VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

ZÁKLADY BEZPEČNOSTNÍHO POVĚDOMÍ PRO ŽÁKY ZÁKLADNÍCH ŠKOL

BASICS OF SECURITY AWARENESS FOR PUPILS AT PRIMARY SCHOOL

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. Aleš Přibyl

AUTHOR

VEDOUCÍ PRÁCE — Ing. Petr Sedlák

SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Aleš Přibyl**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2019/20

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Základy bezpečnostního povědomí pro žáky základních škol

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem práce je vytvoření vzdělávacích modulů, které budou sloužit pro vybudování základního bezpečnostního povědomí v oblasti kybernetické a informační bezpečnosti pro žáky základních škol. Tyto vzdělávací moduly budou zaměřené především na aktivity, se kterými se děti v jednotlivých věkových skupinách setkávají, a na možná nebezpečí s nimi spojená.

Základní literární prameny:

ČSN ISO/IEC 27001, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnostiinformací - Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnostiinformací - Soubor postupů. Praha: Český normalizační institut, 2014.

DOUCEK, P., L. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

ONDRÁK, V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2019/20

V Brně dne 29.2.2020

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Tato diplomová práce se zabývá vybudováním vzdělávacích modulů, které budou sloužit pro vybudování základního povědomí o bezpečnosti pro děti na základních školách. Teoretická část popisuje základní informace z této oblasti. Další část popisuje zadání jednotlivých modulů a také popisuje školy, na kterých probíhala výuka. V praktické části jsou uvedeny podrobné náplně těchto vzdělávacích modulů.

Klíčová slova

budování bezpečnostního povědomí, informační a kybernetická bezpečnost, sociální sítě, heslo

Abstract

This diploma thesis looks at building educational modules that will serve to build a basic awareness of safety for children in primary schools. The theoretical part describes the basic information from this area. The next part describes the assignment of individual modules and also describes the schools where the teaching took place. The practical section contains detailed fillings of these education modules.

Key words

security awareness education, information and cyber security, social networking, password

Bibliografická citace

PŘIBYL, Aleš. *Základy bezpečnostního povědomí pro žáky základních škol* [online]. Brno, 2020 [cit. 2020-05-10]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/127748. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 15. května 2020

_____

podpis studenta

Poděkování

Touto cestou bych chtěl poděkovat vedoucímu práce Ing. Petru Sedlákovi a oponentce Ing. Janě Kolajové za jejich cenné rady a odborné připomínky, které mi udělovali během psaní diplomové práce.

OBSAH

ÚVOD

Informační a komunikační technologie jsou dnes neodmyslitelnou součástí naší civilizace. Už si prakticky bez nich nedokážeme život představit. Čím dál častěji s nimi přicházejí do styku nejmenší děti, které běžně umí používat například telefony, počítače, tablety a s jejich pomocí se pohybovat v prostředí internetu, pouštět si hry či videa. Kromě zábavy se využívají tyto technologie v pracovních prostředích. Z tohoto důvodu je nutné znát nejen výhody využívání ICT, ale znát také možné nevýhody, především ty, které ohrožují naši bezpečnost.

Společnost v minulosti viděla hlavně přínosy moderních technologií (například rychlost, pohodlnost, dostupnost nebo efektivitu) a neřešila se bezpečnost. To se v posledních letech mění. Podíl na tom nesou kybernetické útoky, které se odehrávají. Za zmínku stojí útoky na nemocnice z posledních měsíců (podzim 2019 – jaro 2020). Díky tomu se oblast informační a kybernetické bezpečnosti stává něčím, co vnímají všichni a začínají s tím pracovat. Podniky, organizace, úřady běžně zavádí programy pro budování informační a kybernetické bezpečnosti. Ovšem nesmíme zapomenout, že bezpečnostní povědomí by měli mít všichni uživatelé těchto technologií či služeb.

Budovat bezpečnostní povědomí se musí už od těch nejmenších. Také oni jsou zapojeni do kyberprostoru, který jim současný svět nabízí, ba dokonce je někdy přímo nutí k jeho využívání. Díky tomu by se v této oblasti měly vzdělávat už děti navštěvující základní školy, které jsou mnohdy nejzranitelnější skupinou. Oblast bezpečnosti neznamená pouze ochranu před hackerskými útoky, ale také ochranu sebe sama v prostředí internetu. Právě ta je v dnešní době, kdy narůstá počet obětí kyberšikany nebo dalších jiných forem nevhodného chování, velmi důležitá. Téma zneužívání dětí na internetu je další oblastí, o které se na veřejnosti začíná hodně diskutovat a nutí vnímat důležitost problematiky týkající se kyberbezpečnosti.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

V této diplomové práci se budu zabývat vybudováním základního bezpečnostního povědomí pro žáky základní školy. Cílem je vytvořit jednotlivé moduly zaměřené především na oblasti, které se nejvíce týkají dětí v daném věku. Tyto výukové moduly budou v rámci práce také odučeny na vybraných školách.

Práce je rozdělena do tří částí. První bude obsahovat základní teoretické informace z oblasti informační a kybernetické bezpečnosti, ze kterých budu vycházet při tvorbě jednotlivých modulů. Tyto poznatky jsou nezbytné pro pochopení návrhu řešení.

V analytické části bude popsán smysl tohoto programu. Dále zde bude uvedeno rozdělení tříd do jednotlivých skupin. Pro každou skupinu bude individuální zadání, které je přizpůsobené chápání dětí, a především aktivitám, se kterými se nejčastěji setkávají.

Poslední část se bude věnovat jednotlivým modulům, jejich detailní náplni i tomu, jak by měla taková výuka probíhat. Výstup práce by neměl sloužit pouze pro vybrané školy, ale výukové moduly by mohly být použitelné pro všechny typy základních škol, které by chtěly u svých dětí vybudovat alespoň základy bezpečnostního povědomí v oblasti kybernetické a informační bezpečnosti.

1 TEORETICKÁ VÝCHODISKA

V kapitole si představíme základní pojmy z oblasti kybernetické a informační bezpečnosti a další teoretické znalosti, ze kterých budeme vycházet pro část vlastní návrhy. Tato část práce je nezbytná pro správné pochopení obsahu vyučovacích modulů.

1.1 Základní pojmy

Aktiva – všechny hmotné i nehmotné zdroje (HW, SW, služby, informace), které mají hodnotu a mají být chráněny pomocí bezpečnostních opatření (1, s. 346).

Antivirový program – základ celé informační bezpečnosti, chrání všechny vstupní body do systému. Ochraňuje nás před škodlivými kódy, které se mohou do počítače dostat různými způsoby, nejčastěji pomocí elektronické pošty nebo navštívených internetových stránek (1, s. 112).

Data – popisují reálný svět formou vhodnou ke zpracování, vyhodnocování nebo komunikaci. Data vytváří informaci (1, s. 12).

GDPR – evropské nařízení o ochraně osobních údajů, které má zvyšovat ochranu těchto údajů. Týká se firem, institucí i jednotlivců (2).

Hardware – hmotné technické vybavení počítače, které je potřebné pro správnou funkci systému. Hardware můžeme rozdělit na: **vnitřní technické vybavení**, bez kterých by počítač nefungoval (základní deska, procesor, napájecí zdroj, a další) a **periferie**, které usnadňují nebo rozšiřují možnosti využívání počítače (monitor, klávesnice, ...) (3, s. 59).

Heslo – tajný řetězec znaků, který slouží pro ověření uživatele (autentizaci). Zvolí si ho každý uživatel sám podle stanovených pravidel. Heslo by mělo být dostatečně složité, aby nemohlo dojít k jeho snadnému uhádnutí (4).

Hrozba – potencionální událost, síla, aktivita nebo osoba, která může způsobit škodu (1, s. 348).

Informace – data, která mají vlastní specifikaci a organizaci za účelem prezentace v takovém kontextu, který dává příjemci smysl a význam (5).

Informační bezpečnost – ochranu informací ve všech formách v celé organizaci. Zahrnuje ochranu informací z pohledu zachování integrity (správnosti a úplnosti informací), dostupnosti (přístup k informacím v požadovaný čas) a důvěrnosti (přístup pouze oprávněným uživatelům) (6).

Internet – globální systém navzájem propojených počítačových sítí, které spojují jednotlivé počítače pomocí síťových prvků. Komunikace probíhá pomocí protokolů TCP/IP, které zajišťují, aby komunikace probíhala mezi správnými počítači bez chyb. Internet neznamená pouze www stránky nebo email, jak se část lidí domnívá, to jsou pouze služby, které lze díky internetu používat (7).

Kyberprostor – virtuální svět, který nemá začátek ani konec. Kyberprostor je nehmotné médium, které je tvořeno hmotnými prvky (počítače, IS, síťové prvky, úložiště, …). Vzniká tak digitální svět, který vytvářejí informační a komunikační technologie. Mezi znaky kyberprostoru patří otevřenost, bohatost na informace (včetně nepravdivých informací) nebo globálnost. V tomto virtuálním světě nebudou fungovat pravidla, která známe z reálného světa. Ovšem projevy z kyberprostoru mají velký dopad na reálný svět, což se v posledních letech projevuje čím dál častěji (3, s. 42-48).

Osobní údaj – veškeré informace o identifikované nebo identifikovatelné fyzické osobě (subjekt údajů). Jednat se může o údaje, které mohou identifikovat určitou osobu pomocí identifikátoru (např.: jméno, rodné číslo, identifikační číslo) nebo na základě jednoho či více zvláštních prvků dané osoby, např.: fyzické, fyziologické, kulturní, ekonomické (2).

Opatření – aktivita, která je navržena tak, aby snížila zranitelnost, dopad hrozby nebo její působení. Pomocí přijatých opatření zvyšujeme bezpečnost (1, s. 347).

Patch – označení pro záplaty, jedná se o opravy nebo pravidelné aktualizace používaného softwaru (1, s. 350).

Riziko – stupeň ohrožení aktiva, že se uplatní hrozba a dojde k nežádoucímu výsledku. Můžeme charakterizovat jako pravděpodobnost, že dojde k ohrožení aktiva v kombinaci s dopadem (škodou, kterou způsobí hrozba svým působením) (1, s. 347–351).

Software – programové či netechnické vybavení počítače. Jedná se například o operační systémy nebo veškeré aplikace od jednoduchých až po komplexní programové systémy (3, s. 63).

Zranitelnost – slabé místo aktiva, které by mohlo být zneužito jednou nebo více hrozbami (1, s. 16).

1.2 Počítačové viry a škodlivé kódy

V této části si rozebereme základní pojmy, které se používají v oblasti počítačových virů a které se také často objevují v médiích. Nejprve si rozdělíme škodlivé kódy podle šíření, dále si pak uvedeme základní druhy škodlivých kódů.

1.2.1 Škodlivé kódy podle šíření

Počítačový virus – pro své šíření používá jiné soubory, do kterých je vkládán, a tak infikuje další systémy. K tomu se využívají spustitelné soubory (s koncovkou exe, com, …) nebo různé dokumenty (doc, xls a mnoho dalších) (8).

Počítačový červ – od viru se liší tím, jak se šíří. Replikuje se sám od sebe, nepotřebuje k tomu žádný soubor. Zpravidla se šíří prostřednictvím počítačových služeb. Často ke svému šíření využívají chyby v programech a systémech (8).

Trojský kůň – nejsofistikovanější skupina škodlivého softwaru, která se vydává za užitečný program. Dostane se tak do počítače legálním způsobem. Ovšem má v sobě část kódu, která plní i jiné funkce a umožňuje útočníkovi ovládat počítač, získávat data z počítače nebo hesla. Trojské koně se většinou nesnaží o samovolné šíření (8).

1.2.2 Malware

Název pochází ze složení dvou anglických slov, **mal**icious = škodlivý a soft**ware,** tedy škodlivý software. Malware je souhrnné označení pro všechny typy škodlivých kódů, které mají za úkol infikovat systém a tam provést nežádoucí akce, např. odstranit data, sledovat uživatele nebo ho obtěžovat (9).

1.2.3 Adware

Název pochází z anglických slov **ad**vertising support soft**ware** (software podporující reklamy). Adware jsou programy podporující reklamu. Tato forma malwaru není sama o sobě nebezpečná, ale je spíše obtěžující. Jedná se o zobrazování reklamy například v aplikacích či webových stránkách. Nebezpečným se adware může stát se spojením s jiným druhem škodlivého kódu (3, s. 205-206).

Obrázek č. 1: Adware – ukázka (Zdroj: 3, s. 207)

1.2.4 Keylogger

Jak název napovídá, **key**stroke = stisknutí klávesy a **logger** = zapisovač, jedná se o software zaznamenávající stisky jednotlivých kláves na infikovaném počítači. Nejčastěji se využívá k získání přihlašovacích údajů, které následně odesílá útočníkovi (3, s. 210).

1.2.5 Ransomware

Název odvozený z anglických slov **ransom** = výkupné a soft**ware**, jedná se o vyděračský software, který brání či omezuje oběti útoku v normálním využívání počítačového systému do doby, než bude zaplaceno požadované výkupné. Nejčastěji se šíří jako malware, který je součástí přílohy e-mailu nebo je umístěn na webových stránkách. Při jeho stažení se bezpečně usídlí do počítačového systému a stáhne vlastní ransomware. Ten pak buď omezí funkčnost celého systému nebo nechá počítačový systém funkční, ale zamezí pouze v přístupu k datům. Zaplacení výkupného se většinou požaduje ve virtuální měně, například v Bitcoinu (3, s. 221-231).

