s mobilními telefony a jak je zřetelné z výsledků dotazníku, téměř každý žák vlastní vlastní mobilní telefon. Jelikož jsou to právě chytré telefony, se kterými děti často přichází do kontaktu, dříve než s počítači, je potřeba adresovat rizika s nimi spojená.

Důležitou součástí ochrany mobilních zařízení je zámek obrazovky. Ten slouží k ochraně přístupu do zařízení před neautorizovanými osobami. Se stále větším zapojením mobilních telefonů ve dvoufázovém ověřování je důležité, aby tento přístup měli pouze oprávněné osoby. O to důraznější je tento požadavek, umožňuje-li uživatel platby pomocí mobilního telefonu či má nastavené mobilní bankovnictví, které je mnohdy vázané i na biometrické údaje uložené v mobilním telefonu. Z výsledků dotazníku je zřetelné, že žáci jsou ochotni tyto přístupové údaje sdílet i se svými přáteli a to především ve vyšších ročnících.

Aplikace instalované na mobilní zařízení často vyžadují pro svou funkčnost různá oprávnění, u kterých uživatel musí zvážit zda je povolí. Zamítnutí požadovaného oprávnění vede často k ztrátě určité funkcionality aplikace či k úplné nemožnosti aplikaci využít. Z toho důvodu je uživatel nucen vyhodnocovat, zda je ochoten oprávnění dané aplikaci udělit či nikoliv. Toto rozhodování vyžaduje určitou obezřetnost, protože mnohé podvodné aplikace díky uděleným oprávněním shromažďují o uživateli data, které dále předprodávají. Aby uživatel předcházel instalaci podvodných aplikací, měl by se o dané aplikaci edukovat, například skrze čtení uživatelských recenzí, které mohou upozorňovat na nebezpečí. Pozorný by měl být i ke zdroji doporučení, například reklamy mohou být cíleně zavádějící. Podle reklam se o instalaci aplikace rozhoduje přes 32 % respondentů. Z dotazníku také je viditelné, že více než 17 % žáků nekontroluje oprávnění nainstalovaných aplikací. Z výsledků taktéž vyplývá, že toto procento roste s vyššími ročníky, kdy u 9. ročníků je to přes 27 % žáků.

Ochrana soukromí je důležitou složkou informační bezpečnosti. Uživatelé by si měli být vědomi rizik plynoucí z konverzace prostřednictvím chatovacích aplikací a používaní sociálních sítí. Veškeré informace, které o sobě uživatel uvádí, mohou být útočníkem zneužity a využity pro vytvoření propracovanějšího podvodu. Díky sociálnímu inženýrství je možné vyhlídnutou oběť přesvědčit o kontaktu známé osoby a tímto způsobem jí nalákat k provedení rizikové operace, kterou může být například kliknutí na odkaz vedoucí na infikovanou stránku, nebo vylákání finančních prostředků…Uživatel by tedy neměl spoléhat pouze na odesílatele a měl by kontrolovat další faktory, než na odkaz klikne. Dle výsledků dotazníku se 19 % žáků rozhoduje o kliknutí na odkaz pouze dle odesílatele zprávy.

# Kapitola 4

# Vybrané materiály k výuce informační bezpečnosti

Osvěta je základním prvkem prevence, neboť právě dostatek informací umožňuje jedinci učinit informované rozhodnutí. Z tohoto důvodu je potřeba informovat o možných rizicích a metodách, kterými jim lze předcházet. V této kapitole jsou popsány zdroje a materiály k výuce informační bezpečnosti.

Následující materiály pokrývají vždy alespoň jedno z témat v kapitole 1 vymezených: **Přihlašovací údaje**, **Software** a **Sociální inženýrství**.

## 4.1 Osvěta NÚKIB

Tato podkapitola primárně čerpá z [50].

Vzdělávací portál NÚKIBu[1] a jeho kurzy zaměřené na školy pokrývají především sociální aspekty používání digitálních technologií, jako je závislost, nebezpečí spojená s komunikací online a kyberšikana. Jejich kurzy se však tématicky věnují všem vytyčeným kategoriím – přihlašovacím údajům, software a sociální inženýrství.

Osvěta nabízí kurzy zaměřené na kybernetickou a informační bezpečnost. Mnohé z těchto kurzů jsou přístupné pro veřejnost, pro jiné je potřeba individuální registrace či registrace dané organizace. Tyto kurzy lze filtrovat podle tagů – tedy pro koho jsou primárně určeny (veřejnost, školy, zdravotnictví a úřady). NÚKIB pro veřejnost nabízí řadu volně přístupných kurzů, které jsou otevřené bez nutnosti přihlášení a je tak možné je volně prohlížet. Pro dokončení kurzu, absolvování testu a získání certifikátu, je nutné provést registraci.

Pro školy je vypracováno několik kurzů, včetně kurzu pro pracovníky prevence a zaměstnance školy. Kurzy pro žáky jsou rozdělené podle doporučených ročníků. U každého kurzu pro školy jsou stanoveny vzdělávací cíle a jejich vymezení v rámci RVP ZV 2017 a 2021. Portál také nabízí rozcestník osvětových materiálů určený pro pedagogy, který slouží jako přehled dalších zdrojů materiálů a vzdělávacích aktivit.

[1] Dostupný skrze `https://osveta.nukib.cz/local/dashboard/`

**Tabulka 4.1** Osvěta NÚKIB – kurzy pro základní školy, zpracováno na základě [50]

| Kurz a doporučený ročník | Náplň | RVP ZV 2021 očekávané výstupy | Zpracování |
|---|---|---|---|
| **Vanda a Eda v Onl@jn světě**<br>1.-3. | Závislost na digitálních technologiích<br>Seznamování se online<br>Sdílení fotografií<br>Pravdivost informací na internetu | ČJS-3-5-03 chová se obezřetně při setkání s neznámými jedinci, odmítne komunikaci, která je mu nepříjemná; v případě potřeby požádá o pomoc pro sebe i pro jiné; ovládá způsoby komunikace s operátory tísňových linek<br>ČJS-3-5-01 uplatňuje základní hygienické, režimové a jiné zdravotně preventivní návyky s využitím elementárních znalostí o lidském těle; projevuje vhodným chováním a činnostmi vztah ke zdraví | - Interaktivní povídky<br>- Obrázkové karty s lektorskou příručkou<br>- Audiorádio [2] |
| **Digitální stopa: Příběh Svůďáka**<br>4.-5. | Sdílení informací online<br>Falešná identita<br>Kybergrooming<br>Kyberšikana<br>Přihlašovací údaje<br>Online platby<br>Autorská práva | ČJS-5-2-02 rozpozná ve svém okolí jednání a chování, která se už nemohou tolerovat<br>I-5-4-03 dodržuje bezpečnostní a jiná pravidla pro práci s digitálními technologiemi | - Komiks s textovým přepisem a minikvízem<br>- Chatbot<br>- Metodické listy (45 - 90 minut) |
| **Digitální stopa: Příběh Báry**<br>5.-7. | Sdílení informací<br>Kyberšikana<br>Falešná identita<br>Nebezpečné výzvy na sociálních sítích<br>Podvodné nabídky<br>Platby online | VO-9-1-07 uplatňuje vhodné způsoby chování a komunikace v různých životních situacích<br>VZ-9-1-14 vyhodnotí na základě svých znalostí a zkušeností možný manipulativní vliv vrstevníků, médií, sekt; uplatňuje osvojené dovednosti komunikační obrany proti manipulaci a agresi<br>EV-9-1-01 komunikuje otevřeně, pravdivě, s porozuměním pro potřeby druhých a přiměřeně situaci<br>I-5-4-03 dodržuje bezpečnostní a jiná pravidla pro práci s digitálními technologiemi | - Komiks s textovým přepisem a minikvízem<br>- Metodické listy (45 - 90 minut) |
| **Jsem netvor na základce**<br>8.-9. | Umělá inteligence<br>Pravdivost informací (Hoax, DeepFake…)<br>Autorské práva<br>Přihlašovací údaje<br>Malware<br>Hackování<br>Sdílení informací<br>Online platby<br>Soukromí komunikace | I-9-3-01 vysvětlí účel informačních systémů, které používá, identifikuje jejich jednotlivé prvky a vztahy mezi nimi; zvažuje možná rizika při navrhování i užívání informačních systémů<br>I-9-4-01 popíše, jak funguje počítač po stránce hardwaru i operačního systému; diskutuje o fungování digitálních technologií určujících trendy ve světě<br>I-9-4-05 dokáže usměrnit svoji činnost tak, aby minimalizoval riziko ztráty či zneužití dat; popíše fungování a diskutuje omezení zabezpečovacích řešení<br>EV-9-1-08 analyzuje etické aspekty různých životních situací | - Videokurz s minikvízem<br>- Metodické listy (9x 45 - 90 minut) a pracovní listy |

[2] K poslechu na radio junior
https://junior.rozhlas.cz/vanda-a-eda-v-onljn-svete-jak-se-neztratit-na-internetu-8335191

## 4.2 O2 Chytrá škola

Tato podkapitola primárně čerpá z [51] a [52].