1.2.6 Spyware

Jak název vypovídá, z anglických slov **spy** = špion a soft**ware**, jde o špionážní software, který bez souhlasu uživatele odesílá data z provozu počítačového systému k útočníkovi. Jednat se může například i o osobní data, informace o navštívených webových stránkách apod. Často je spyware součástí balíčků programů. Šířit se může i jako součást volně šiřitelných programů, kdy ve smluvních podmínkách uživatel dobrovolně souhlasí s monitorováním vlastních aktivit. Kromě odesílání dat útočníkovi může být spyware nebezpečný i tím, že jeho součástí mohou být i další funkce, které mohou ovlivňovat činnost uživatele (3, s. 207).

1.2.7 Botnet

Nejedná se o škodlivý kód, nýbrž o způsob využívání cizích zařízení k nevědomé činnosti. Funguje tak, že se infikuje velký počet zařízení, které jsou pomocí softwaru propojeny do velké sítě. Tato síť má vlastního správce, který vydává všem infikovaným počítačům zapojených do jeho sítě příkazy. Jednat se může i o legální činnost, například pro distribuované výpočty. Využívá se však i k nelegálním činnostem, například odesílání spamu, DDoS útoky a mnoho dalších způsobů využití (3, s. 193-202).

DDoS útoky – při útoku dochází k zahlcení počítačového systému z důvodu, že na něj přichází spoustu paketu z jiných systémů. Napadený systém se zahltí a dojde k výpadku (3, s. 296).

1.3 Rizikové chování v on-line prostředí

Kapitola představí rizikové chování spojené s využíváním internetu dětmi, především sociálních sítí.

1.3.1 Kyberšikana

Pod pojmem šikana si můžeme představit ubližování, vysmívání se, zesměšňování, krádeže, vysypávání a rozhazování věcí a další formy neustálého obtěžování. Aby se jednalo o šikanu, musí se ubližování opakovat. O kyberšikanu se jedná, dějí-li se tyto věci v kyberprostoru (10).

Jinými slovy, pro kyberšikanu se využívají ICT technologie nebo služby, které nabízí kyberprostor. O kyberšikanu se může také jednat, bude-li někdo nahrávat „klasickou“ šikanu, např. fyzické ubližování, a pak taková videa bude sdílet na webových stránkách (3, s. 309).

Mezi znaky kyberšikany můžeme zařadit:

- **Pocit anonymity** – útočník si myslí, že na internetu může být anonymní
- **Neomezenost útoku** – útočník může oběť šikanovat kdykoliv a kdekoliv, nezáleží na místě, kde se nachází. Vzdálenost mezi útočníkem a obětí může být neomezená. Kyberšikana často vyžaduje menší úsilí než fyzická šikana
- **Neomezený okruh účastníků** – v digitálním prostředí nezáleží na věku, síle či postavení ve skupině. Agresor nebo oběť může být kdokoli
- **Obtížná zjistitelnost** – kyberšikana nemusí mít vnější projevy, např. modřiny, odřeniny, chybějící věci a další viditelné známky (3, s. 309-312).

Kyberšikanu můžeme dělit na:

- **Přímá** – útočník atakuje oběť sám
- **Nepřímá** – útočník využívá další osobu, kterou zmanipuluje a nabádá, aby šikanovala oběť místo něho (11).

Formy kyberšikany mohou být:

- Publikování ponižujících videí nebo fotografií
- Obtěžování, ponižování nebo pomlouvání (na webových stránkách i v uzavřených skupinách)
- Krádež identity a vytváření falešných profilů
- Natáčení fyzických útoků – Happy slapping
- Provokování a napadání při online komunikaci – veřejné (např.: komentáře u příspěvků) i neveřejné (např.: chat)
- Neustálé sledování nebo kontaktování – viz. kyberstalking (11).

1.3.2 Kyberstalking

Jedná se o nebezpečné pronásledování. Útočník využívá informační a komunikační technologie k tomu, aby získal o své oběti co nejvíce informací nebo jejich pomocí prováděl útoky na oběť. Získané informace využívá k tomu, aby se snažil svou oběť dlouhodobě a opakovaně kontaktovat, vyhrožovat jí nebo ji nějak poškodit před rodinou, přáteli nebo kolegy. V rámci kyberstalkingu útočníci mohou vyhledávat svou oběť na internetu, tudíž ji osobně nemusejí znát. Stalkeři mohou být bývalí partneři, uctívači (touží po vztahu s osobou, která je zaujala, např.: celebrity, spolupracovníci), sexuální útočníci nebo jedinci, které uspokojuje pocit moci nad jinou osobou (12).

1.3.3 Kybergrooming

Kybergrooming je typ chování, kdy se dospělá osoba snaží manipulovat s dítětem. Útočník (kybergroomer) ke svému útoku využívá většinou falešnou identitu. Nejdřív se snaží o navázání kontaktu a získání důvěry, poté se se pokouší vylákat oběť na osobní schůzku, kde může dojít k pokusu o fyzický, sexuální nebo jakýkoli jiný útok. Nejčastějšími oběťmi kybergroomingu jsou dívky ve věku 11 až 17 let (13).

Nejčastější postup kybergroomingu:

- Navázání kontaktu a získání co nejvíce informací
- Izolování dítěte od rodiny
- Uplácení formou malých dárků
- Emoční závislost
- Zneužití nebo jiný útok (13).

Nejčastější typy obětí jsou:

- *„Děti s nízkou sebeúctou nebo nedostatkem sebedůvěry (lze je snadněji citově či fyzicky izolovat)*
- *Děti s emocionálními problémy, oběti v nouzi (často hledají náhradu za své rodiče a potřebují pomocnou ruku)*
- *Děti naivní a přehnaně důvěřivé (jsou ochotnější zapojit se do online konverzace s neznámými lidmi, obtížněji rozpoznávají rizikovou komunikaci)*
- *Adolescenti/teenageři (zajímá je lidská sexualita, jsou ochotni o ní hovořit)“* (12).

1.3.4 Sexting

Z názvu je patrné, že se jedná o posílání zpráv se sexuálním obsahem. Nemusí se jednat pouze o text, ale i fotografie nebo videa. Nejčastěji tyto materiály pořizují samotní odesílatelé. Po ukončení komunikace nebo vztahu jeden z účastníků tyto zprávy zneužívá. Útočník, který má takové materiály k dispozici, může chtít po své oběti další zprávy, osobní setkání nebo může mít další požadavky. K tomu může využívat vyhrožování, že již dostupné materiály bude sdílet na webových stránkách nebo pošle

rodině či přátelům oběti. Často k vydírání dochází i mezi partnery po ukončení vztahu, během kterého došlo k posílání takových zpráv. Další ohroženou skupinou jsou i děti druhého stupně ZŠ, protože jsou ve věku, ve kterém je oblast sexuality zajímá (3, s. 314-316).

1.3.5 On-line výzvy

On-line výzvy vyzývají uživatele k provádění různých činností. Ty mohou být pozitivní nebo negativní. Největší podíl na jejich šíření mají sociální sítě (14).

Pozitivní výzvy – jsou takové, které mohou prospět dobré věcí, například výzvy mající charitativní nebo ekologický rozměr. Pozitivní výzvy nejsou škodlivé účastníkům ani okolí (14).

Negativní výzvy – jsou především pro děti a dospívající velmi lákavé, protože nabízejí dostatek adrenalinu, větší ohlas nebo sdílení na sociálních sítí. Z toho důvodu se rychleji šíří a dostanou se mezi větší množství uživatelů. Negativní výzvy můžeme označit také jako rizikové, patří mezi ně ty, které nabádají různou formou k sebepoškozování (ať už způsobováním bolesti, polykáním nebo vdechováním předmětů, koření a dalších), ubližování druhým nebo poškozování cizího majetku (14).

1.3.6 Falešné profily

Důležité při pohybu na internetu, především na sociálních sítích, je vnímání rizika falešných profilů. Jejich vytvoření je velice jednoduché. Mnoho podvodníků se nebojí takové účty vytvářet a používat. Falešné účty pak slouží například k urážení, pomlouvání, navazování kontaktů, získávání důležitých informací, rozesílání nevyžádaných zpráv, šíření nepravdivých informací, ale i ke kyberšikaně, kyberstalkingu nebo kybergroomingu (15).

K riziku falešných profilů můžeme zařadit také klonování profilů. Takové chování vychází z ukradení fotografií, jména, případně dalších informací o určité osobě. Na tuto osobu pak útočník vytvoří falešný účet, který je k nerozeznání od pravého profilu.

V podstatě se útočník vydává za někoho cizího, využívá jeho identitu ke své činnosti (15).

1.3.7 Krádež identity

Identity theft je forma útoku, kdy útočník odcizí oběti virtuální identitu (profil). Odcizení probíhá nejdřív prolomením nebo získáním hesla k účtu. Tento účet pak útočník využívá k vlastním účelům, podobně jako při falešných profilech. Nejedná se o vytváření nového účtu, ale o krádež cizího profilu (3, s. 318-319).

1.4 Další projevy nevhodného chování

V kapitole o dalších projevech nevhodného chování si představíme formy využívání upravených nebo falešných informací. Ujasníme pojmy, které se používají v souvislosti se šířením nevyžádaných zpráv.

1.4.1 Spam

Jedná se o zasílání nevyžádaných zpráv. Spam můžeme rozdělit do dvou oblastí podle významu, který si pod pojmem lze představit. V užším smyslu se jedná o reklamní sdělení, které se šíří pomocí elektronické komunikace. V širším smyslu se jedná o jakékoliv nevyžádané zprávy, tedy i o zprávy obsahující škodlivý kód (3, s. 231).

Obrázek č. 2: Rozdělení spamu (Zdroj: 3, s. 232)

Pro zasílání nevyžádaných zpráv se nejčastěji používají různé komunikační nástroje, např. e-mail, SMS, MMS, messenger, sociální sítě, diskusní fóra apod. Tyto nevyžádané zprávy mohou obsahovat reklamní nebo obchodní sdělení, informace o zdraví či medicíně (různé zázračné přípravky), finanční nabídky, vzdělávací nabídky různých kurzů nebo politické či náboženské informace (3, s. 231-235).

Nebezpečnější formou spamu jsou zprávy obsahující škodlivý kód, odkaz na podvržené stránky nebo podvodné nabídky. Tyto nevyžádané zprávy spadají do skupiny, které mají kriminální nebo podvodný obsah a nesou vlastní označení scam, z anglického slova scam, které se překládá jako podvod, podraz (3, s. 231-235).

1.4.2 Hoax

Hoax vychází z anglického slova hoax, které se překládá jako falešná nebo klamná zpráva, úmyslná mystifikace či novinářská kachna. Jak název napovídá, jedná se o spamy, ve kterých se objevuje klamavá, nepravdivá nebo falešná informace (3, s. 240).

Šíří se pro zábavu nebo pro vyvolání falešného pocitu nebezpečí. Častým jevem hoaxu je, že se v nich objevují názory osobností nebo fotografie, které jsou buď upravené nebo vytržené z kontextu. Mnohdy se snaží vyvolat dojem, že článek je založen na tvrzení smýšlených odborníků. Často obsahují výzvu k dalšímu šíření z důvodů, že média, vlády, výrobci nebo jiné skupiny tuto událost tají. Hoaxy provázejí lidstvo po celou historii, ovšem internet jejich šíření usnadnil a urychlil. Další významný vliv na šíření těchto zpráv mají sociální sítě, kde se tyto ne zcela pravdivé informace objevují hojně. Hoaxy jsou také někdy úmyslně vytvářeny a šířeny za účelem propagandy, např. politické strany (16, s. 141-151).

Charakteristické rysy hoaxu můžeme shrnout na:

- emotivní téma případně dramatický popis události
- poutavý titulek, který má za cíl okamžitě upoutat čtenáře
- princip autority – využívání a zneužívání odborníků nebo známých osobností
- výzva k šíření (16, s. 141-151).

Proč hoaxům stále lidé věří se dá popsat tím, že nehledáme co nejpřesnější pravdu, ale spoléháme se na intuici. Nehledáme co nejvíc informací, ale snažíme se co nejrychleji rozhodnout, abychom nemuseli moc přemýšlet. Tato rozhodnutí jsou ovlivněna tím, jaké máme a jaké v nás článek vyvolává emoce. Proto je důležité se vždy krátce zamyslet a případně si ověřit informace. Pokud tyto úkony nebudeme dělat, necháme se pohltit emocemi, které článek vyvolává a sklouzneme ke stereotypnímu vidění světa (za vše špatné může EU, každý muslim je terorista atp. (16, s. 143-145).

Snadno jim také uvěříme díky tomu, že selektivně vybíráme fakta, která jsou v souznění s našimi názory. Takže pokud v sobě máme nějaké přesvědčení, snadněji uvěříme falešným zprávám, které s našimi již dříve vytvořenými názory korespondují (16, s. 143-145).

1.4.3 Phishing

Phishing je způsob podvodného jednání, které má za úkol získat informace o oběti, na kterou je prováděn útok. Jedná se například o přihlašovací údaje (jméno, heslo), čísla kreditních karet, osobní informace atd. Tyto zprávy se často rozesílají velkému množství uživatelů internetu. Nejčastěji se jedná o zprávy, které obsahují odkaz na podvržené webové stránky. Tyto stránky jsou velice podobné těm skutečným a liší se hlavně adresou, případně stránky obsahují různé formuláře pro vyplnění požadovaných údajů (3, s. 246).

Za phishing se označuje také zpráva odkazující na podržené stránky, ze kterých dojde ke stažení malwaru. Tento škodlivý kód si sám získá informace, bez vědomí a interakce uživatele (3, s. 248).

1.4.4 Fake news

Fake news jsou lživé, klamavé, falešné informace, které se šíří prostřednictvím médií a sociálních sítí. Tyto informace jsou vypouštěny do světa zcela úmyslně a většinou jsou úmyslně také sdíleny. Účelem fake news je dosáhnout zisku. Nemusí se jednat o finanční zisk, ale třeba o politický. Do fake news nepatří satira ani parodie (16, s. 18).

1.5 Anonymita uživatele

Uživatelé se často mylně domnívají, že v prostředí kyberprostoru jsou anonymní. To proto, že veškeré systémy, aplikace nebo webové služby shromažďují o uživatelích velké množství informací. A to i ty, které nepotřebují ke svému fungování. Mezi shromažďované informace můžeme zařadit nejen osobní údaje (jméno, příjmení, e-mail, adresa, telefonní číslo apod), ale i například lokalizační údaje (GPS souřadnice, informace o bezdrátovém připojení, …), případně informace o OS, verzi aplikace, cookies a různé další informace. Shromažďované informace můžou být využívány například k lepšímu cílení reklam, nabídkám dalších služeb a v nejhorším případě se tato data mohou stát komoditou, se kterou se obchoduje (3, s. 132-133).

1.5.1 Digitální stopa

S anonymitou také souvisí digitální stopa. Digitální stopa je otisk, který za sebou každý uživatel zanechává na internetu. Tyto stopy můžeme rozdělit na ovlivnitelnou a neovlivnitelnou (3, s. 135).

Obrázek č. 3: Digitální stopa (Zdroj: 17)

Ovlivnitelná (aktivní) digitální stopa – uživatelé ji zanechávají vlastním přičiněním. Jedná se o informace, které dobrovolně poskytujeme (příspěvky, fotografie, videa, texty zpráv, osobní informace apod). Tyto stopy můžeme snadno ovlivnit tím, jaké informace o sobě sdílíme. Nejvíce ovlivnitelných stop za sebou uživatelé zanechávají na sociálních sítích (3, s. 134-145).

Neovlivnitelná (pasivní) digitální stopa – nezanechávají jí uživatelé vědomě, ale vznikají komunikací mezi systémy nebo na základě funkčnosti systémů a aplikací. Jedná se například o historii vyhledávání na internetu, IP adresa, informace o poskytovali, cookies (soubory, které si do počítače vkládají navštívené webové stránky, např. údaje o nastavení). Tyto stopy lze hůře ovlivnit (3, s. 135-144).

Pokud se budeme pohybovat ve světě ICT, můžeme si zapamatovat jedno pravidlo: *„pokud kdykoliv cokoliv nahrajete, přenesete, zprostředkujete, vložíte do kyberprostoru, zůstane to tam navždy“* (3, s. 135).

1.6 Sociální sítě

Sociální síť je služba na internetu, která umožňuje uživatelům vytvářet vlastní profily, sdílet obsah s ostatními uživateli, diskutovat, komunikovat a provádět další aktivity. Obsah, který na těchto sítích uživatelé sdílí je buď veřejně dostupný všem, kteří danou službu využívají nebo dostupný jen vybraným uživatelům. Díky obrovské popularitě vznikají nové sítě, které se snaží napodobit úspěch některých významných předchůdců, např. Facebooku, YouTube. Sociální sítě nepoužívají jen fyzické osoby, ale také firmy, pro které se tyto služby staly nástrojem marketingu (18, s. 24-26).

Sociální sítě můžeme rozdělit na české a mezinárodní.

1.6.1 České sociální sítě

Tyto služby jsou zaregistrované na území ČR. Mezi dětmi a mládeží zdaleka nedosahují takové popularity, jako je tomu u velkých mezinárodní služeb. Mezi české sociální sítě patří například libimseti.cz, stěsti.cz (18, s. 24-26).

Známější jsou v těchto věkových skupinách následující příklady:

- Lidé.cz – největší česká sociální síť, která se zaměřuje na uživatelské profily, diskusní fóra a soukromé chaty
- ČSFD.cz – zaměřuje se na filmové fanoušky (18, s. 24-26).

1.6.2 Mezinárodní sociální sítě

Mezi rizika těchto sítí musíme zařadit, že se případné problémy řídí právem a zvyklostmi státu, ve kterém jsou služby registrovány. Tyto sítě jsou rozšířené po celém světě, dokonce v ČR jsou mnohem populárnější než české služby (18, s. 24-26).

Krátce si představíme nejrozšířenější sociální sítě, které využívají žáci základních škol:

Facebook – nejpoužívanější síť podle počtu uživatel. Vznikla jako studentský projekt, který se velmi rychle rozšířil do celého světa. Nabízí sdílení obsahu, komunikační nástroje, vytváření zájmových skupin, a také se využívá jako reklamní nástroj. Denně se v průměru nahraje na Facebook přes 200 milionů fotografií (18, s. 25-26).

Instagram – služba poskytující prostor pro sdílení fotografií nebo videí (18, s. 25-26).

YouTube – hlavně mezi mladšími ročníky nejpoužívanější služba na internetu. Poskytuje prostor pro nahrávání a přehrávání videí. Tato videa lze také komentovat, případně tvořit vlastní playlisty. Na tuto síť přistoupí denně přes dvě miliardy uživatelů (18, s. 24-26).

TikTok – dříve se tato sociální síť jmenovala Musical.ly, od roku 2017 nese jméno TikTok. Jedná se o službu, která je cílená především na děti. Síť slouží pro nahrávání krátkých videí, která lze sdílet, komentovat, lajkovat. Síť si získává stále více a více uživatelů nejen ve světě, ale i v ČR. V naší republice používá TikTok zhruba 28 % dětí ve věkové skupině 10–12 let. Na této sociální síti je velké množství nevhodných videí, která obsahují sexuální tématiku. Přes TikTok se také šíří velké množství výzev. Stejně jako na dalších sítích dochází i zde ke kyberšikaně a k dalším nevhodným typům chování, které jsou popisovány dříve. Tato síť s sebou nese jedno velké nebezpečí, a to takové, že ve výchozím nastavení jsou účty veřejné a veškerý obsah je přístupný všem uživatelům (19).

Obrázek č. 4: Logo TikToku (Zdroj: 19)

Mezi další známé sociální sítě patří Twitter (umožňuje sdílení krátkých zpráv), LinkedIn (profesní síť, umožňuje vkládání životopisu), Facebook Messenger, Snapchat, WhatsApp, Pinterest, Viber, Google+, Spoti.fy, Skype a mnoho dalších

1.7 Autorská práva

Všechna díla, ať už umělecká, vědecká nebo jiná (včetně softwarů) jsou chráněna právy, která jsou dána v autorském zákonu, zákon č. 121/2000 Sb. V této práci nebudeme rozebírat celý zákon, ale zaměříme se pouze na základy, které z něho vychází a měl by je znát každý uživatel internetu. Autorský zákon nezakazuje stahovat z internetu písničky nebo filmy pro osobní účely. Ale zakazuje tato díla šířit. Dále se mohou v odůvodněné míře používat výňatky z cizích děl ve vlastní tvorbě. Také je povoleno používat díla při výuce nebo k neziskovým vědeckým účelům. V oblasti počítačových programů však volné stahování pro vlastní účely neplatí. Programy jsou ovšem opatřeny licencí, která definuje, jak s programem můžeme nakládat (20).

1.8 Normy a standardy

Norma – je pouze doporučení jak by proces, služba, výrobek apod. měl vypadat (1, s. 40).

- **normy ČSN** – označení pro české technické normy. Ty vznikají buď podle národních požadavků a potřeb nebo jsou přejímány od jiných normalizačních institutů (označují se pak jako ČSN IEC, ČSN ISO, ČEN EN apod.)

- **ISO** – International Organization for Standardization, posláním je podporovat rozvoj standardů pro usnadnění mezinárodních směn zboží a služeb a na spolupráci v intelektuálních, vědeckých, technických a ekonomických aktivitách
- **IEC** – International Electronical Comission – celosvětová organizace vydávající normy z oblasti elektrotechnických, komunikačních a jim příbuzných oblastech (1, s. 41-44).

Normy řady 27 K

Normy z této oblasti se zabývají oblastí informační bezpečnosti.

- ČSN ISO/IEC 27000: Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti – Přehled a slovník
- ČSN ISO/IEC 27001: Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti – Požadavky
- ČSN ISO/IEC 27002: Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti – Soubor postupů
- ČSN ISO/IEC 27003: Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací
- ČSN ISO/IEC 27004: Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Měření
- ČSN ISO/IEC 27005: Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací
- ČSN ISO/IEC 27006: Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací (1, s. 48-51).

Standard – je dokument, který vznikl společnou úmluvou. Obsahuje technická, specifická nebo jiné pevně stanovená kritéria. Standardy zajišťují, že materiály, výrobky, procesy apod. jsou přesně takové, jaké měly být. Např.: formát telefonních nebo kreditních karet, komunikační protokol (1, s. 40).

1.8.1 NIST standardy

National Institute for Standards and Technology je americký vládní standardizační orgán, který se zabývá oblasti vývoje a podpory standardů měřících technik a technologií s účelem zvýšit produktivitu, usnadnit obchod a zlepši život (1, s. 45).

V této diplomové práci jsou využívány následující standardy NIST:

NIST SP 800-16 – poskytuje požadavky a koncepční rámec pro školení v oblasti bezpečnosti ICT. Zmíněné požadavky jsou vhodné pro výpočetní prostředí. Rámec poskytuje možnost rozšíření pro budoucí využívání nových technologií (21).

NIST SP 800-50 – slouží pro vybudování vzdělávacího programu pro zvyšování bezpečnostního povědomí. V rámci standardu je definovaný návod, jak program vybudovat. Popisuje návrh a rozvoj programu, implementaci i post-implementační část. S předchozí směrnicí se navzájem doplňují (22).

NIST SP 800-63B – obsahuje standardy pro autentizaci a správu identity. Pro tuto práci je důležitá část, která se věnuje politice hesel, kde definuje požadavky, jak by hesla měla vypadat (4).

1.9 Program SAE

Program Security Awareness Education (SAE) slouží pro zvyšování bezpečnostního povědomí. Aby byl program úspěšný, musí se skládat z následujících kroků (22).

- budovat politiky informační bezpečnosti
- informovat uživatele o jeho odpovědnosti
- určit kroky pro monitoring a přezkoumávání programu (22).

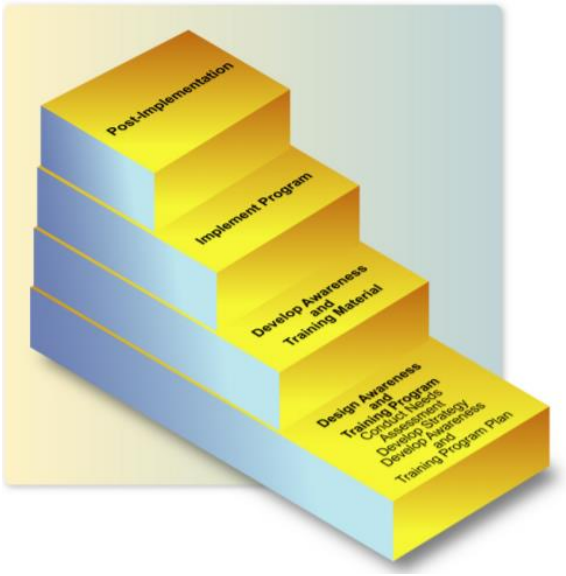
Jako každý program, tak i budování bezpečnostního povědomí musí mít určené role a odpovědnosti (aby bylo jasné, kdo má co na starosti a kdo za dané části odpovídá). Dále musíme uživatele rozdělit do skupin a pro každou skupinu stanovit cíle, kterých má být dosaženo v rámci programu. Skupiny budou rozděleny především podle pozice, kterou daný účastník v organizaci zastává. Pro každou skupinu musí být vytvořené vzdělávací

materiály. Nezbytnou součástí programu je také dokumentace a kalkulace nákladů. Posledním krokem v programu SAE je post-implementační část, ve které dochází k získání zpětné vazby, a hlavně k vyhodnocení programu, jestli splnil očekávané cíle (22).

1.9.1 Klíčové kroky programu SAE

Program SAE můžeme rozdělit do následujících kroků:

- navrhnout program
- vytvořit školící a podpůrné materiály
- implementace programu
- post-implementační část (22)



Obrázek č. 5: Kroky programu SAE (Zdroj: 22)

První část můžeme označit za nejdůležitější. Dochází v ní k návrhu programu. Tento návrh musí být v souladu s požadavky organizace a jejími možnostmi. Musí být stanoven plán, cíle a náklady programu bezpečnostního povědomí. Dochází také k rozdělení uživatelů do jednotlivých skupin. V druhé části programu dochází k vytvoření školících a podpůrných materiálů pro jednotlivé skupiny dle jejich potřeb a požadavků. V poslední části dochází k samotné implementaci programu. Po realizaci můžeme přidat již zmiňovanou poslední post-implementační část (22).

1.9.2 Modely programu SAE

Program SAE má tři základní modely. Výběr konkrétního modelu závisí na faktorech jako velikost dané organizace, geografickém rozmístění a organizační struktuře, ze které vychází definice rolí a odpovědnosti (22).

Centralizovaný model – veškerá odpovědnost za program budování bezpečnostního povědomí připadá pověřené osobě. Tento model je vhodný pro malé organizace, kde mají vysoký stupeň centrálního řízení (22).

Částečně decentralizovaný model – odpovědnost za vytvoření politik i strategie je na odpovědné osobě. Samotná implementace je distribuována na další uživatele. Tento model je vhodný pro středně velké podniky, které mají široké geografické rozmístění poboček, případně pro organizace s decentralizovanou organizační strukturou (22).