O2 Chytrá škola[3] a jejich web Bezpečně v síti.cz[4] jsou projekty Nadace O2 jehož cílem je učit děti, rodiče a učitele správnému využívání technologií a dodržování bezpečnostních zásad.

Portál Bezpečně v síti.cz nabízí přehled článků, výzkumů a dalších materiálů (videí, kvízů…), zaměřených na témata internetové bezpečnosti a osvěty s digitálními technologiemi spojené. V sekci Výuka jsou vyčleněny čtyři tématické okruhy a to:

- Online bezpečnost
- Mediální gramotnost
- Počítačová gramotnost
- Technologie ve vzdělání

**Tabulka 4.2** O2 Chytrá škola – výuka, zpracováno na základě [52]

| Téma | Sekce | Metodické náměty | Infoleták | Kvíz |
|---|---|---|---|---|
| Online Bezpečnost | Kybernetická šikana | ano | ano | ano |
| | Sexting | ano | ne | ano |
| | Online radikalizace | ano | ne | ano |
| | Phishing, viry a sociální inženýrství | ne | ano | ano |
| | Bezpečné seznamování online | ano | ne | ano |
| | Jak mluvit s dětmi o online bezpečí | ano | ne | ano |
| | Kybergrooming | ne | ano | ano |
| | Kyberstalking | ne | ne | ne |
| | Nakupování online | ne | ne | ne |
| | Ukradené a falešné účty | ano | ano | ano |
| | Rizikové online výzvy (challenges) | ne | ano | ano |
| | Zdraví v online světě | ano | ano | ano |
| | Děti a porno: společně na internetu | ano | ano | ano |
| Mediální gramotnost | Fake news, ddeepfake a hoaxy | ano | ano | ano |
| | Autorské práva | ne | ano | ano |
| | Typy médií | ano | ano | ano |
| | Ochrana osobních údajů | ne | ano | ano |
| | Reklama | ano | ano | ano |
| | Mediální stereotypy | ano | ano | ano |
| | Propaganda a cenzura | ano | ano | ano |
| Počítačová gramotnost | Bezpečné heslo | ano | ano | ano |
| | Připojujte se na Wi-Fi bezpečně | ne | ne | ne |
| | Jak se chránit na sociálních sítí | ano | ano | ne |
| | Algoritmy sociálních sítí | ano | ano | ne |
| | Jak chránit svá data, počítač a mobil | ano | ano | ano |
| | Praní všemi deseti | ne | ne | ne |
| | Online hry | ne | ne | ne |
| | Cookies | ano | ne | ne |

Jednotlivé okruhy jsou dále členěny na tématické sekce. Základem sekce je vždy textový obsah a doplňující videa popisující danou problematiku. V podkladech ke stažení jsou často k dispozici vypracované metodické náměty a výukové aktivity, spolu s dalšími materiály, například infolisty a brožurami. Tématický okruh Technologie ve vzdělání se věnuje především vysvětlení jednotlivých nástrojů a způsobů, jakým mohou být při výuce využity.

[3] Dostupný skrze `https://o2chytraskola.cz/`
[4] Dostupný skrze `https://bezpecnevsiti.cz/`

Tématicky pokrývá portál všechny prací vymezené témata a dalším tématům se věnuje. Přihlašovacím údajům se primárně věnuje v tématickém okruhu Počítačová gramotnost – Bezpečné heslo, kde jsou připravené rady k ochraně a tvorbě přihlašovacích údajů spolu s kvízem, infolistem a metodickým námětem na výukové aktivity. K dispozici je také příručka pro děti a rodiče určena především dětem od 6 do 12 let. Sociálnímu inženýrství a nebezpečí malware je věnována sekce Online bezpečnost – Phishing, viry a sociální inženýrství. K dispozici je infolist a kvíz.

U metodických námětů nebývají uvedené RVP cíle, časová náročnost materiálů a cílová skupina pro kterou jsou materiály a aktivity vypracovány. Materiál je vypracován s návodem včetně řešení, doplňujících ilustračních obrázků a případných návrhů pracovních listů.

## 4.3 Kraje pro bezpečný Internet

Tato podkapitola primárně čerpá z [53].

Kraje pro bezpečný Internet[5] je projekt Asociace krajů ČR, který vznikl v roce 2013. Cílem je zvýšit informovanost o rizicích na internetu a možné prevenci.

Na portálu jsou volně přístupné pracovní listy, což jsou jednostránkové, převážně informativní materiály. Na oficiálním youtubovém kanálu, jsou pak k dispozici edukativní videa.

Součástí projektu je každoroční online kvíz o věcné ceny s tématikou internetové bezpečnosti, do které je nutné se zaregistrovat a správně odpovědět na všechny otázky kvízu (počet pokusů je neomezen). Soutěžící se mohou zúčastnit ve 3 věkových kategorií:

- 1. stupeň základních škol
- 2. stupeň základních škol a odpovídající stupeň víceletých gymnázií
- Střední školy

Soutěžní kvíz PLUS je nadstavbou a účastnit se ho mohou úspěšní řešitelé soutěžního kvízu. S maximálním počtem tří pokusů se účastník snaží zodpovědět deset otázek, které pokud zodpoví všechny správně, je zařazen do výsledkové listiny s dosaženým časem.

E-Kurzy jsou rozdělené dle cílových kategorií a to na:

- Kurz pro děti a studenty
- Kurz pro rodiče a veřejnost
- Kurz pro sociální pracovníky
- Kurz pro příslušníky a občanské zaměstnance Policie České republiky
- Kurz pro pedagogy
- Kurz pro seniory

Kurz je tvořen z primárně textového obsahu doplněného o vhodné ilustrativní obrázky, občas v nepříliš kvalitním rozlišení. Některé lekce jsou k dispozici formou videa a případného pracovního listu. Kurzy je možné si prohlédnout bez registrace, ta je však nutná v případě, že chce zájemce získat certifikát.

## 4.4 E-Bezpečí

Tato podkapitola primárně čerpá z [54].

E-Bezpečí[6] je projekt Centra prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého. Jedná se o certifikovaný projekt primární prevence rizikového chování a dalšího vzdělávání pedagogických pracovníků. Projekt je zaměřený na vzdělávání, výzkum a osvětu v oblasti bezpečnosti na internetu. Hlavními tématy E-Bezpečí jsou:

[5] Dostupný skrze `https://www.kpbi.cz/`
[6] Dostupný skrze `https://www.e-bezpeci.cz/`

- kyberšikanu a sexting
- kybergrooming
- kyberstalking a stalking
- rizika sociálních sítí
- hoax, spam a fake news
- online závislosti
- fenomén youtubering
- zneužití osobních údajů v prostředí elektronických médií

E-Bezpečí realizuje multimediální přednášky/besedy, celorepublikova výzkumná šetření, online poradnu, publikaci tiskovin pro žáky a učitele, e-kurzy a řadu dalších aktivit.

Vzdělávací akce jsou určeny pro žáky 2. stupně základních škol a zaměřují se především na digitální a mediální gramotnost. Besedy o délce 2 x 45 minut probíhají prezenčně či formou webináře a jejich cena je uvedena na stránkách projektu.

Na portálu E-Bezpečí je možné nalézt řadu materiálů ke stažení, jako jsou odborné studie a informační letáky. K dispozici je kniha Bezpečné chování na internetu pro kluky a pro holky, která nabízí rozsáhlou sadu námětů na výukové aktivity. Ty se věnují tématům jako jsou základy počítačové bezpečnosti, kyberšikana či online komunikace.

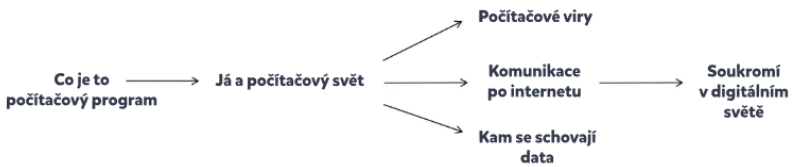
## 4.5 Datová Lhota

V této kapitole jsem vycházela z [55] a materiálů na [56] dostupných.

Datová Lhota[7] spolu s veškerými materiály je dostupná na stránkách České televize. Projekt pokrývá oblast Software a věnuje se i dalším oblastem, primárně s cílem vysvětlit fungování na internetu.