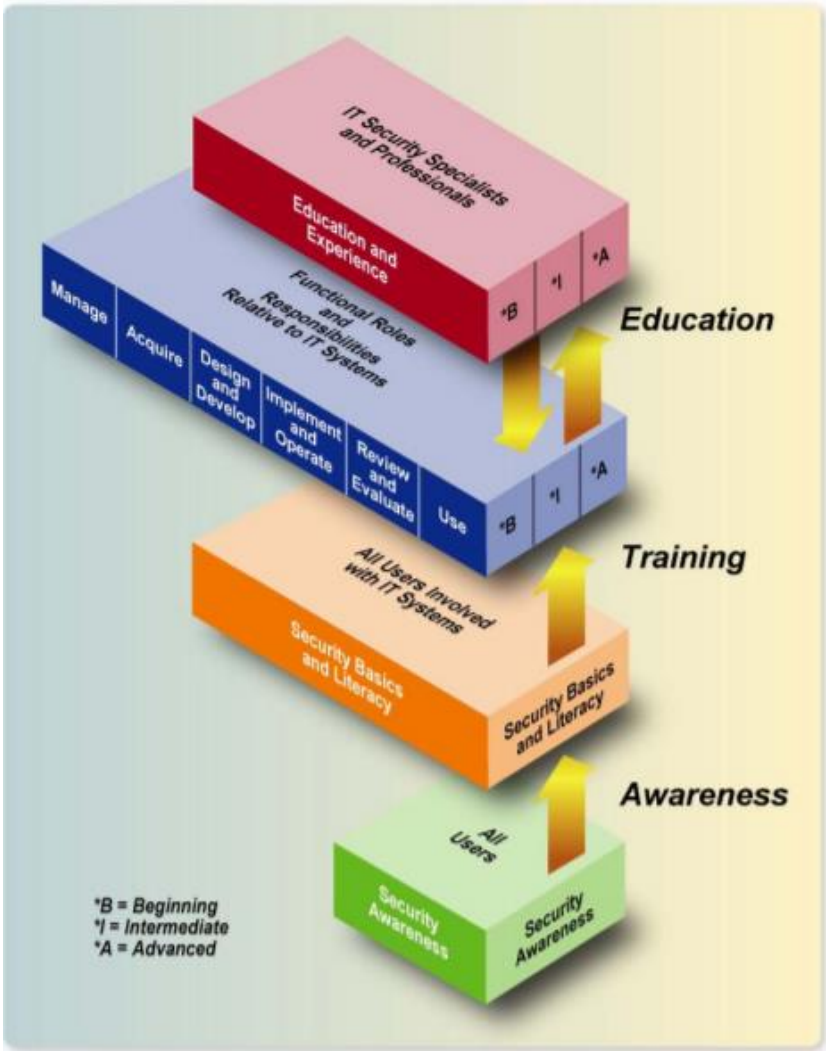
Decentralizovaný model – odpovědná osoba tvoří pouze bezpečnostní politiky organizace. Strategie i samotná implementace je delegována na jiné uživatele. Model je vhodný pro velké podniky (22).

1.9.3 Fáze programu

Program je sestaven pro kontinuální vzdělávání uživatelů. Vzdělávání začíná budováním bezpečnostního povědomí, z kterého vycházejí další fáze (22).

Program SAE je složen ze čtyř fází:

- Povědomí
- Školení
- Vzdělávání
- Profesní rozvoj (22).



Obrázek č. 6: Fáze programu SAE (Zdroj: 22)

1) Povědomí

Účelem této fáze programu je získat základní informace o bezpečnosti. Účastníci si mají uvědomit základní rizika a hrozby z oblasti informační a kybernetické bezpečnosti a umět na tyto hrozby reagovat. Tento stupeň programu je pro všechny členy organizace. Každý uživatel informačních systémů i internetu by měl mít povědomí o bezpečnosti (21).

Mezi první a druhou fází programu SAE definuje norma NIST SP 800-16, ze které vychází tento program, spojovací můstek nazvaný jako Security Basisc and Literacy (základy bezpečnostní gramotnosti). Tento mezistupeň zahrnuje hlubší pochopení bezpečnosti (21).

Do tohoto mezistupně můžeme zařadit například znalosti:

- zranitelnosti IS
- typů kybernetických útoků
- sociálního inženýrství
- základních principů zabezpečení
- základních kryptografických algoritmů
- terminologie (22).

2) Školení

Účelem je vytvořit relevantní a potřebné bezpečnostní dovednosti a kompetence uživatelům z jiných oblastí, než je IT. Jednat se může například o management, oddělení vývoje, auditu apod. Rozdíl oproti předchozí fázi je, že se nezaměřuje jen na pozornost k bezpečnosti, ale učí nové dovednosti, které dovolují účastníkům vykonávat určitou funkci (21).

Fáze školení rozděluje účastníky do tří skupin:

- začátečník
- středně pokročilý
- pokročilý (22).

Rozdělení uživatelů probíhá na základě dosavadních dovedností a znalostí. Pro každou skupinu je stanoven odlišný cíl, kterého má být dosaženo. K tomu je přizpůsobena náplň školení (21).

3) Vzdělávání

Další fáze programu je vzdělávání, která spojuje všechny dovednosti a kompetence z oblasti bezpečnosti do souboru znalostí. Tato fáze se snaží vychovat specialisty informační a kybernetické bezpečnosti, kteří jsou schopni proaktivně reagovat na reálné hrozby a vytvářet vizi v oblasti bezpečnosti (21).

Vzdělávání může probíhat například formou studia na vysoké škole, kde je několik předmětů, které slouží k získání a prohloubení znalostí a dovedností nebo formou vzdělávacích kurzů (22).

4) Profesní rozvoj

Fáze profesního rozvoje slouží, aby uživatelé měli znalosti z oblasti informační a kybernetické bezpečnosti na úrovni, kterou potřebují ve svém profesním životě. Znalosti lze využít k získání certifikátů (22).

Fáze programu definuje dva typy certifikátů:

- obecný – uživatel musí prokázat základní znalosti z oblasti informační a kybernetické bezpečnosti
- technický – pro získání musí uživatel prokázat znalosti z oblasti technického zabezpečení (22).

2 ANALÝZA SOUČASNÉHO STAVU

Protože se svět moderních technologií rozvíjí závratným tempem a v budoucnosti se dále rozvíjet bude, bude nutné, aby se lidé orientovali v tomto světě. Přesto, že se na základních školách učí předměty zaměřené na informační a komunikační technologie, které jsou dány vzdělávacími plány, kvalita výuky je různá a záleží především na znalostech a dovednostech vyučujícího.

Základy bezpečnosti se učí v minimálním rozsahu. Dnes víme, že tato oblast byla po dlouho dobu zanedbávána, ale napravit jí bude velmi obtížné. V budoucnu to bude jedna ze základních oblastí znalosti, kterou by měl každý uživatel, který se bude pohybovat v kyberprostoru, znát. Proto se zaměřím na budování bezpečnostního povědomí pro děti na základní škole. Tento program bych popsal třemi otázkami, co, proč a jak.

2.1 Co je smyslem programu

Smyslem těchto výukových modulů bude seznámit děti s bezpečnostním povědomím. Jelikož dnes děti od brzkého věku využívají telefony, tablety, počítače, mají přístup k internetu, hrají hry, jsou na sociálních sítích a mnoho dalších, pokládám za důležité, aby věděly, jaká rizika se v kybernetickém světě vyskytují. A hlavně, s čím se mohou potkat během aktivit, které provádějí.

V rámci své diplomové práce nejen navrhnu takové moduly, ale také na dvou vybraných školách tento bezpečnostní program odučím, abych v závěru mohl zhodnotit, jak to probíhalo a mohl zapracovat případné připomínky či nedostatky. To proto, aby případně podle těchto modulů mohlo probíhat budování bezpečnostního povědomí i na dalších školách.

Nebo by mohl vzniknout, podle metodiky SAE, decentralizovaný model, kde by učitelé ICT technologií na školách, po absolvování bezpečnostního školení, mohli tyto materiály využít při vzdělávání dětí v rámci svých předmětů, případně kroužků zaměřených na IT. Tak by se v budoucnu zajistilo, že by každé dítě mohlo mít aspoň základy bezpečnostního povědomí.

2.2 Proč budovat bezpečnostní povědomí…

… Na tuto otázku je jednoduchá odpověď. Abychom byli v bezpečí. Dnešní technologie jsou úžasné, ať už z pohledu, že nám usnadňují mnoho práce, nebo dokonce dělají práci za nás nebo nám přinášejí zábavu, snazší a rychlejší komunikaci a mnoho dalších výhod. Stejně jako všude se i v rámci používání těchto technologií kromě pozitivních stránek objevují i negativní. Ty jsou spojené především s tím, že v kyberprostoru neexistují žádná pravidla.

V ohledu, proč budovat bezpečnostní povědomí už u malých dětí, můžeme odpověď rozdělit do dvou časových dimenzí.

a) Pro budoucnost

Svět technologií se rozvíjí a každý z nás je používá a využívat je bude. Z toho důvodů je dobré znát nějaké zásady, abychom se nevystavovali zbytečnému nebezpečí. Každé z dětí bude využívat sociální sítě, bankovní služby a mnoho dalších služeb v rámci internetu, případně mohou být obětí propagandy, dezinformací či fake news. V neposlední řadě je také důležité mít na mysli, že jednou budou z těchto dětí zaměstnanci. Víme, že velkým problémem v bezpečnosti jsou lidé. Budou se jim získané informace v této oblasti hodit v budoucnosti. Takže je to dobrý vklad a investice do profesního života.

b) Pro současnost

Současnost je momentálně ještě důležitější než budoucnost. Především díky tomu, že také malé děti používají moderní technologie. Proto je důležité je seznámit s tím, jak správně technologie využívat a jak se chovat na internetu, aby uměly rozpoznat správné a špatné chování. Možná si to ani neuvědomujeme, ale když děti používají mobilní telefony nebo počítače svých rodičů, mohou svým špatným chováním způsobit bezpečnostní incidenty. O to hůř, pokud využívají pracovní zařízení některého z členů rodiny.

Velice důležité je seznámit děti s tím, co se děje na internetu, jak si musejí dávat pozor na chování ostatních lidí, že se mohou potýkat s ovlivňováním. Příkladem mohou být

různé hry nebo výzvy, které se objevují na internetu. Zmínit se musíme o zneužívání. Je důležité vědět, jak se chovat na sociálních sítích, a co dělat při nějakém podezřelém chování, kterého jsou děti svědkem nebo přímo účastníkem. Případně je také potřebné se zaobírat chováním, kde se mohou děti stát nejen obětí, ale bohužel i útočníky. Jedná se o kyberšikanu. A taky nesmíme zapomenout na další fenomén dnešní doby, nadměrné sdílení informací a možná rizika s tím spojená, která si děti vůbec neuvědomují.

2.3 Jak bude probíhat budování bezpečnostního povědomí

Žáci základních škol jsou rozděleni do tří skupin. První skupinu tvoří I. – III. třída, druhou IV. – V. třída a poslední třetí skupinou je druhý stupeň ZŠ. Pro každou skupinu bude trvat bezpečnostní školení v rozsahu dvou vyučovacích hodin. V rámci toho se děti dozví základní informace a doporučení. Součástí budou také různé hry na procvičení. K těm budou návody, jak je využívat, aby je pak mohli učitelé v případě zájmu kdykoliv využít. Výuka těchto modulů na vybraných základních školách bude probíhat v období březen–duben 2020.

2.4 Zadání modulů

V této kapitole si představíme jednotlivé výukové moduly, jejich rozdělení a základní oblasti, které budeme probírat.

2.4.1 I. – III. třída

V úvodu musíme nastínit, o čem se vlastně budeme bavit a proč je to důležité. Pak se budeme zabývat hlavně tím, co děti vědí. Nejdřív se seznámíme, jaké zařízení znají, jak je využívají. Pokud nějaké zařízení neznají, představíme jej. Hlavním cílem bude děti upozornit, na co si dát pozor, jak by mohla být různá zařízení nebezpečná, a jak je správně používat. Děti bude nutné seznámit i s prostředím internetu a s většinou jeho hrozeb. Zaměříme se také na kyberšikanu a nevhodné chování v on-line prostředí.

2.4.2 IV. – V. třída

V této věkové skupině mají skoro všechny děti svá zařízení. Samy si stahují různé hry, mnoho dalších aplikací a různých souborů. Takže je musíme seznámit s tím, na co si dát pozor, jak snadno můžou stáhnout něco, co nechtějí. Taky už začínají vyhledávat témata, která je zajímají. Proto by bylo vhodné se zabývat i okruhy, jako je sdílení informací, případně nastavení soukromí na sociálních sítích, všem nástrahám, které je mohou potkat v souvislosti se sociálními sítěmi. Stejně jako v předchozím modulu je nutné seznámit děti s nevhodným chováním na internetu, kyberšikanou, ale i s dalšími způsoby nebezpečí. Rovněž je vhodné uvést v realitu, že ne vše, co je na internetu, je vždy pravdivé. Dál se budeme věnovat doporučením, jak správně vytvořit heslo a jak se k heslům chovat.

2.4.3 V. – IX. třída

Pro většinu to bude zřejmě první školení o kyberbezpečnosti. V úvodu s nimi probereme stejná témata jako s předchozí kategorií, samozřejmě do větší hloubky. Výrazně víc bychom se měli zabývat chováním nejen na sociálních sítích, ale i na internetu. Zmíníme podvodné jednaní, falešné e-maily, hoaxy, ovlivňování chování lidí, fake news. Také si představíme rizika s připojováním se na veřejné Wi-Fi. Probereme s nimi některé další pojmy, jako kyberšikana, kybergrooming nebo kyberstalking.