Seriál Datová Lhota vznikl ve spolupráci České televize, Matematicko-fyzikální fakulty Univerzity Karlovy a společnosti CZ.NIC. Jedná se o animovaný seriál jehož součástí je webová hra a výukové materiály pokrývající vybrané části RVP ZV 2021 vzdělávací oblasti Informatika.

Cílovou skupinou jsou především žáci druhého až pátého ročníku. Seriál obsahuje deset pětiminutových epizod a devět bonusových episod s názvem Kubova talkshow. Bonusové episody mají délku od pěti do osmnácti minut. Výukové materiály jsou vypracovány ve dvou obtížnostech, které lze navzájem kombinovat. Lekce jsou strukturovány do fází a v bodech navádějí k jednotlivým aktivitám s žáky. Lekce obsahují také přílohu s dalšími materiály, jako jsou tabulky, obrázky, příklady možných otázek s odpovědmi a doprovodné technické informace. Kromě toho jsou k dispozici vypracované materiály k dodatečným aktivitám a technický popis dílů a použité metafory.




**Obrázek 4.1** Návaznost témat Datové Lhoty,převzato z [57]

[7] Dostupný skrze `https://decko.ceskatelevize.cz/datova-lhota`

**Tabulka 4.3** Datová Lhota – témata a časová náročnost, zpracováno na základě [56]

| **Lekce a doporučený ročník** | **Náplň** | **RVP ZV 2021 očekávané výstupy** | **Vyučovací hodiny** |
|---|---|---|---|
| **Co je to počítačový program**<br>2.-4. | Programování a pojmy s tím spojené<br>Co vše je počítač<br>Aktualizace | I-5-4-01 najde a spustí aplikaci<br>I-5-2-01 sestavuje a testuje symbolické zápisy postupů<br>I-5-2-02 popíše jednoduchý problém, navrhne a popíše jednotlivé kroky jeho řešení<br>I-5-4-03 dodržuje bezpečnostní a jiná pravidla pro práci s digitálními technologiemi<br>*I-9-4-04 poradí si s typickými závadami a chybovými stavy počítače* | 2 hodiny |
| **Já a počítačový svět**<br>2.-4. | Data a jejich přenos<br>Šifrování | I-5-4-01 žák pracuje s daty různého typu<br>I-5-1-01 žák uvede příklady dat, která ho obklopují | 1 hodina |
| **Kam se schovají data**<br>2.-4. | Paměťová úložiště<br>Správa dat | I-5-4-01 žák pracuje s daty různého typu<br>I-5-4-03 dodržuje bezpečnostní a jiná pravidla pro práci s digitálními technologiemi | 1 hodina |
| **Počítačové viry**<br>2.-4. | Malware<br>Antivirové programy | I-5-4-03 dodržuje bezpečnostní a jiná pravidla pro práci s digitálními technologiemi<br>*I-9-4-04 poradí si s typickými závadami a chybovými stavy počítače*<br>*I-9-4-05 dokáže usměrnit svoji činnost tak, aby minimalizoval riziko ztráty či zneužití dat; popíše fungování a diskutuje omezení zabezpečovacích řešen* | 1 hodina |
| **Komunikace po internetu**<br>4.-5. | Internetová komunikace (Wi-Fi, router, DNS server, IPadresa)<br>Internetová bezpečnost | I-5-4-02 propojí digitální zařízení, uvede možná rizika, která s takovým propojením souvisejí<br>I-5-4-03 dodržuje bezpečnostní a jiná pravidla pro práci s digitálními technologiemi<br>I-5-1-01 uvede příklady dat, která ho obklopují a která mu mohou pomoci lépe se rozhodnout; vyslovuje odpovědi na základě dat<br>I-5-1-03 vyčte informace z daného modelu<br>*I-9-4-02 ukládá a spravuje svá data ve vhodném formátu s ohledem na jejich další zpracování či přenos*<br>*I-9-4-03 uvede příklady sítí a popíše jejich charakteristické znaky*<br>*I-9-4-05 dokáže usměrnit svoji činnost tak, aby minimalizoval riziko ztráty či zneužití dat* | 2 hodiny |
| **Soukromí v digitálním světě**<br>4.-5. | Datová stopa<br>Cookies<br>Online reklama (cílená reklama) | I-5-4-02 propojí digitální zařízení, uvede možná rizika, která s takovým propojením souvisejí<br>I-5-4-03 dodržuje bezpečnostní a jiná pravidla pro práci s digitálními technologiemi<br>*I-9-4-05 dokáže usměrnit svoji činnost tak, aby minimalizoval riziko zneužití dat* | 1 hodina |

## 4.6 #nePINdej

Tato podkapitola primárně čerpá z [58].

Kampaň #nePINdej[8] je celonárodní vzdělávací kampaň od České bankovní asociace a jejích partnerů, která reaguje na rostoucí útoky na klienty bank. Projekt se zabývá především metodami sociálního inženýrství a nebezpečí s nimi spojenými.

Na stránkách kampaně jsou vypracovány materiály o základních krocích bezpečnosti na internetu a nejčastějších typech podvodů mezi které patří phishing, smishing, vishing, podvodné veřejné WiFi sítě a další. Své vědomosti si může uživatel ověřit právě pomocí kvízu, který zároveň svými ukázkami působí jako edukativní nástroj.

## 4.7 Internetoví úžasňáci

Tato podkapitola primárně čerpá z [59].

Program Internetoví úžasňáci[9] je součástí projektu Be internet awesome, který se věnuje tématům kyberprevence. Program byl vytvořen společností Google ve spolupráci s organizací iKeepSafe a Online Family Safety Institute. V rámci České republiky ho realizuje nezisková organizace Jules a Jim, z. ú.

Program nabízí školení pro pedagogy základních škol, které je díky grantu od Googlu zdarma. Školení je rozděleno do dvou bloků o celkové délce 5 hodin, během kterého jsou pedagogové proškoleni v připraveném učebním plánu využívajícího interaktivní hru Interland.

Učební plán je rozdělen do 5 lekcí:

- Sdílej s rozumem – sdílení informací a dalšího obsahu online
- Neskákej na fejky – phishing, dezinformace…
- Chraň si svoje tajemství – tvorba přihlašovacích údajů
- Laskavost je super – chování a komunikace na internetu
- Když se ti něco nezdá, ozvi se

Plán obsahuje různé aktivity, přičemž ne všechny vyžadují práci na počítači. Lekce je možné využít i během výuky jiných předmětů, než je informatika, například v hodinách etické a mediální výchovy.

Interland je volně přístupná hra rozdělená do čtyř tématických sekcí a jejich perspektivních mini-her, které odpovídají prvním čtyřem tématům lekcí. Každá mini-hra je jiná.

## 4.8 Další projekty

**iMyšlení.cz** Projekt Podpora rozvoje informatického myšlení (dále jen PRIM) vznikl za účelem podpory vyučování předmětu informatika na všech stupních mateřských, základních a středních školách.

Projekt iMyšlení.cz[10] vznikl jako reakce na potřebu IT odborníků a všeobecnou informovanost populace v oblasti informatiky. Cílem bylo připravit školní kurikulum, vzdělávací materiály, podporovat inovace v oblasti školské informatiky a další. Projekt byl ukončen v září 2020, avšak některé z navázaných aktivit stále pokračují.

[8] Dostupný skrze `https://www.kybertest.cz/`
[9] Dostupný skrze `https://www.internetoviuzasnaci.org/`
[10] Dostupný skrze `https://imysleni.cz/`

V rámci projektu vzniklo několik vzdělávacích materiálů, včetně učebnic Základy informatiky pro 1. stupeň ZŠ a Základy informatiky pro 2. stupeň ZŠ schválenými 28. 4. 2021 MŠMT a zařazenými do seznamu učebnic pro základní vzdělávání jako součást ucelené řady učebnic pro vzdělávací obor Informatika s dobou platnosti šest let. Učebnice byly upravené, aby odpovídaly očekávaným výstupům dle RVP ZV 2021. K dispozici jsou i pracovní listy.

**Internetem Bezpečně** Projekt Internetem Bezpečně[11] od neziskové organizace you connected, z. s. Projekt je zaměřený na zvyšování povědomí o rizicích na internetu. K dispozici je několik brožur včetně učebnice Informatiky.

**Vím, kam klikám** Projekt Vím, kam klikám[12], je projektem vytvořeným ve spolupráci projektu Kraje pro bezpečný Internet a společnosti GODRIC, jehož cílem je informovat o bezpečnostních rizicích spojených s Internetem. V rámci projektu jsou publikované články zaměřené na bezpečné využívání internetu a varující před aktuálními rizikovými trendy.

**Internet Highway** Projekt Internet Highway[13] od E-Bezepčí vznikl za podpory MŠMT. Jedná se o interaktivní vzdělávací hru pro žáky základních škol, jejíž cílem je informovat o internetových rizicích.

**Replug me** Projekt Replug me[14] nabízí workshopy pro třídy a akreditované kurzy pro učitele v oblasti digitální výchovy (zdravý přístup k digitálním technologiím a zacházení s nimi).

**How Secure Is My Password** Projekt How Secure Is My Password[15], spravovaný společností Security.org, umožňuje vyzkoušet sílu hesla.

**Website Security Checker** Webová stránka Website Security Checker[16] od společnosti Sucuri umožňuje vložit URL adresu a stránka zkontroluje zda daný odkaz vede na webovou stránku nakaženou známým malwarem či je jinak potenciálně nebezpečná.

**Have I Been Pwned?** Projekt Troye Hunta Have I Been Pwned?[17] je webová stránka, která umožňuje zjistit, zda daný účet byl kompromitován při úniku dat.

## 4.9 Vyhodnocení

Tabulka 4.4 shrnuje poznatky výše uvedených projektů. Jednotlivé sloupce znázorňují:

**Ročník** – doporučený ročník, pro který je materiál tvořen

**RVP ZV** – zda jsou uvedeny očekávané výstupy dle RVP ZV u daného materiálu

**Materiály** – jakou formu nabývá materiál, vyjma metodických listů

**Metodické listy** – zda jsou k látce vypracovány metodické listy či metodické návrhy na aktivity

[11] Dostupný skrze `https://www.internetembezpecne.cz/`
[12] Dostupný skrze `https://www.vimkamklikam.cz/`
[13] Dostupný skrze `https://www.internethighway.cz/`
[14] Dostupný skrze `https://www.replug.me/`
[15] Dostupný skrze `https://howsecureismypassword.net/`
alternativně `https://www.security.org/how-secure-is-my-password/`
[16] Dostupný skrze `https://sitecheck.sucuri.net/`
[17] Dostupný skrze `https://haveibeenpwned.com/`

**Tabulka 4.4** Projekty – nabídka materiálů, jejich forma a cílová skupina, vlastní tvorba na základě předchozích podkapitol

| Název projektu | Ročník | RVP ZV | Materiály | Metodické listy |
|---|---|---|---|---|
| **Osvěta NÚKIB** | 1. - 9. | ano | komiks, povídky, videokurz | ano |
| **O2 Chytrá škola** | neuveden | částečné[18] | videa, text | většinou ano |
| **Kraje pro bezpečný Internet** | neuveden | ne | e-kurzy, videa | ne |
| **E-Bezpečí** | 6. - 9. | ne | e-kurzy, besedy | ne |
| **Datová Lhota** | 2. - 5. | ano | videa, hra | ano |
| **#nePINdej** | 6. - 9. | ne | text, kvíz | ne |
| **Internetoví úžasňáci** | 2. - 5 | ne | hra | ano |

V rámci této práce byla vymezena tři témata informační bezpečnosti: **Přihlašovací údaje, Software** a **Sociální inženýrství**. V rámci tabulky 4.5 je zaznamenáno pokrytí těchto témat danými projekty. Hodnota „ano“ znázorňuje, že se daný projekt věnuje tématu ve většině jeho vymezení v kapitole 1.

**Tabulka 4.5** Pokrytí témat informační bezpečnosti danými projekty, vlastní tvorba na základě předchozích podkapitol

| Název projektu | Pokrytí témat vymezených v této práci | | |
|---|---|---|---|
| | **Přihlašovací údaje** | **Software** | **Sociální inženýrství** |
| **Osvěta NÚKIB** | ano | ano | ano |
| **O2 Chytrá škola** | ano | ano | ano |
| **Kraje pro bezpečný Internet** | ano | ano | ano |
| **E-Bezpečí** | ne | okrajově | okrajově |
| **Datová Lhota** | ne | ano | ne |
| **#nePINdej** | ne | ne | ano |
| **Internetoví úžasňáci** | ano | ne | ne |

Všechny zmíněné projekty nabízí určité materiály, které lze pro účely výuky převzít či z nich během výuky vycházet. Převzatelnost těchto materiálů se napříč projekty liší stejně jako jejich podoba. Jelikož jsou tyto materiály volně přístupné (s výjimkou besed od E-Bezpečí, které se zaměřují primárně na témata mimo rámec této práce), největším nákladem je čas, který pedagog stráví při jejich přebírání a začleňovaní do výuky. Tyto skutečnosti a další poznatky s materiály spojenými jsou popsány níže:

**Osvěta NÚKIB** Portál nabízí vypracované metodické listy, ke svým kurzům. Kurzy jsou uzpůsobeny cíleným věkovým kategoriím a často je lze procházet více způsoby (audio forma povídek, interaktivní chat…).

Kurz určený pro poslední dva ročníky základních škol, Jsem netvor, se věnuje všem v prací vymezeným tématům a dalších témat se dotýká. Kurzy pro nižší ročníky se zaměřují především na práci s informacemi (jejich sdílení a přistupování k nim) a mezilidskou komunikaci na internetu. Dotýkají se metod sociálního inženýrství, jakými jsou podvodné identity a sběr informací pomocí sociálních sítí a jiných veřejných informací, které jsou následně zneužity.

**O2 Chytrá škola** Portál je především informační a zaměřen na samostatné vzdělávání se v daných oblastech. Mimo to, ale nabízí i několik materiálů připravených pro výuku na školách.

**Kraje pro bezpečný Internet** Portál je především zaměřen pro samovzdělávání. Absolvování e-kurzu je možné realizovat i v rámci školní výuky. Prací vymezené téma **Přihlašovacích údajů** by v rámci kurzu mohlo být probráno důkladněji nad rámec obecných doporučení

[18] U vybraných materiálů je zmíněno v rámci kterých oblastí jsou očekávané výstupy daného materiálu. Výstupy však nejsou explicitně zmíněné ve formátu uvedeným RVP ZV.

(délka hesla, jeho unikátnost…), protože právě toto pochopení umožňuje lépe předcházet rizikům.

K dispozici je i několik pracovních listů, jak v rámci e-kurzu, tak volně přístupných ke stažení, které lze převzít a pracovat s nimi v jejich nezměněné podobě. Tyto listy jsou však velice barevně zpracované, což ztěžuje jejich případný tisk.

**E-Bezpečí** Projekt nabízí především výzkumné zprávy a vzdělávací články. K dispozici je několik brožur a jiných materiálů poskytující náměty na výukové aktivity, které lze převzít, či se jimi inspirovat.

E-Bezpečí nabízí besedy, které se primárně věnují jiným tématům, než má tato práce vymezené. Besedy jsou vyučovány lektorem poskytnutým projektem a jsou zpoplatněny.

**Datová Lhota** Projekt Datová Lhota poskytuje vhodný základ k porozumění fungování digitálních technologií a rizik s nimi spojených. K dispozici jsou vypracované metodické listy ke každé lekci, které lze převzít a vést dle nich hodinu.

**#nePINdej** Kvíz je možné využít jako edukativní nástroj na kterém si žáci procvičí své rozpoznávací schopnosti v oblasti metod sociálního inženýrství. Nabízí řadu ilustrativně zpracovaných reálných metod sociálního inženýrství a ve své podstatě tak zároveň v průběhu jeho vyplňování vzdělává.

**Internetoví úžasňáci** Projekt nabízí volně přístupnou hru Interland a kurz pro pedagogy. Kurz má za účel informovat účastníky o využitelnosti hry Interland během výuky a představit vzdělávací materiály k projektu vypracované a jak s nimi zacházet. Po absolvování kurzu, jsou absolventům poskytnuty prezentace a další podklady pro výuku.

Nejlépe převzatelné materiály pro výuku celé vyučovací hodiny nabízí Osvěta NÚKIB a Datová Lhota, která má zpracované jak metodické listy sloužící jako podklad pro lekci, tak uvedené výstupy RVP ZV. Oboje pomáhá k lepšímu začlenění materiálů do hodin. Podobně zpracované materiály nabízí O2 Chytrá škola, která však neuvádí očekávané RVP ZV. Jelikož materiály k lekcím od projektu Internetoví úžasňáci nejsou volně přístupné, nelze jejich převzatelnost hodnotit. Pro převzetí a inspiraci v aktivitách jsou vhodné materiály od Kraje pro bezpečný Internet a E-Bezpečí. Kampaň #nePINdej a její kvíz může sloužit jako doplňková vzdělávací aktivita.