2.5 Popis základních škol

Základní škola Těšany je úplná škola s devíti postupnými ročníky. V každém ročníku je jedna třída. Obec se nachází jihovýchodně od Brna ve vzdálenosti asi 25 km. Školu navštěvují nejen místní děti, ale i z okolních vesnic. Počet žáků ve škole se pohybuje kolem 190. Škola má přibližně 30 zaměstnanců. Součástí školy je také prostorná tělocvična, školní družina, jídelna a venkovní areál.

V budově školy se právě rekonstruovala nová učebna informačních technologií. V každé třídě se nachází dataprojektor, který slouží k výuce. Ve všech třídách jsou k dispozici interaktivní tabule a počítače. Škola pořídila tablety pro výukové účely, 20

tabletů je pro první stupeň, 10 pro druhý a 10 tabletů se využívá ve školce. Každý z pedagogických pracovníků má školní notebook, který užívá nejen pro výuku.

Veškeré softwarové vybavení je licencováno. Na každém počítači je nainstalován antivirový program, kancelářský balík Microsoft Office. Každý z učitelů má vlastní školní e-mail, ze kterého komunikuje se zástupci žáků. Škola má k dispozici různé výukové programy a elektronické materiály, kterými doplňuje a obohacuje vyučovací hodiny.

Druhá vybraná základní škola se nachází ve městě Brně. Zřizovatelem školy je město Brno. Ve škole je zaměstnáno 37 pedagogických pracovníků a 24 nepedagogických pracovníků. Škola disponuje kapacitou 600 míst. Součástí školy jsou dvě počítačové učebny. První z nich obsahuje 30 počítačů a druhá 15 počítačů, všechny zařízení jsou značky HP.

Škola vlastní 10 notebooků a 10 tabletů pro studenty, které využívají pro výukové účely. Učitelé mají k dispozici notebooky, které využívají pro výuku, včetně zápisů do elektronické třídní knihy. Ve většině odborných učeben jsou pro výuku k dispozici dataprojektory, součástí běžných tříd jsou interaktivní tabule. Na počítačích jsou nainstalovány antivirové programy a Microsoft Office

K evidenci žáků, zaměstnanců školní matriky a rozvrhu hodin slouží informační systém Edookit, ke kterému kromě zaměstnanců mají přístup také žáci a zákonní zástupci. Pro druhý stupeň systém nahradil žákovské knížky.

3 VLASTNÍ NÁVRHY ŘEŠENÍ

Tato část práce se bude zabývat především náplní jednotlivých výukových modulů programu vybudování základního bezpečnostního povědomí u žáků základních škol. Cílem práce není vybudovat metodiku, ale především náplň výukových aktivit, které zajistí, aby měli žáci alespoň základy bezpečnosti v oblasti ICT. Bude popsáno také to, jak by měla výuka probíhat, aby byla efektivní a došlo k naplnění cíle.

Nejdřív si krátce představíme program budování bezpečnostního povědomí pro žáky základních škol.

3.1 Cíl programu

V dnešní době žáci základní školy, včetně těch nejnižších ročníků, využívají informační technologie a pohybují se na internetu. Protože většina dětí má nízké povědomí o nebezpečích, které tyto technologie a služby přinášejí, je důležité se negativním stránkám věnovat. Proto vznikl tento program, který je zaměřený na žáky základní škol. Program si klade za cíl seznámení posluchačů s možnými riziky a možnou obranou proti nim.

3.2 Role a odpovědnosti

V rámci programu pro vybudování bezpečnostního povědomí u žáků vybraných škol můžeme definovat následující role a jejich odpovědnost:

- Ředitelé škol – ředitel školy je nejdůležitější součástí, protože musí schválit, že se v rámci výuky vyčlení požadovaný čas, aby mohla proběhnout výuka.
- Učitelé – učitelé jsou v rámci této práce spíše pozorovateli a aktivními posluchači. Není vyloučeno, že i oni se dozví nové informace z oblasti bezpečnosti. Součástí by se mohli stát v případě, že by pro vyučování zakomponovali něco z nabízeného programu, ať už hry nebo jiné výstupy této práce. Speciální kategorií jsou učitelé ICT, se kterými probíhala domluva na

náplni a v rámci jejich odpovědnosti za výuky ICT museli navrhované výukové moduly schválit.

- Pověřená osoba – v rámci návrhu řešení a jeho aplikace na vybrané školy jsem se stal pověřenou osobou já, autor práce. Nesl jsem odpovědnost za návrh modulů, vytvoření materiálů i samotnou implementaci.

Pokud by tento návrh vedl k budování bezpečnostního povědomí i na jiných školách, překlopil by se program do decentralizovaného modelu. Změnily by se také role. Ředitel školy by musel kromě přijetí vzdělávacího programu určit odpovědnou osobu, která bude mít odpovědnost za implementaci. Pověřenou osobou by se s největší pravděpodobností stali učitelé ICT.

3.3 Rozsah a rozdělení uživatelů

U žáků základních škol nebude probíhat rozdělování podle pracovní pozice, ale podle navštěvované třídy. Je zřejmé, že žáci první třídy musí mít jinou náplň a přístup než žáci devátého ročníku. Pro každou ze skupin tak vznikne specializovaný modul, který je náplní i způsobem výuky přizpůsoben jejich chápání a znalostem.

3.4 Modul pro I. – III. třídu

V této skupině se nachází malé děti. Je nutné jim nejdřív vysvětlit, o čem se budeme bavit. Nastínit pojem kybernetická bezpečnost by bylo složité a těžko pochopitelné. Je potřeba situaci přirovnat k příkladu, který určitě všechny děti znají - cesta do školy.

Při navazování komunikace s dětmi připomínáme rady, které jim rodiče, případně učitelé, dávají, aby se jim na cestě nic nestalo. Například, že nemají nikam chodit s cizími lidmi, na přechodu se musí pořádně rozhlédnout, zda nejede auto, případně, že nemají hladit neznámá zvířata a mnoho dalších.

Následně přejdeme k tomu, jak používat moderní technologie, tak, aby se nám nestalo něco špatného, abychom byli v bezpečí. Cílem není děti vystrašit a vzbudit v nich nějaký odpor k užívání těchto zařízení, ale ukázat, že když budou dodržovat dané

zásady, nemusí se vůbec ničeho obávat. Stejně jako cesta do školy. Když dodržujeme všechny rady, nemělo by se nám nic stát.

3.4.1 Základní pojmy

Všechny děti nemusí znát veškerá nabízená zařízení, a dokonce i ty, které znají, nemusí využívat. Záleží, s čím přijdou ve svých rodinách do kontaktu, případně jak a co jim rodiče dovolí. Proto je zapotřebí nejdřív se seznámit s těmito technologiemi a pojmy, aby všechny děti byly v obraze k dalšímu pokračování. Proto bylo vytvořeno pexeso na tématiku, která souvisí s informačními a komunikačními technologiemi. Na začátek bude dobré si tuto hru zahrát. Pexeso je součástí přílohy 1.

Po skončení hry si společně projdeme obrázky z pexesa. Budeme si postupně s dětmi vysvětlovat, co je znázorněno na obrázku. Ideálně budeme obrázky promítat pomocí dataprojektoru. Děti zapojíme tak, že budou moci říct, jestli a k čemu takové zařízení využívají. U zařízení, bude-li to možné, připojíme zároveň nějakou bezpečnostní zásadu, kterou by děti v tomto věku měly znát.

Počítač – slouží k práci i zábavě, např. k vyhledávání informací, sledování videí, prohlížení internetu, hraní her. Důležité je dodržování zásad:

- ke každému počítači by se mělo přihlašovat pomocí hesla
- používat speciální programy (antivirová ochrana)
- budeme-li chtít hrát nějakou hru nebo sledovat video, měli bychom se zeptat rodičů

Notebook – je přenosný počítač. Platí pro něj to stejné, jako pro počítač.

Klávesnice a myš – pomocí těchto zařízení ovládáme počítač. Klávesnicí píšeme a myší pohybujeme kursorem po obrazovce.

Telefon – využíváme pro telefonování, psaní textových zpráv, ale také k zábavě, hraní her, fotografování, natáčení videí, poslouchání hudby a mnoho dalších. K telefonu je důležité znát několik rad, které bychom měli splňovat. Jsou to:

- nedávejme cizím lidem své telefonní číslo
- pokud hrajeme hry, dávejme pozor na vyskakující reklamy
- stahujeme-li novou hru (aplikaci) přečteme si všechny informace k této aplikaci. Tato činnost může být nebezpečná a děti by jí měly přenechat rodičům, kteří by si měli přečíst všechny informace a zvážit, zda můžete stáhnout
- při focení nebo natáčení videí se vždy zeptejte, neměli bychom fotit osoby, které nechtějí být dokumentovány

Tablet – počítač, který vypadá jako velký telefon.

Televize – slouží ke sledování televizních stanic. Nové televize se už umí připojit i k internetu a umožňují mnoho dalších služeb.

Web kamera – pomocí ní můžeme natáčet například video, nebo využívat videohovor. Takovou kameru najdeme na každém notebooku, V současnosti se objevují i na některých televizích. Tato kamera se dá schovat pomocí speciálních krytek, aby nás nikdo nemohl sledovat.

Sluchátka – využíváme je, když nechceme rušit okolí při poslouchání hudby, hraní her nebo poslouchání namluvených knih. Zde je důležité děti seznámit s tím, že nikdy by neměly používat sluchátka, když jedou na kole nebo jdou po silnici, protože pak neslyší okolí, například jedoucí auto, cyklisty, a mohlo by se něco špatného stát.

Tiskárna – slouží k vytisknutí dokumentů, obrázků.

Skener – opak tiskárny; dokumenty nebo obrázky, které máme na papíře můžeme naskenovat (nafotit) do počítače.

Tiskárnu i skener lze mít jako samostatné zařízení, nebo mohou být společné.

USB Flash disk – malé zařízení, které slouží pro ukládání dat. Využijeme jej, pokud budeme chtít z jednoho počítače přenést data to druhého počítače. Nebo pokud si na něj uložíme film, můžeme ho poté spustit na televizi. K USB flash disku přidáváme důležité doporučení, najdeme-li někde cizí USB flash disk, neměli bychom ho nikdy použít, protože nevíme, co je na něm uložené.

Internetové (webové) prohlížeče – jsou programy, které umožňují přístup k internetu. Pomocí nich navštěvujeme různé stránky, na kterých vyhledáváme informace, hrajeme hry, sledujeme videa, komunikujeme s přáteli, nakupujeme a mnoho dalšího.

Obrázek č. 7: Internetové prohlížeče (Zdroj: 23)

Internetové (webové) vyhledávače – abychom pomocí internetového prohlížeče našli webové stránky, které hledáme, musíme využít některý z internetových vyhledávačů, který nám vyhledá stránky podle zadaných informací.

Obrázek č. 8: Internetové vyhledávače (Zdroj: 24)

Antivirové programy – speciální programy, které nám pomáhají chránit naše zařízení (počítače, telefony, ...). Kontrolují nejen naše data, která máme uložená, ale také webové stránky, na které přistupujeme a ze kterých stahujeme data (hry, videa, …). Vyhledávají viry, které by nám mohly uškodit. Je to základní obrana a měli bychom na každém počítači mít zakoupený některý z antivirových programů.

Obrázek č. 9: Ikony antivirových programů (Zdroj: 25)

Antivirovým programům bychom měli věnovat více času. Narazili jsme na pojem počítačový virus. Vysvětlíme na jednoduchém příkladu ze života. Děti samotné prošly některými nemocemi. A my představíme počítačový virus jako nemoc. Tak jak je potřebné chránit sebe, doplňovat vitamíny, správně se oblékat, abychom nechytili virus, který způsobí rýmu, kašel, teplotu, tak existují i počítačové viry, které můžou napadnout náš počítač.

Malé děti si můžou počítačový vir představit jako červíka, který bude umět následující úlohy:

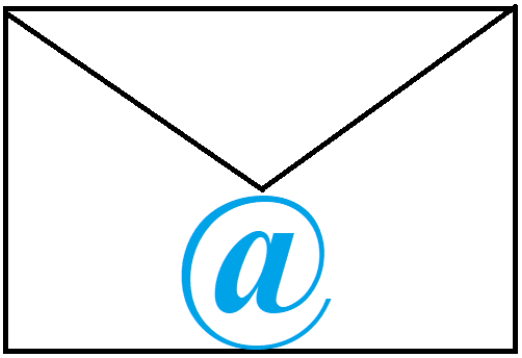
- červík ničitel – dokáže celý počítač nebo jiné zařízení úplně zničit nebo smazat vše, co máme uložené
- červík zloděj – ukradne nám vše, co máme v počítači uložené, např. fotky, videa.
- červík zvědavec – může sledovat vše, co na počítači děláme nebo píšeme a informace předat někomu cizímu.

Proto je důležité se chránit a používat již zmíněné antivirové programy.

Obrázek č. 10: Ochrana antivirovým programem (Zdroj: 26)

Sociální sítě – spojuje lidi, kteří pomocí nich komunikují, nebo sdílí fotografie případně zážitky. Tady je potřeba se dětí zeptat, jestli znají některé sociální sítě, případně jestli už někdy slyšely pojmy jako Facebook, Twitter, Instagram, WhatsApp, YouTube. Dále upozorníme děti, že se na sociálních sítích vyskytují různí lidé, kteří nemusí být vždy „hodní“, a proto máme být obezřetní k využívání sociálních sítí. Kvůli nízkému věku nebudeme rozebírat nebezpečí spojené s využíváním těchto sítí, to probereme až se starší skupinou.

E-mail – slouží v elektronickém světě k posílání zpráv. V podstatě to můžeme dětem přiblížit jako elektronický dopis nebo pohled, který můžeme poslat a bude doručen okamžitě. Protože nepředpokládám, že děti do třetí třídy by měly vlastní e-maily, nebudeme v tomto modulu řešit správné zacházení s e-mailem. Pouze upozorníme, že jelikož se dá s jeho pomocí poslat cokoliv, je opět důležité pracovat s ním pozorně.



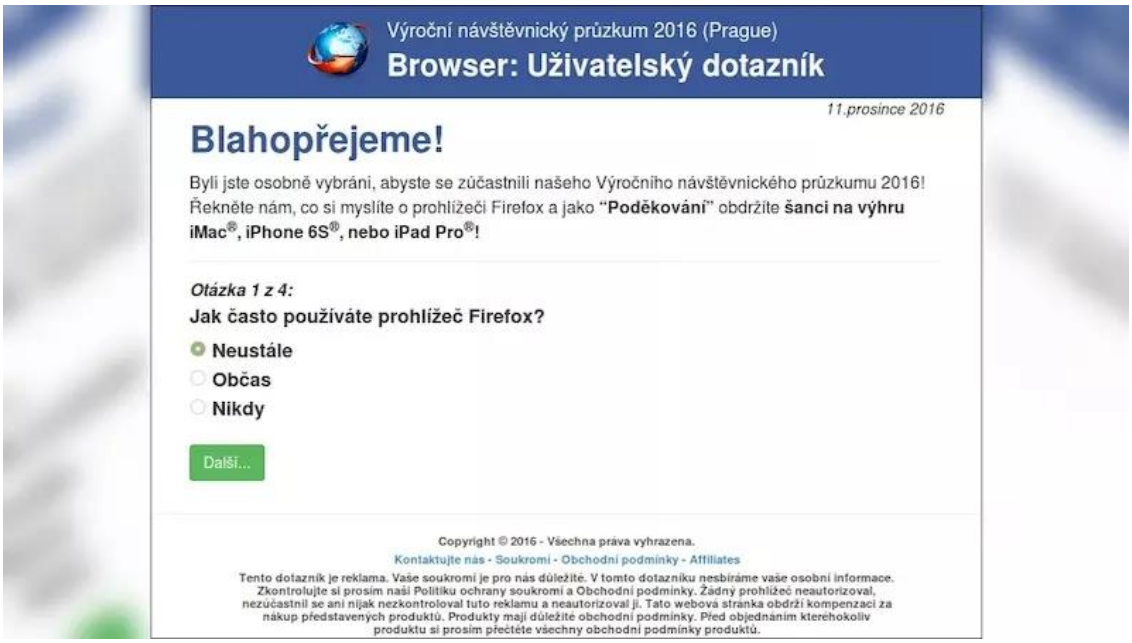
Obrázek č. 11: E-mail (Zdroj: Vlastní zpracování)

Po představení a vysvětlení základních pojmů, které se objevily během pexesa, přikročíme k druhé části. V té se budeme zabývat internetem a on-line prostředím.

V tuto chvíli je důležité všem dětem vysvětlit, že v prostředí internetu se mohou potkat s kýmkoliv. A jak v našem světě, tak i v kybernetickém světe se nacházejí zlí lidé. Proto musíme dávat pozor na to, co děláme. Protože děti v této věkové skupině nedokážou posoudit všechna rizika, je vhodné, aby si osvojily nějaké zásady. A to například, že by samy neměly stahovat žádnou hru do svého telefonu nebo počítače, ale měly by požádat rodiče o dovolení. Ti by měli zodpovědně posoudit situaci. Dalším důležitým bodem je, aby si děti zažily to, že na internetových stránkách si každý může psát co chce. Proto

nesmí věřit všemu a dělat vše, co jim někdo doporučuje. Pokud se jim něco nezdá, měly by opět informovat rodiče nebo učitele.

Tato věková skupina využívá internet především k hraní her. Kromě již zmíněného stahování se můžou setkat i s vyskakujícími reklamami. Opět musíme děti informovat o obezřetnosti, na co klikají. Tyto reklamy se snaží pouze o to, abychom buď dodali nějaké informace, nebo si něco zakoupili. Více upozorníme na to, pokud na ně vyskočí nějaké okénko, že vyhráli, a aby vyplnili údaje, nesmí vyplňovat nic a toto okénko zavřít. Případně opět přivolají rodiče nebo dospělou osobu o pomoc. Na ukázku přikládám jeden vyskakující uživatelský dotazník.



Obrázek č. 12: Vyskakovací okna – výhra (Zdroj: 27)

3.4.2 Kyberšikana

Dalším důležitým tématem je kyberšikana. Pojem šikana se s dětmi rozebírá od mateřské školy. Nyní ji probereme z pohledu kybernetického světa. Samozřejmě se jedná o špatnou věc. Pod tímto pojmem si můžeme představit ubližování, zesměšňování, vydírání, pomlouvání pomocí sociálních sítí, zpráv, e-mailů nebo diskusemi na internetu. Pokud se někdo stane svědkem takového chování, musí opět informovat dospělé.

Zaměřil bych se na způsoby, jak se může stát, že někdo se stane tím, kdo může šikanovat. Pro příklad uvedu - děti ještě nemají sociální sítě, ale mají telefony. Jako kyberšikana může být považováno natáčení nebo focení ostatních dětí. Na fotkách a videích vypadají například směšně nebo škaredě. Na základě těchto materiálů se jim pak vysmívají, případně to ukazují všem ostatním a dotyčné pomlouvají. Děti si mohou osvojit následující pravidlo, než někoho vyfotím, nejprve se zeptám, zda-li můžu.

3.4.3 Hra na opakování

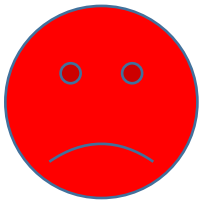
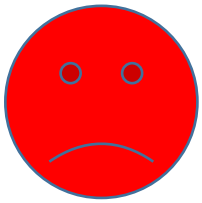
Na závěr bych přidal další malou hru, která vychází ze hry Semafor „bezpečně na YouTube“, kterou ve své metodice vydal Národní úřad pro kybernetickou a informační bezpečnost. Hru jsem upravil podle potřeb pro současný vzdělávací modul. Slouží pro zopakování všeho, co jsme probírali. Šablona pro vyplnění hry je přiložena v příloze 2.

Hra spočívá v tom, že si děti přečtou situaci a do vedlejšího sloupce namalují smajlíka. Pokud je situace správná, namalují zeleného usměvavého smajlíka. Pokud je řešení situace špatné, namalují červeného smutného smajlíka.

Na konci hry se vrátíme k situacím, které budou červené. Popovídáme si s dětmi, co je špatně nebo jak by se měly správně zachovat v určité situaci.

Tabulka č. 1: Hra na opakování (Zdroj: Vlastní zpracování dle 28)

Moji kamarádi vymysleli novou hru, která se jmenuje „Na šneky“. Při této hře se rozběhnete a jedním skokem rozšlápnete šnečí ulitu. Holky říkají, že je to nechutné a týrání zvířat, ale pro nás kluky je to velká zábava, a proto natočím video, aby se pobavili i ostatní.	
Na každém počítači by mělo být heslo pro přihlášení.	

Používat antivirový program je zbytečné a nepomůže nám.	
Když chceme hrát hru na počítači nebo telefonu, zeptáme se rodičů.	
Potkám na ulici někoho, koho neznám. On bude chtít, abych mu dal své telefonní číslo. Já mu své číslo dám.	
Vyfotím svého kamaráda, a ten na fotce vypadá směšně. On bude chtít, abych fotku smazal. Ale já ji budu ukazovat ostatním a smát se mu.	
Jdu na kroužek, a aby mi cesta rychle utekla, nasadím si sluchátka a budu po cestě poslouchat muziku.	
Začnou mi chodit zprávy, kde mě bude někdo napadat, vyhrožovat nebo urážet. Nahlásím tyto informace rodičům.	
Najdu si novou hru a chci si ji zahrát. Ptát se rodičů, jestli si jí můžu stáhnout je zbytečné, protože se mi nemůže nic stát.	
Na internetu píšou články různí lidé, proto nesmím věřit všemu, co si přečtu, a také dělat vše, co mě někdo radí.	

Při hraní her na mě vyskočí stránka, že jsem vyhrál. Mám vyplnit nějaké informace. Chci vyhrát, a tak vyplním své jméno, příjmení, bydliště a další informace.	
Jdu do školy a najdu na zemi USB flash disk. Jsem zvědavý, co je na něm, a tak ho vložím do počítače, abych to zjistil.	
Jsem v pokoji se svým sourozencem. Ten se chce učit a já poslouchat hudbu. Abych ho nerušil, použiji sluchátka.	

Situace, kde se objevuje červený smutný smajlík projdeme s dětmi znovu a necháme děti říct, co je špatně a proč. A jak by bylo správné se zachovat.

Tabulka č. 2: Oprava hry (Zdroj: Vlastní zpracování dle 28)

Moji kamarádi vymysleli novou hru, která se jmenuje „Na šneky“. Při této hře se rozběhnete a jedním skokem rozšlápnete šnečí ulitu. Holky říkají, že je to nechutné a týrání zvířat, ale pro nás kluky je to velká zábava, a proto natočím video, aby se pobavili i ostatní.	Špatné chování, protože ubližovat zvířatům se nesmí. A sledovat taková videa je také špatné a nemorální.
Používat antivirový program je zbytečné a nepomůže nám.	Musíme používat antivirový program, je to základní ochrana pro naše zařízení.
Potkám na ulici někoho, koho neznám. On bude chtít, abych mu dal své telefonní číslo. Já mu své číslo dám.	Své číslo bychom neměli nikdy dávat cizím lidem.

Vyfotím svého kamaráda, a ten na fotce vypadá směšně. On bude chtít, abych fotku smazal. Ale já ji budu ukazovat ostatním a smát se mu.	Pokud po nás někdo chce, abychom smazali fotku, na které je vyfocen, je správné to udělat. Takové chování by mohlo být považováno za kyberšikanu.
Jdu na kroužek, a aby mi cesta rychle utekla, nasadím si sluchátka a budu po cestě poslouchat muziku.	Když budeme mít sluchátka, neuslyšíme, co se kolem nás děje, např.: jedoucí auto, zvonící kolo.
Najdu si novou hru a chci si ji zahrát. Ptát se rodičů, jestli si jí můžu stáhnout je zbytečné, protože se mi nemůže nic stát.	Při stahování her můžu stáhnout i nějaký vir. Proto stahovat hry do telefonu musíme obezřetně.
Při hraní her na mě vyskočí stránka, že jsem vyhrál. Mám vyplnit nějaké informace. Chci vyhrát, a tak vyplním své jméno, příjmení, bydliště a další informace.	Takové výhry jsou většinou jen záminkou, aby někdo získal osobní údaje, např.: jméno, adresu, …
Jdu do školy a najdu na zemi USB flash disk. Jsem zvědavý, co je na něm, a tak ho vložím do počítače, abych to zjistil	Nesmím používat cizí zařízení, může obsahovat vir.

Na závěr vyučovacího modulu můžeme zjistit:

- které informace byly pro děti nejzajímavější
- jaké informace byly nové
- jestli se chtějí na něco zeptat či něco dalšího doplnit
- jestli je to bavilo a chtěly by další pokračování na toto téma

3.5 Modul pro IV. – V. třídu

V uvedené skupině jsou děti větší a odpovídá tomu nejen jejich chápání, ale i využívání různých technologií. V těchto třídách převážná většina dětí vlastní svoje zařízení, zejména jsou to mobilní telefony. Využívání počítačů a internetu je na jiné úrovni než v předchozí věkové kategorii. Zmiňovaný modul bych rozdělil do několika menších bloků. Každý z těchto bloků bude rozebírat jinou oblast.

3.5.1 Úvodní seznámení

Nejdřív musíme děti seznámit s tím, čemu se budeme věnovat. Témata k debatě budou, jak správně používat své zařízení, jak využívat a chovat se na internetu. A to vše tak, abychom byli v bezpečí a nestalo se nám něco nepříjemného. Můžeme si udělat představu o aktivitách dětí na internetu následnými otázkami. Vhodné je zjištění, jak často aktivity na telefonu, počítači provádí, jestli pravidelně každý den nebo jednou za čas. Při pravidelnosti využívání se ptáme na délku časové frekvence:

- Kdo z vás má telefon? Stahujete hry?
- Kdo z vás má jiné zařízení, počítač nebo notebook?
- Kdo z vás hraje on-line hry na internetu? Kdo hraje každý den?
- Kdo z vás sleduje videa na YouTube? A jak často?
- Využíváte internet ke psaní úkolů do školy?
- Víte, co jsou to sociální sítě? Využívá z vás někdo nějakou?
- Jaké další aktivity provádíte na internetu?