Na základě tabulek 4.4, 4.5, hodnocení výše zmíněného a veškerých poznatků v práci uvedených tato práce pro výuku vymezených témat informační bezpečnosti doporučuje následující projekty, s přihlédnutím na další témata, kterým se projekt věnuje:

**Pro první stupeň** využít k výuce materiály poskytnuté projektem Datová Lhota, které nabízí pochopení fungování digitálních technologií, na které lze navázat v pozdějších ročnících hlubším porozuměním. Datová Lhota se téměř nevěnuje práci s přihlašovacími údaji, což je téma které je vhodné doplnit. Projekt Internetoví úžasňáci se mu v rámci své 3. lekce věnuje, případně se mu věnuje minihra Věž pokladů v rámci hry Interland, která může být zajímavým zpestřením pro mladší žáky.

**Pro druhý stupeň** nejobsáhlejším zdrojem materiálů je Jsem netvor od NÚKIBu, který pokrývá prací vymezené témata. Vhodným doplňkem je kampaň #nePINdej, která informuje především o metodách sociálního inženýrství, s kterými se lze pravidelně setkat.

# Kapitola 5

# Diskuze a navazující práce

Jedním z cílů této bakalářské práce bylo provést analýzu informačně bezpečnostních rizik pro žáky základních škol. K popsání rizikových oblastí došlo především v kapitole 1.

V rámci práce bylo vypracováno dotazníkové šetření. Při tvorbě dotazníku bylo zvoleno tématicky široké pásmo otázek, které tak bylo možné vyhodnotit pouze povrchově. V navazujících pracích či jiných pracích těmito tématy se zabývajících, by bylo vhodné výraznější tématické vymezení. To by umožnilo věnovat více otázek jednomu tématu a lépe analyzovat pochopení tématu jednotlivými žáky. Například otázku č. 18 „Sdílíš na sociálních sítích své osobní údaje?“ by bylo vhodné doplnit otázkou „Máš sociální sítě?“ díky níž by získaná data měla větší vypovídající hodnotu. V rámci této problematiky by pak bylo dále potřeba vymezit pojem sociálních sítí, kterýžto pojem mohou žáci intuitivně vyhodnocovat odlišně a v závislosti na tom zahrnovat jiné služby do něj patřící.

Při tvorbě dotazníku bylo využito konzultací a testovací dotazník, před samotným vyplněním žáků škol, byl vyplněn malým vzorkem žáků. V následujících pracích by bylo doporučeno prohloubit spolupráci s vyučujícími žáků, která by umožnila lépe formulovat otázky zaměřené především na nižší ročníky. Bylo by vhodné i zvětšit testovací vzorek respondentů, neboť mezi jednotlivými respondenty mohou být velké rozdíly a to především v nižších ročnících. Díky většímu testovacímu vzorku respondentů by bylo tak možné lépe odchytit jakékoliv nepřesnosti ve formulacích a usnadnit tak respondentům odpovědi na dotazník.

Výsledky dotazníku a této práce jsou ovlivněny mnoha faktory. Jedním z těchto faktorů je epidemie covidu 19, díky které došlo k distanční výuce. Distanční výuka často vyžadovala práci s výpočetní technikou a díky tomu se lze domnívat, že došlo k určitému proškolení žáků i vyučujících v této oblasti. Bylo by zajímavé posoudit jaký vliv měla právě epidemie a distanční výuka s ní spojená na vzdělanosti v oblasti informační bezpečnosti a práci s ICT.

Výrazným faktorem je v současné době nastupující nové RVP ZV 2021, podle kterého již některé školy vyučují a jiné teprve začnou. V následujících letech tak bude možné pozorovat posun způsobený zvýšením časové dotace ve vzdělávací oblasti Informatika a způsobu kterým školy její výuku pojmou. Z toho důvodu by bylo vhodné zvážit provedení stejné či podobné práce spolu s dotazníkovým šetření za několik let a analyzovat dopady nových RVP.

# Kapitola 6
# Závěr

Síla digitalizace je neúprosná a její vliv na život lze pozorovat i u těch nejmladších. Cílem škol je připravit jedince na život a digitální technologie se staly neodmyslitelnou součástí tohoto života. To reflektují RVP ZV 2021 v kterých došlo v zásadní změně v nově přejmenované vzdělávací oblasti Informatika. Ta posílila z 1 hodiny na prvním stupni a 1 hodiny na stupni druhém na 2 hodiny na stupni prvním a 4 hodiny na stupni druhým. Za předpokladu, že školy budou vyučovat jednu hodinu týdně během jednoho ročníku bude časová dotace pokrývat 4. až 9. třídu.

Bakalářská práce si kladla za cíl podpořit učitele při výuce informační bezpečnosti pomocí navrhnutí možných preventivních aktivit.

Teoretická část práce popisuje vybraná informačně bezpečnostní rizika, kterým je žák základní školy vystaven. Tyto rizika byla popsaná včetně několika obecných doporučení spojených s jejich prevencí. Informačním bezpečnostním rizikům se věnuje kapitola 1 a rizika jsou vymezena do třech tématických oblastí a to **Bezpečnost přihlašovacích údajů**, **Sociální inženýrství** a **Bezpečnost software**. Kapitola 2 se zaměřuje především na popis RVP ZV z roku 2005, 2017 a 2021, které udávají rámec pro výuku informatiky na základních školách. Současně nastupující RVP ZV 2021 se informatice věnují důsledněji a značně navyšují její časovou dotaci. Jedním z jejich primárních cílů v oblasti informatiky je u žáků rozvinout informační a algoritmické myšlení.

Analytická část se v kapitole 3 zabývá analýzou výsledků dotazníkového šetření provedeného na základních školách. To ukazuje, že žáci stále mají nedostatky v informační bezpečnosti a vystavují se rizikům například používáním jednoho hesla pro všechny účty. V kapitole byla provedena i analýza konkrétní základní školy a jejího přístupu k výuce informatiky a prevenci informačně bezpečnostních rizik. Tato základní škola již vyučuje podle nových RVP ZV 2021.

V praktické části v kapitole 4 byly zhodnoceny vybrané zdroje nabízející podpůrné materiály pro výuku informační bezpečnosti. Bylo provedeno vyhodnocení převzatelnosti těchto materiálů a byl vypracován návrh z kterých zdrojů nejlépe čerpat. Pro první stupeň základních škol byl doporučen projekt Datová Lhota od České televize a Internetový úžasňáci. Pro stupeň druhý pak primárně kurz Jsem Netvor od Osvěty NÚKIB, doplněná případně o kampaň #nePINdej.

# Dodatek A

# Informační bezpečnost dotazník

V této kapitole je přiložená pdf verze Informačního dotazníku, který byl vytvořen v rámci této bakalářské práce. Dotazník byl distribuován v jeho online podobě.

# Informační bezpečnost

Ahoj!
Prosíme o Tvoji pomoc s vyplněním dotazníku na téma informační bezpečnost. Nejde o žádný test: nejsou tu žádné správné ani špatné odpovědi.
Odpovídej, prosím, upřímně. Dotazník je anonymní. Tvé odpovědi nebudou spojeny s tvým jménem a ani nebudou předány učiteli. Informace
slouží pouze pro účely výzkumu.

* Označuje povinnou otázku

1. V jakém ročníku studuješ? *

*Označte jen jednu elipsu.*

- 3
- 4
- 5
- 6
- 7
- 8
- 9

2. Které heslo je podle Tebe nejbezpečnější? *

*Označte jen jednu elipsu.*

- 123456
- heslo
- passw0rd
- Sk8kPes,P5esOves
- Kralicek12
- BatManJede!

3. Co děláš pro zapamatování hesla? Můžeš vybrat více odpovědí. *

*Zaškrtněte všechny platné možnosti.*

- [ ] Uložím si ho do prohlížeče (Chrome, Firefox, MS Edge, ...)
- [ ] Zapíšu si ho do sešitu ve kterém mám další hesla
- [ ] Napíšu si ho na lístek, který mám hned na očích
- [ ] Použiji PasswordManager (jde o správce hesel, jehož úkolem je si pamatovat hesla za vás)
- [ ] Používám hardwarové klíče (hardwarové zařízení, například USB, připojující se k počítači a sloužící jako klíč)
- [ ] Mám jedno heslo pro všechno a to si pamatuji
- [ ] Uložím si heslo do textového souboru (v mobilu, v počítači)
- [ ] Svoje hesla si pamatuji
- [ ] Hesla mi spravuje rodina

4. Máš vlastní mobilní telefon? *

*Označte jen jednu elipsu.*

- ◯ Ano
- ◯ Mám víc mobilních telefonů
- ◯ Mám ho se sourozenci společně
- ◯ Ne

5. Kdo všechno umí odemknout Tvůj mobil (např. zná Tvůj PIN)? Můžeš vybrat více odpovědí. *

*Zaškrtněte všechny platné možnosti.*

- [ ] Jen já
- [ ] Moji rodiče
- [ ] Moji sourozenci
- [ ] Jiný rodinný příslušník
- [ ] Někteří moji kamarádi
- [ ] Nemám heslo
- [ ] Nemám mobil