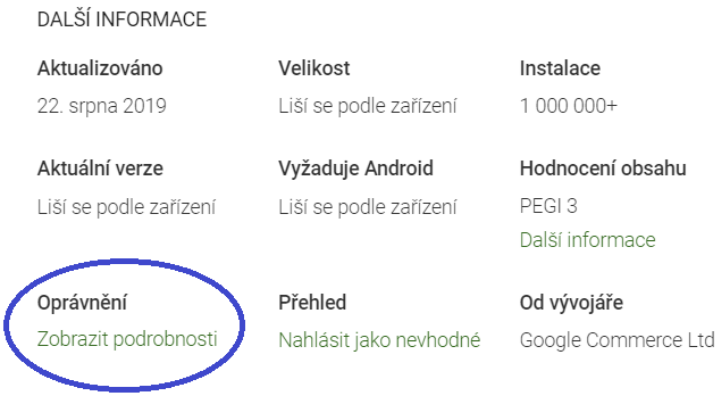
V první řadě je potřeba probrat, jak chránit svá zařízení. Například počítač. Určitě by si každý uživatel, pokud je dítě, měl uvědomovat, že na každém počítači by mělo být heslo, aby k němu mohl přistupovat jen ten, kdo tohle heslo zná. Dalším důležitým aspektem je, aby každý věděl, co je antivirový program a proč je dobré jej využívat.

Stejně tak je důležité probrat mobilní telefon. Děti už ho určitě znají, většina z nich dokonce vlastní. Důležité je upozornit na následující chování:

- nedávat číslo cizím lidem (zvážit zveřejňování na internetu)
- dávat pozor při stahování her a aplikací
- pozor na fotografování (viz část pojednávající o kyberšikaně)

3.5.2 Stahování her a aplikací

K oblíbeným činnostem, které děti provádějí na telefonu, určitě patří hraní her, stahování různých lákavých aplikací, ať už pro zábavu nebo i pro smysluplné využívání. Protože se i na Google Play objevily nebezpečné aplikace, je potřeba používat rozum před tím, než si něco nainstaluji. Horší je, když stahují něco z různých nezabezpečených stránek, odkud si mohou stáhnout i něco, co nechtějí. Proto je zapotřebí si vždy klást otázku, jestli stahuji z bezpečných zdrojů. Avšak závadné aplikace se objevují všude. Proto je nutné se zamyslet, zda stahovanou aplikaci opravdu potřebuji a k čemu jí budu využívat. Když už se rozhodneme, že jí potřebujeme nainstalovat, musíme si přečíst podmínky využívání. Obzvlášť pak jaké oprávnění aplikace vyžadují.



Obrázek č. 13: Oprávnění aplikací (Zdroj: Vlastní zpracování dle 29)

Když se podíváme na požadované oprávnění, měli bychom následně zvážit, zda aplikace opravdu potřebuje taková oprávnění, která vyžaduje. Jako příklad se můžeme podívat na výzkum společnosti Avast, který se zaměřil na svítilny.

Svítilny by ideálně měly požadovat jen jediné oprávnění, a to pro přístup k fotoaparátu, kterým lze ovládat LED světlo. Do výzkumu se vybralo 937 svítilen. Některé z nich potřebovali až 77 různých oprávnění. Například 180 aplikací chtělo číst kontakty v telefonu, 77 chtělo nahrávat zvuk nebo 131 chtělo získat přesnou polohu (30).

Nastávají jednoduché otázky:

- K čemu vybraná aplikace potřebuje monitorovat GPS polohu, kde se pohybuji?
- Proč potřebuje mít přístup ke kontaktům uložených v telefonu?

Odpověď na otázky jsou jasné. Nepotřebnost. Proto bychom neměli takové aplikace instalovat do telefonu. Tyto otázky je důležité si klást pokaždé, než něco stáhneme. Případně bychom se měli podívat co už ve svém telefonu máme a k čemu mají oprávnění. Podezřelé aplikace je pak vhodné odinstalovat. V novějších telefonech jde některá oprávnění zakázat.

Přestože ve školním řádě je zakázané používat telefony ve škole, můžeme udělat malou výjimku. Děti, pokud budou mít u sebe telefon, se můžou podívat, jaká oprávnění využívají aplikace, které mají na svých zařízeních. Případně pokud nemají telefony u sebe, můžeme se společně podívat na oprávnění těch, která znají či využívají.

3.5.3 Chování na internetu

V tomto věku se děti pohybují na internetu bez dohledu a vyhledávají témata, o která se zajímají. V této části se budeme věnovat, jak se bezpečně chovat na internetu. V první řadě bych se zaobíral sdílením informací.

Sdílení informací

Nejdřív musíme děti seznámit s tím, že není vhodné na internet sdílet své osobní údaje. Protože se k nim může dostat kdokoliv a informace zneužít. Skupiny děti budou v brzké době využívat sociální sítě, někteří už je využívají teď. Proto se zaměříme na to, co by neměly zveřejňovat nejen na sociálních sítích, například:

- telefonní číslo
- e-mail
- adresu bydliště
- informace o tom, do které školy chodím nebo které kroužky navštěvuji.

Protože žáci na internetu vyhledávají i stránky s tématy, o která se zajímají, někdy je možnost se na těchto stránkách také registrovat. Ať už je důvod jakýkoliv, musí děti vždy zvážit, jestli to je potřeba. Měly by mít namysli, že tak někomu dají svoje údaje. Pokud už se někam registrujeme, měli bychom vyplňovat co nejméně údajů o sobě.

Všeobecně, než něco sdílíme, musíme si to pořádně rozmyslet. Obzvlášť pokud jsme aktivní na sociálních sítích, kde se mnozí stávají závislými nad sdílením každodenních činností. Ne každého zajímá, co právě děláme, nebo co jsme dnes měli k obědu. Je vhodné s dětmi probrat, že než něco budou sdílet, je potřeba si to rozmyslet. Jako pomůcka se dá použít představa, že jdou po ulici a někoho potkají. Řekly by mu nebo ukázaly by mu, co chtějí sdílet? Těžko by kolemjdoucím na ulici ukazovaly fotky obědů nebo jim vykládaly, co vše dnes dělaly, kde byly apod. Opravdu není potřeba sdílet takové věci. Doporučení může být, aby každý uživatel sdílel jen ty zážitky, fotky nebo aktivity, o kterých chce informovat své okolí, které by svým přátelům řekl nebo ukázal při nejbližším setkání.

Dále se dostaneme i ke sdílení fotografií, případně videí. Jedná se o velmi populární činnost, která skýtá mnohé nebezpečí. Za prvé bychom neměli zapomínat na to, že než zveřejníme nějakou fotografii, měli by souhlasit všichni, kteří jsou na fotce. Pokud už budeme sdílet fotografii například se svým spolužákem, který bude chtít, abychom tu fotku smazali, musíme jí smazat, protože je to naše povinnost.

Nakonec bychom neměli zapomenout na to, že bychom neměli sdílet intimní fotky, ale taky fotky z domácnosti, protože nikdy nevíme, kdo je uvidí. Mohlo by to přilákat zloděje.

Autorská práva

Tady je potřeba zmínit především takové aktivity, kterými lze snadno porušovat zákon. Na internetu lze snadno najít zápisky do čtenářského deníku nebo referáty do školy. Všichni jistě známe oblíbené zkratky CTRL + C a CTRL + V. Ale pozor! Vydávat něčí práci za svou je trestné. Děti také musí vědět, že i fotky na internetu mají autorská práva a používat cizí fotky bez souhlasu je nelegální.

Online výzvy

Nejdřív je potřeba si říct, co vlastně online výzvy jsou. Musíme si ujasnit, že máme pozitivní a negativní výzvy.

Pokud narazíme na výzvu, musíme opět použít svou hlavu. Jestliže se jedná o pozitivní výzvu, nemusíme se bát jí vyplnit, například

- Trashtag Challenge v rámci niž účastníci uklízí přírodu a veřejný prostor a pak sdílí fotografie před a po úklidu (31).

Pokud mám pochybnosti a výzva se řadí mezi negativní, není vhodné jí plnit, případně dále šířit. Žáci musí vědět, uvidí-li svého kamaráda, jak zkouší nějakou nebezpečnou výzvu, měli by informovat učitele nebo rodiče, protože se snadno mohou dostat do nebezpečí. Takových výzev na internetu koluje velké množství. Na ukázku si představíme některé z nebezpečných výzev:

- Ghost Pepper Challenge – lidé polykají pálivé chilli papriky (31).
- Blue Whale Challenge (Modrá velryba) – vznikla původně jako hoax, panika měla za následek, že se posléze stala tato výzva skutečnou. Jde o plnění několika úkolů, kde docházelo k sebepoškozování. Posledním úkolem byla sebevražda. Tato výzva si vyžádala nemalý počet obětí z řad dětí. Výzva bohužel vedla k vytvoření dalších nebezpečných her, kde se měly plnit nebezpečné úkoly např. Momo Challenges (31).
- Choking Game, Purple Dragon, Space Monkey, Blackout Game nebo Choking Challenge – názvy výzev, které nabádají ke škrcení, dokud nedojde k omdlení. V USA v na následky těchto výzev ročně zemře přibližně 100 dětí (31).

Ne všechny informace jsou pravdivé

Na závěr části věnované chování na internetu se musíme už s těmito dětmi bavit o tom, že internet je svobodný. Takže si na něm může psát každý, co chce. Proto každý uživatel by měl vědět, že nesmí věřit všemu, případně dělat vše, k čemu ho někdo nabádá. To všechno se děje proto, aby někdo někoho ovlivnil, podvedl nebo jen rozšířil strach.

Tudíž by si už malé děti měly zapamatovat, že musí používat svůj rozum a informace si ověřovat na více zdrojích. Pokud si přečtou nějakou neuvěřitelnou zprávu, určitě je vhodné to probrat s rodiči nebo učiteli, jestli je to vůbec možné. Nebo zda se jedná o nepravdivé informace. Dětem můžeme ukázat následující ukázku, aby si lépe představily, o co se jedná.

Obrázek č. 14: Ukázka falešných informací (Zdroj: 32)

3.5.4 Kyberšikana

Pojem šikana již děti určitě slyšely. Zajisté už slyšely i pojem kyberšikana. Kromě definic, o co se jedná, je důležité dětem vysvětlit, že pokud se stanou obětí nebo svědkem jakéhokoliv obtěžování, je důležité to nahlásit. Víme, že tento fakt není jednoduchý. Často najít odvahu něco sdělit a vyjádřit nepříjemnost, ubližování, je nejen pro děti, ale často i pro dospělého, složitým a časově náročným aspektem. Děti musí pochopit, že se v takovém případě nejedná o žalování.

Nestačí si pojem pouze vysvětlit. Je dobré si také následně procvičit, zda děti poznají případy kyberšikany. Zároveň si tak ukážeme příklady, jak může šikana probíhat, a také

různé formy kyberšikany. K tomu využijeme kvíz od O2 Chytrá škola. Pokud budou k dispozici počítače nebo tablety, mohou děti vyplnit tento kvíz elektronicky na adrese https://www.o2chytraskola.cz/test/4/7.

Kvíz od O2 Chytrá škola – Co je kyberšikana

1. *„Kamarád ti pošle ošklivou SMS zprávu, ve které tě urazí, a pak už to nikdy neudělá.*
2. *Někdo tě vyfotí svým mobilním telefonem a fotku upraví tak, aby tě zesměšňovala. Pak ji začne rozesílat tvým spolužákům.*
3. *Někdo ti vytvoří falešný profil na Facebooku a pomocí něj uráží, pomlouvá a napadá další uživatele internetu.*
4. *Někdo tě pomocí mobilního telefonu natočí, jak sedíš na záchodě. Video nahraje na YouTube.*
5. *Maminka ti zakázala internet, protože jsi zlobil/a.*
6. *Někdo ti napsal na tvoji zeď na Facebooku, že tě nemá rád (nepoužil nadávky).*
7. *Spolužáci o tobě na internetu vytvořili veřejnou diskusní skupinu, ve které o tobě rozšiřují lži a pomluvy.*
8. *Spolužák tě vydírá, že pokud mu nebudeš odevzdávat kapesné, rozšíří o tobě na internetu, že jsi homosexuál (gay/lesba).*
9. *Tvůj nejlepší kamarád ti na profil napíše: „Ty jsi ale dobytek!“ a doprovodí svůj vzkaz několika smajlíky.*
10. *Kamarád tě ve škole urazil, a proto jsi se rozhodl/a pomstít. Tajně jsi ho ve škole vyfotil/a, a začal/a jsi jeho fotografii rozšiřovat internetem s doprovodným komentářem, že je zloděj*“ (33).

Řešení, zda se jedná o šikanu

1. Ne. Pokud to bude jednou. Při opakování by se už o šikanu jednalo.
2. Ano.
3. Ano. Krádež identity je projev kyberšikany.
4. Ano.
5. Ne.

6. Ne. Lidé mají právo vyjadřovat názory i negativní. Pozor, při opakovaném psaní takových komentářů by se mohlo jednat o kyberšikanu.
7. Ano.
8. Ano. Vydírání je projev kyberšikany.
9. Ne. Kamarádi mohou použít i vulgární výrazy, přesto je nevnímají jako ponižující a ubližující. Opět se při častém opakování jedná o projev kyberšikany.
10. Ano.

3.5.5 Hesla

S dětmi si probereme několik pravidel pro práci a tvorbu hesel. Nejdřív můžeme nechat děti vysvětlit, jak chápou heslo. Co to je a jestli už jej někde užívají.

Heslo si můžeme představit jako klíč. Tak, jako máme klíček od domu nebo od skřínky, abychom se dostali domů nebo do skřínky, musíme mít správný klíč. Klíč odemkne pouze dveře, ke kterým je určen. Abychom se dostali například k počítači, nebo k nějaké službě na internetu pouze my, používáme heslo. Tudíž se k počítači dostane pouze ten, kdo má správné heslo (tak jako se do domu dostane pouze ten, kdo má od něho klíč).