6. Jaký máš zámek na mobilní telefon? *

*Označte jen jednu elipsu.*

- Heslo
- Gesto (znak, přejetí po obrazovce)
- PIN kód
- Biometrické údaje (otisk, obličej) a heslo
- Biometrické údaje (otisk, obličej) a znak
- Biometrické údaje (otisk, obličej) a PIN kód
- Žádné
- Nemám mobilní telefon

7. Používáš jiné heslo pro každý účet? *

*Označte jen jednu elipsu.*

- Ano, pro každý
- Ano, pro ty důležité (email, počítač, školní údaje, banka...)
- Ne
- Hesla k účtům mi řeší rodina

8. Aktualizuješ pravidelně software? (aplikace, hry, windows, antivir...) *

*Označte jen jednu elipsu.*

- Ano
- Ano, ty důležité
- Ne
- Řeší to za mě rodina

9. Setkal ses někdy s útokem na svůj účet? *

*Označte jen jednu elipsu.*

- Ano, byl mi ukraden
- Ano, ale nebyl mi ukraden
- Nevím
- Nevím, jak to poznat
- Ne

10. Používáš na všech zařízeních antivir (program, který má za cíl detekovat a případně odstranit škodlivý kód)? *

*Označte jen jednu elipsu.*

- Ano, mám na nich nainstalovaný antivirový program (ESET, AVAST...)
- Myslím si, že ano
- Ne
- Nevím, řeší to za mě rodina

11. Kontroluješ oprávnění aplikací (k čemu mají přístup - např. fotky, dokumenty, Tvoje poloha)? *

*Označte jen jednu elipsu.*

- Ano, při stažení
- Ano, jednou za čas si je projdu
- Ne
- Řeší to za mě rodina

12. Jak si vybíráš, kterou aplikaci si nainstaluješ? (hry na mobil...) Můžeš vybrat více odpovědí. *

*Zaškrtněte všechny platné možnosti.*

- [ ] Doporučení kamarádů či rodiny
- [ ] Reklama v jiné hře
- [ ] Reklama jinde na internetu
- [ ] Náhodné nalezení hry
- [ ] Recenze, či jiná doporučení
- [ ] Přijde mi emailová či jiná zpráva (messenger, instagramová zpráva, sms...) s odkazem na stažení

13. Ptáš se před stažením aplikace rodinného příslušníka? (bratr, sestra, rodiče...) *

*Označte jen jednu elipsu.*

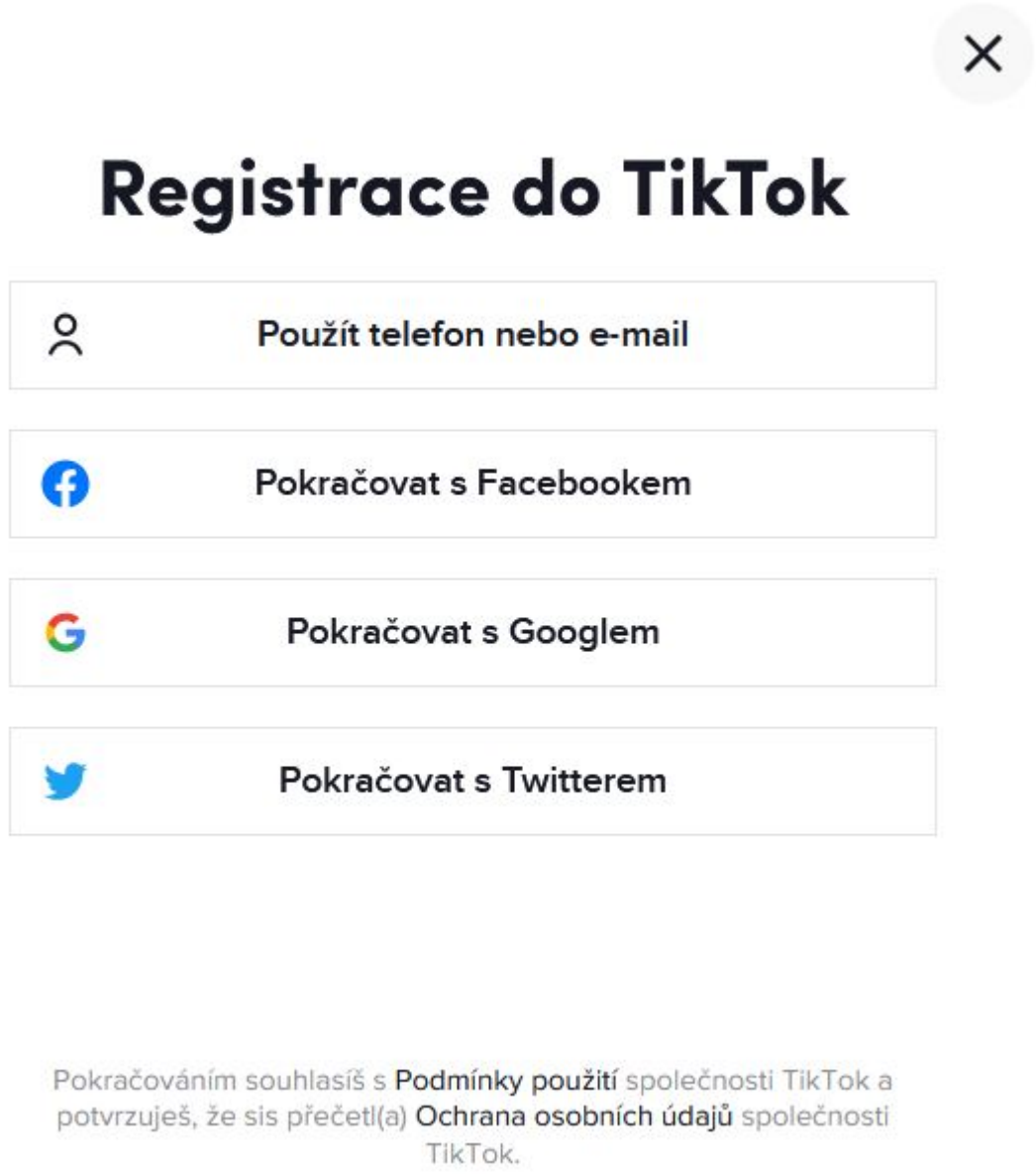
- ◯ Ano
- ◯ Ano, ale někoho jiného než rodinného příslušníka
- ◯ Občas
- ◯ Ne

14. Kontroluje rodina jakým způsobem využíváš výpočetní techniku? (mobil, notebook, počítač, herní konzole...) Můžeš vybrat více odpovědí. *

*Zaškrtněte všechny platné možnosti.*

- [ ] Hlídají obsah, ke kterému přistupuji
- [ ] Hlídají, kolik času u nich strávím
- [ ] Občas se zeptají
- [ ] Nekontrolují vůbec
- [ ] Občas mě upozorní na nebezpečí

15. V případě potřeby založení účtu (k aplikaci, pro webovou stránku, sociální síť...) využiješ možnost přihlášení pomocí jiného již existujícího účtu (nejčastěji google, facebook, twitter)? Obrázek je ilustrační. *




*Označte jen jednu elipsu.*

- Ano, vždy využiji možnost propojení k již existujícímu
- Ano, většinou využiji již existující účet
- Ne, vždy zakládám účet pro daný produkt
- Nikdy se sám/sama neregistruji do aplikací
- Účty mi spravuje rodina

16. Jaké chatovací aplikace používáš pro osobní komunikaci (komunikaci s rodinou, kamarády...)? Můžeš vybrat více odpovědí. *

*Zaškrtněte všechny platné možnosti.*

- [ ] Telegram
- [ ] Viber
- [ ] Signal
- [ ] WhatsApp
- [ ] Facebook Messenger
- [ ] Line
- [ ] WeChat
- [ ] Skype
- [ ] Google messages
- [ ] Google Hangouts
- [ ] Apple iMessages
- [ ] SMS
- [ ] Slack
- [ ] Snapchat
- [ ] Discord
- [ ] Microsoft Teams
- [ ] Instagram
- [ ] TikTok
- [ ] Kik
- [ ] Olvid
- [ ] Wire
- [ ] VKontakte
- [ ] Jiné: _____

17. Posíláš osobní fotografie pomocí chatovacích aplikací (WhatsAPP, instagram, Messenger)? Můžeš vybrat více odpovědí. *

*Zaškrtněte všechny platné možnosti.*

- [ ] Ano, rodině
- [ ] Ano, kamarádům
- [ ] Ano, pouze důvěryhodným osobám
- [ ] Ano, ale pouze pomocí zašifrované komunikace
- [ ] Ano, ale zprávy se automaticky mažou po nastaveném časovém úseku
- [ ] Ne, nikomu

18. Sdílíš na sociálních sítích své osobní údaje? Můžeš vybrat více odpovědí. *

*Zaškrtněte všechny platné možnosti.*

- [ ] Ano, mám tam svou fotografii
- [ ] Ano, mám tam uvedeno, kde bydlím
- [ ] Ano, mám uvedenou školu, kterou navštěvuji
- [ ] Ano, postnul/a jsem fotografii z místa, kam pravidelně chodím (jinde než doma či ve škole)
- [ ] Ano, někdy tam uvádím, kde se právě nacházím
- [ ] Ano, mám tam uvedené rodinné příslušníky (bratr, sestra, rodiče atd.)
- [ ] Myslím si, že neuvádím své údaje
- [ ] Ne

19. Komu řekneš heslo na wifi u sebe doma? Můžeš vybrat více odpovědí. *

*Zaškrtněte všechny platné možnosti.*

- [ ] Členům domácnosti
- [ ] Kamarádům
- [ ] Příbuzným
- [ ] Přítel/Přítelkyně
- [ ] Návštěvě
- [ ] Komukoliv, kdo požádá
- [ ] Řeší to za mě rodina - já nikomu

20. Co rozhoduje, zda klikneš na odkaz, který ti někdo pošle? Můžeš vybrat více odpovědí. *

*Zaškrtněte všechny platné možnosti.*

- [ ] Kdo mi ho poslal
- [ ] Jak ten odkaz vypadá
- [ ] Kam ten odkaz skutečně vede (například e-mail umí při přejetí myší přes odkaz ukázat adresu na kterou vede)
- [ ] Zda jsem očekával/a, že ho dostanu
- [ ] Obsah zprávy u níž se odkaz nachází
- [ ] Na jaké platformě jsem ho obdržel/a

21. Jsme na konci. Moc děkujeme za Tvůj čas a Tvé odpovědi. Pokud nám chceš ještě něco vzkázat, můžeš v tomto okénku :)

# Bibliografie


1. MACHACKOVA, H.; BLAYA, C.; BEDROSOVA, M.; SMAHEL, D.; STAKSRUD, E. *Children's experiences with cyberhate.* [online]. EU Kids Online., 2020 [cit. 2023-03-06]. Dostupné z: https://doi.org/10.21953/lse.zenkg9xw6pua.
2. JUDR. JAN KOLOUCH, Ph.D. *CYBERCRIME.* První české vydání. Praha: CZ.NIC, z. s. p. o., 2016. ISBN 978-80-88168-18-8.
3. JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* Páté doplněné a upravené vydání. Praha: Česká pobočka AFCEA, 2022. ISBN 978-80-908388-4-0.
4. *Základy kybernetické bezpečnosti: Dávej kyber!* [online]. NÚKIB [cit. 2023-03-12]. Dostupné z: https://osveta.nukib.cz/course/view.php?id=123.
5. ISO CENTRAL SECRETARY. *Information technology — Security techniques — Information security management systems — Overview and vocabulary.* Geneva, CH, 2018. Standard, ISO/IEC 27000:2018. International Organization for Standardization. Dostupné také z: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en.
6. ISO CENTRAL SECRETARY. *Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* Geneva, CH, 2022. Standard, ISO/IEC 27001:2022. International Organization for Standardization. Dostupné také z: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en.
7. *Co to jsou přihlašovací údaje a k čemu slouží - Policie České republiky* [online]. [cit. 2023-03-15]. Dostupné z: https://www.policie.cz/clanek/co-to-jsou-prihlasovaci-udaje-a-k-cemu-slouzi.aspx.
8. MALKUSOVÁ, Tereza; MUDRÁKOVÁ, Lucie. *Proč Si nechat Heslo K Netflixu Pro Sebe?* [online]. 2022-10. [cit. 2023-03-16]. Dostupné z: https://www.dvojklik.cz/proc-si-nechat-heslo-k-netflixu-pro-sebe/.
9. *Bezpečná hesla* [online]. cz.nic [cit. 2023-03-12]. Dostupné z: https://www.nebojteseinternetu.cz/page/3448/bezpecna-hesla/.
10. KOHOUT, Roman; KLOZOVÁ, Miroslava. *Heslo* [online]. 2021-10. [cit. 2023-03-14]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/navody/heslo/.
11. KUMAR, Mohit. *Comodohacker responsible for DigiNotar attack* [online]. 2011-07. [cit. 2023-03-13]. Dostupné z: https://thehackernews.com/2011/09/comodohacker-responsible-for-diginotar.html.
12. *Jak Na Bezpečné Heslo? Nejčastější Chyby, které (zřejmě) děláte také* [online]. [cit. 2023-03-13]. Dostupné z: https://ujezd.net/jak-na-bezpecna-hesla.

13. *The Curse of the Secret Question* [online]. [cit. 2023-03-13]. Dostupné z: https://www.schneier.com/blog/archives/2005/02/the_curse_of_th.html.

14. VILČEK, Ivan. *Slovenská ministryně informatiky Zveřejnila Omylem Heslo Ke Svému Počítači - Novinky* [online]. Novinky, 2022 [cit. 2023-03-17]. Dostupné z: https://www.novinky.cz/clanek/zahranicni-slovenska-ministryne-informatiky-zverejnila-omylem-heslo-ke-svemu-pocitaci-40401620.

15. MALKUSOVÁ, Tereza; MUDRÁKOVÁ, Lucie. *Jak tvořit Spolehlivá Hesla?* [online]. 2020. [cit. 2023-03-12]. Dostupné z: https://www.dvojklik.cz/jak-tvorit-spolehliva-hesla/.

16. MALKUSOVÁ, Tereza; MUDRÁKOVÁ, Lucie. *Co Je to password manager a proč Ho Používat?* [online]. 2020-07. [cit. 2023-03-12]. Dostupné z: https://www.dvojklik.cz/co-je-to-password-manager-a-proc-ho-pouzivat/.

17. BENEŠOVSKÁ, Michala. *Jednotné přihlašování: Je Bezpečné Přihlašovat se přes Google, Facebook Nebo Apple? • professional computing* [online]. 2022-10. [cit. 2023-03-27]. Dostupné z: https://procomputing.cz/jednotne-prihlasovani-je-bezpecne-prihlasovat-se-pres-google-facebook-nebo-apple/.

18. *Eduid.cz* [online]. [cit. 2023-03-27]. Dostupné z: https://www.eduid.cz/wiki/eduid/index.

19. *CZ.NIC - O Sdružení* [online]. [cit. 2023-03-13]. Dostupné z: https://www.nic.cz/page/351/.

20. *Ověřená Online Identita* [online]. cz.nic [cit. 2023-03-13]. Dostupné z: https://www.mojeid.cz/.

21. SKALKOVÁ, Olga. *Konec potvrzovacích SMS? Podmínky zpřísnily i dvě největší banky* [online]. 2022-03. [cit. 2023-03-14]. Dostupné z: https://www.penize.cz/osobni-ucty/433271-konec-potvrzovacich-sms-podminky-zprisnily-i-dve-nejvetsi-banky.

22. SPOLEČNOSTI, Odbor statistik rozvoje. *Informační Společnost V číslech 2022 - český statistický úřad* [online]. 2022. [cit. 2023-03-06]. Dostupné z: https://www.czso.cz/documents/10180/164503431/06100422.pdf/69ccf5e2-92e8-4dcd-b22a-cb3df3e8119a?version=1.3.

23. PEVNOST, Digitální. *Brute Force útok* [online]. [cit. 2023-03-17]. Dostupné z: https://www.digitalnipevnost.cz/viki/brute-force-utok.

24. JAN.HANACEK. *Útoky Hrubou Silou (Brute-force) A Jak Se Jim Bránit* [online]. 2021. [cit. 2023-03-17]. Dostupné z: https://msolutions.cz/2021/05/24/utoky-hrubou-silou-brute-force-a-jak-se-jim-branit/.

25. *Eliminace dětské kybernetické kriminality: sborník příspěvků z mezinárodní konference : Jihlava [11.-12.10.] 2012*. 1. vyd. Jihlava: Vyšší policejní škola Ministerstva vnitra v Jihlavě, 2012. ISBN 978-80-260-3492-6.

26. VRBASOVÁ, Lenka. *Ochrana před sociálním inženýrstvím*. 2017. Dostupné také z: https://theses.cz/id/nz86us/. Bachelor's thesis. Mendelova univerzita v Brně, Faculty of Business a Economics Brno. SUPERVISOR: Mgr. Tomáš Foltýnek, Ph.D.

27. MASARYKOVY UNIVERZITY, Kyberbezpečnostní tým. *Příběhy Technik Sociálního Inženýrství* [online]. [cit. 2023-03-21]. Dostupné z: https://security.muni.cz/socialni_inzenyrstvi.

28. *Jednotlivé druhy kyberkriminality* [online]. [cit. 2023-03-23]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx.

29. *Email: Nebezpečné odkazy* [online]. [cit. 2023-03-19]. Dostupné z: https://napoveda.seznam.cz/cz/email/nebezpecne-odkazy/.

30. *Co Je keylogger* [online]. [cit. 2023-03-17]. Dostupné z: https://www.sprava-site.eu/keylogger/.

31. *Formáty Open XML a přípony názvů souborů* [online]. [cit. 2023-04-04]. Dostupné z: https://support.microsoft.com/cs-cz/office/form%5C%C3%5C%A1ty-open-xml-a-p%5C%C5%5C%99%5C%C3%5C%ADpony-n%5C%C3%5C%A1zv%5C%C5%5C%AF-soubor%5C%C5%5C%AF-5200d93c-3449-4380-8e11-31ef14555b18.

32. *KOMUNIKAČNÍ APLIKACE S END-TO-END ŠIFROVÁNÍM: SOUČASNÝ TRH NABÍZÍ ŠIROKOU ŠKÁLU MOŽNOSTÍ, LIŠÍ SE KOMFORTEM, BEZPEČNOSTÍ A DŮVĚRYHODNOSTÍ PROVOZOVATELE* [online]. NÚKIB, 2022-03 [cit. 2023-04-04]. Dostupné z: https://www.nukib.cz/download/publikace/analyzy/Analza%5C%20komunikanch%5C%20aplikac_FINAL.pdf.

33. *Varování* [online]. [cit. 2023-04-04]. Dostupné z: https://www.nukib.cz/download/uredni_deska/2023-03-08_Varovani-TikTok_final.pdf. Číslo jednací: 2236/2023-NÚKIB-E/350.

34. VAŠÍČEK, Vladislav. *Historie školství od zavedení povinné školní docházky*. 2012. Dostupné také z: https://theses.cz/id/74mval/. Bakalářská práce. Univerzita Palackého v Olomouci, Filozofická fakulta Olomouc. SUPERVISOR: JUDr. Dalimila Gadasová, Dr.

35. DONÁT, Martin. *Klady a zápory implementace Rámcového vzdělávacího programu základního vzdělávání do školního vzdělávacího programu České republiky na prvním stupni základní školy*. 2016. Dostupné také z: https://theses.cz/id/thbmei/. Diplomová práce. Univerzita Palackého v Olomouci, Pedagogická fakulta Olomouc. SUPERVISOR: Mgr. Dominika Provázková Stolinská, Ph.D.

36. STUCHLÍKOVÁ, Iva; JANÍK, Tomáš; BENEŠ, Zdeněk; BÍLEK, Martin; BRÜCKNEROVÁ, Karla; ČERNOCHOVÁ, Miroslava; ČÍŽKOVÁ, Věra; ČTRNÁCTOVÁ, Hana; DVOŘÁK, Leoš; DYTRTOVÁ, Kateřina; GRACOVÁ, Blažena; HNÍK, Ondřej; KEKULE, Martina; ULIČNÁ, Klára; KUBIATKO, Milan; NEDĚLKA, Michal; NOVOTNÁ, Jarmila; PAPÁČEK, Miroslav; PETR, Jan; PÍŠOVÁ, Michaela; ŘEZNÍČKOVÁ, Dana; SLAVÍK, Jan; STANĚK, Antonín; ŠMEJKALOVÁ, Martina; TICHÁ, Marie; VALENTA, Josef; VANÍČEK, Jiří; VONDROVÁ, Naďa; ZÁVODSKÁ, Radka; ŽÁK, Vojtěch. *Oborové didaktiky: vývoj, stav, perspektivy*. 1. vydání. Brno: Masarykova univerzita, 2015. ISBN 978-80-210-7769-0. Dostupné také z: https://www.ped.muni.cz/didacticaviva/data_pdf/knihy/oborove-didaktiky_online.pdf.

37. MORKES, František. *Tereziánská reforma v českém školství* [online]. 2006. [cit. 2023-02-27]. Dostupné z: https://clanky.rvp.cz/clanek/c/z/827/terezianska-reforma-v-ceskem-skolstvi.html.

38. ÚSTAVODÁRNÉ NÁRODNÍ SHROMÁŽDĚNÍ REPUBLIKY ČESKOSLOVENSKÉ, 1946 - 1948. *95/1948 Sb. Zákon o základní úpravě jednotného školství (školský zákon)*. 1948.

39. NÁRODNÍ SHROMÁŽDĚNÍ, 1948 - 1954. *31/1953 Sb. Zákon o školské soustavě a vzdělávání učitelů (školský zákon)*. 1953.

40. NÁRODNÍ SHROMÁŽDĚNÍ ČESKOSLOVENSKÉ SOCIALISTICKÉ REPUBLIKY, 1960 - 1964. *186/1960 Sb. Zákon o soustavě výchovy a vzdělávání (školský zákon)*. 1960.

41. FEDERÁLNÍ SHROMÁŽDĚNÍ ČESKOSLOVENSKÉ SOCIALISTICKÉ REPUBLIKY, 1981 - 1986. *29/1984 Sb. Zákon o soustavě základních a středních škol (školský zákon)*. 1984.

42. *Rámcový vzdělávací program pro základní vzdělávání - 2005*. [B.r.]. Dostupné také z: https://www.npi.cz/images/RVP_ZV_2005.pdf.

43. *Rámcový vzdělávací program pro základní vzdělávání - 2017*. [B.r.]. Dostupné také z: https://www.npi.cz/images/RVP_ZV_2017.pdf.

44. *Rámcový vzdělávací program pro základní vzdělávání - 2021.* [B.r.]. Dostupné také z: https://revize.edu.cz/files/rvp-zv-2021.pdf.
45. *Nebezpečná TikTok výzva má v Česku možná první oběť. Jak se má boomer bránit?* [online]. Seznam, 2023-03 [cit. 2023-04-19]. Dostupné z: https://www.seznamzpravy.cz/clanek/domaci-zivot-v-cesku-nebezpecna-vyzva-na-tiktoku-ma-v-cesku-mozna-prvni-obet-jak-se-branit-227948?.
46. *About end-to-end encryption* [online]. [cit. 2023-04-29]. Dostupné z: https://faq.whatsapp.com/820124435853543.
47. *Jak na Instagramu zahájit chat opatřený koncovým šifrováním?* [online]. [cit. 2023-04-29]. Dostupné z: https://help.instagram.com/1165835007222763.
48. *FAQs* [online]. 2022-07. [cit. 2023-04-29]. Dostupné z: https://www.tiktokus.info/faqs/.
49. *ZŠ Písnická – O nás* [online]. [cit. 2023-03-19]. Dostupné z: https://www.zspisnicka.cz/.
50. *Osvěta NÚKIB* [online]. [cit. 2023-03-19]. Dostupné z: https://osveta.nukib.cz/local/dashboard/.
51. *02 Chytrá škola* [online]. [cit. 2023-03-19]. Dostupné z: https://o2chytraskola.cz/.
52. *Výuka| Bezpečně v síti.cz* [online]. [cit. 2023-03-19]. Dostupné z: https://bezpecnevsiti.cz/.
53. *Kraje pro bezpečný Internet: buďte o klik napřed* [online]. [cit. 2023-03-19]. Dostupné z: https://www.kpbi.cz/.
54. *Projekt E-bezpečí* [online]. [cit. 2023-03-19]. Dostupné z: https://www.e-bezpeci.cz/.
55. *Seriál Datová Lhota provede školáky virtuálním SVĚTEM* [online]. [cit. 2023-03-19]. Dostupné z: https://www.mff.cuni.cz/cs/verejnost/aktuality/serial-datova-lhota-provede-skolaky-virtualnim-svetem.
56. *Datová Lhota* [online]. [cit. 2023-03-19]. Dostupné z: https://decko.ceskatelevize.cz/datova-lhota.
57. *Úvodní informace* [online]. [cit. 2023-03-19]. Dostupné z: https://decko.ceskatelevize.cz/cms/datova-lhota/docs/uvodni-informace.pdf.
58. *Kybertest.cz: Buďte na internetu v bezpečí* [online]. [cit. 2023-03-19]. Dostupné z: https://www.kybertest.cz/.
59. *Internetoví úžasňáci* [online]. [cit. 2023-03-19]. Dostupné z: https://www.internetoviuzasnaci.org/.

# Obsah přiložených souborů

`dotaznikOdpovedi.xlsx` ..... Odpovědi dotazníkového šetření.