Obrázek č. 15: Heslo jako klíč (Zdroj: Vlastní zpracování)

Základní zásada pro práci s heslem:

- heslo je tajné, nesmíme ho nikomu říkat, ani kamarádům (stejně jako nedáváme klíč od domu cizím lidem)
- heslo si nemáme psát na lístečky, které pak přilepíme například na monitor, nástěnku nebo vložíme pod klávesnici (ani klíč nenecháváme venku v zámku, aby se k němu dostal někdo cizí)
- nepoužívat stejné heslo k více službám, to proto, pokud by nám někdo tohle heslo ukradl, mohl by se pak dostat ke všemu (každé dveře mají svůj klíč)
- v prohlížečích se objevuje možnost zapamatování si hesla. Nikdy bychom neměli nechávat hesla uložená v prohlížečích, pokud má k počítači přístup někdo další
- pokud se někam přihlásíme, musíme se také odhlásit (než odejdu z domu, musím zamknout).

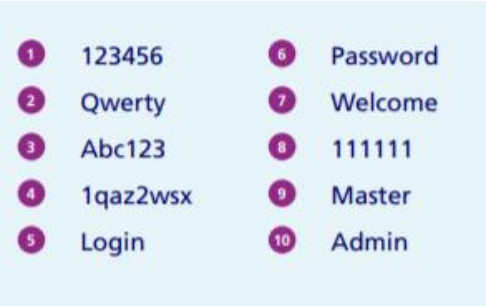
Jak vytvořit heslo

Když už jsme si ukázali, jak správně s hesly pracovat, musíme se naučit také vytvořit si správné heslo. Tvorba hesla není tak jednoduchá, jak se zdá. V dnešní době se dají hesla snadno odhadnout nebo prolomit. Při dnešních možnostech se jednoduché heslo dá rozluštit za několik málo minut.

Začneme tím, jak by heslo nemělo vypadat. Heslo by nikdy nemělo být:

- naše jméno, ani žádné jiné jméno (rodičů, sourozenců, zvířátek)
- datum narození
- nepoužívejme ani slova ze slovníku
- jednoduchá hesla, které se snadno pamatují.

Na následujícím obrázku vidíme 10 hesel, která se běžně využívají. Ovšem, kdo taková hesla používá, koleduje si o problém.



Obrázek č. 16: Špatná hesla (Zdroj: 34)

Teď se tedy pojďme podívat, jak tvořit hesla. Platí pro ně několik všeobecných zásad, které se běžně doporučují, například, že heslo by mělo mít alespoň 8 znaků, kombinace velkých a malých písmen, číslic a speciálních znaků.

Heslo můžeme vytvořit například tak, že si vezmeme nějakou větu. Ideálně aby obsahovala i nějakou číslici. A použijeme první písmena z těchto slov. Číslici napíšeme číslem. Začátek věty a jména budou velkým písmenem.

Např. Máme doma dva malé pejsky Endy a Jessie.

- Heslo: Md2mpEaJ

Více variant: Za nebo před heslo můžeme přidat speciální znak a k čemu patří:

- Heslo k počítači: Md2mpEaJ_pc
- Heslo k Facebooku: Md2mpEaJ_fb
- Heslo k E-mailu: Md2mpEaJ_em

Pokud si nastavíme určitá pravidla, která budeme dodržovat, můžeme si tak vytvořit silná hesla, která si zapamatujeme a nebudeme si je určitě muset nikam psát. Navíc takové heslo splňuje i doporučení americké směrnice NIST, která říká, že heslo by mělo mít kontext jen pro nás. Pokud nebudeme veřejně říkat, jak se naše pejsci jmenují, těžko to bude někdo vědět. Kdybychom se drželi této směrnice, mohli bychom si zvolit za heslo i nějako větu, kterou známe pouze my, např. Babička má nad svou postelí obraz slunečnice. Heslo pak může být: Babickamaslunecninynadposteli. Tuto skutečnost nikdo neví a neví ani, že to máme jako heslo. Pokud pak bude chtít někdo prolomit naše heslo, bude mu to trvat velmi dlouho. Je to v podstatě 27 různých znaků, které se dobře pamatují, než kdyby se jednalo jen o náhodné znaky.

3.5.6 Opakování formou hry

Hra na opakování bude probíhat na motiv známé televizní soutěže AZ kvíz. Popis a pravidla hry jsou přiloženy v příloze.

3.6 Modul pro VI. - IX. třídu

Většina žáků druhého stupně základních škol nemá skoro žádné povědomí o bezpečnosti. Je nutné probrat s nimi úplné základy. Pro ty, kteří se s něčím již setkali nebo mají aspoň nějaké základy bezpečnostního povědomí, to bude opakování, které jistě neublíží.

3.6.1 Seznámení se s náplní výukového modulu

I tuto skupinu dětí nejdřív seznámíme s tím, co budeme probírat. Žáci by měli vědět, co je bezpečnost. Ale pro jistotu je nejdřív můžeme nechat, aby sami zkusili definovat pojmy:

- bezpečnost
- kybernetická bezpečnost

Následně se dostaneme k tomu, že se spolu nebudeme bavit o kybernetické bezpečnosti, protože je to velmi obsáhlé téma na náš kurz, ale budeme řešit, jak se chovat bezpečně v určitých aktivitách, které jistě každý z těchto žáků zná.

Na začátek uděláme základní přehled o aktivitách dětí, podobně jako tomu bylo v předešlé skupině. Zvolíme podobnou formu otázek:

- Víte, co jsou sociální sítě? Jaké znáte? Kolik času trávíte na sociálních sítích?
- Kolik času trávíte sledováním videí na YouTube?
- Kolik času trávíte hraním her na internetu?
- Jak často vyhledáváte informace na internetu?
- Sdílíte často fotografie na sociálních sítích? Případně z jakých aktivit?
- Jak často dáváte nějaké příspěvky (např. z toho co jste dělali) na sociální sítě?

Jako poslední otázku můžeme zvolit:

- Myslíte si, že internet je bezpečné místo? Proč?

Tím se dostaneme k tomu, co budeme vlastně rozebírat, a také k tomu, co dělat, abychom se zbytečně nevystavovali nebezpečí.

3.6.2 Chování na sociálních sítích

Asi nejčastější aktivitou těchto dětí na internetu bude čas strávený na sociálních sítích. Proto se zaměříme na to, jak se na sociálních sítích chovat. Věnovat se budeme hlavně Facebooku, který je momentálně největším fenoménem. Účelem není děti vystrašit nebo znechutit jim využívání sociálních sítí, ale spíš dát základní rady, které je vhodné dodržovat.

Začít můžeme vhodně položenými otázkami, například:

- K čemu Facebook nejčastěji využívají?
- Jaké přínosy vidí v používání Facebooku?

Místo Facebooku se můžeme ptát i na další sociální sítě (TikTok, Instagram, …)

Přátelé, Sledující

Někdy to vypadá, že uživatelé chtějí mít co nejvíce přátel. Nesmíme zapomenout, že tento přístup není úplně nejlepší. Protože s přáteli sdílíme nejčastěji své příspěvky, měli bychom je opravdu znát. Nikdy nevíme, kdo se za daným profilem může skrývat. Proto je vhodné mít na mysli, že žádosti o přátelství posílám pouze těm, které opravdu znám. Totéž platí i o přijímání žádostí. Uživatelé, které neznáme, odmítáme.

Toto je ovšem pouze první část ochrany. Pokud někdo využívá jakékoliv sociální sítě, nesmí zapomínat, že vytvořit si falešný účet není složité. Může za to i nadměrné sdílení osobních informací. Mnozí lidé toho sdílí tolik, že prakticky není problém si najít základní informace a fotografie o dotyčném. Pak už stačí tyto informace využít a

kdokoliv si může udělat účet pod falešnou identitou. Proto musí být všichni obezřetní, a vždy používat svou hlavu, svůj rozum.

Tuto část bychom mohli shrnout do následujících bodů:

- **Není důležité mít co nejvíce přátel**
- **Než se s někým spřátelím na sociálních sítích, musím to pečlivě uvážit.**

Na některých sociálních sítích není možnost přátelství, ale existuje úplně stejná podstata, a to jsou lidé, kteří mě sledují. Pro povolení, aby nás někdo mohl sledovat, platí stejná pravidla, jako pro přijmutí žádosti o přátelství.

Sdílení informací

Z pohledu bezpečnosti uživatelů internetu se jedná asi o nejbolestivější téma. Mnoho lidí sdílí zbytečně mnoho informací a ani si neuvědomují, co všechno se jim díky tomu může stát.

Děti v této věkové skupině si musí osvojit zásady, že by neměly sdílet:

- osobní informace (jméno, rodné číslo)
- bydliště
- telefonní číslo
- e-mail
- informace do které školy chodí, kdy mají jaké kroužky
- intimní fotografie nebo videa
- příliš fotografií nebo videí z domácnosti

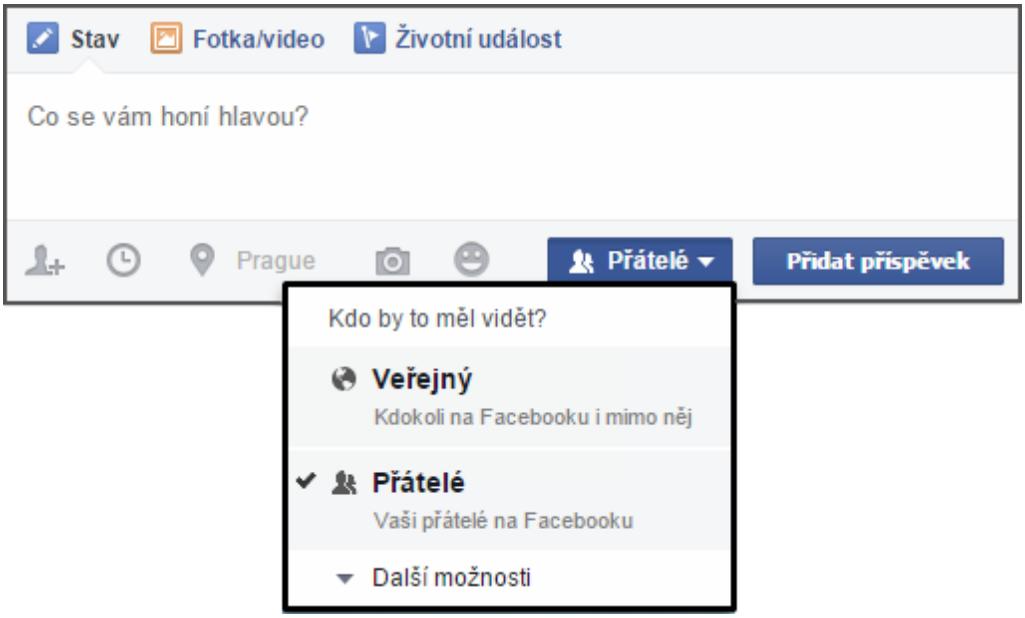
Ti, kteří mají neustálou touhu se o něco na internetu podělit, se mohou zamyslet nad následujícím vtipem:

- *„Protože nemám PC, tak se snažím najít přátele stejným způsobem jako na internetu.*
    - *Každý den chodím ven a vyprávím lidem, co jsem dnes vše jedl, jak se cítím, co jsem dělal předchozí noc a co budu dělat zítra večer.*

- *Pak jim rozdám fotky mé rodiny, mého psa a moje fotky, jak trávím čas na zahradě a v bazénu.*
- *Také poslouchám jejich rozhovory a říkám jim, že je miluji.*

- *A funguje to. Už mám tři přátele.*
  - *Dva policisty.*
  - *A psychiatra"* (18, s.143).

Pokud něco sdílíme na sociálních sítích, je vhodné používat možnost nastavit si, s kým budu příspěvek sdílet. Rozhodně není dobré sdílet příspěvky veřejně, aby každý, kdo si najde náš profil, se k nim dostal. Vhodné je používat možnosti sdílení s konkrétními lidmi či s přáteli. Tím se opět spojuje to, koho máme v přátelích. Ukázku, jak nastavit sdílení příspěvků na Facebooku, vidíme na obrázku. Podobné nastavení je možné i na dalších sociálních sítích.



Obrázek č. 17: Nastavení sdílení u příspěvku na Facebooku (Zdroj: 35)

S kým komunikujeme

Komunikace je důležitá lidská činnost. Bez komunikace bychom nedokázali fungovat. S využíváním internetu je mezilidská komunikace snazší. Můžeme komunikovat v reálném čase, na libovolnou vzdálenost, bez jakéhokoliv zpoždění, stejně, jako kdybychom stáli osobně vedle sebe. Není to jako posílat dopis, kdy čekáme na doručení a případnou odpověď několik dní.

Nebudeme se věnovat způsobu komunikace, ale spíše tomu, s kým komunikujeme. Musíme si uvědomit, že když komunikujeme osobně, vidíme se a mnohdy se známe. Proto musíme být ostražití, když komunikujeme přes internet s někým, koho osobně neznáme. Nikdy nevíme, jaké má cizí člověk záměry. Musíme pečlivě uvažovat, jaké informace mu o sobě podáme.

Hlavně bychom se měli dostat k tématu, které je sice nepříjemné, ale velmi důležité. Tím je zneužívání sociálních sítí k sexuálnímu obtěžování mladistvých. Na konci února 2020 měl v kinech premiéru dokument „V síti“, který se právě zaobírá tímto tématem. Uvedený dokument má dvě varianty. Jedna z nich je dostupná pro děti od 12 let. Nebylo by špatné, aby ty nejstarší děti druhého stupně základní školy viděly zmiňovanou verzi.

Dávat pozor na to, s kým komunikujeme, platí nejen pro sociální sítě, ale pro celý internet. Může se jednat o komunikaci například při hraní on-line her. K rizikům spojených s komunikací se dostaneme v dalších částech.

Tik Tok

Služba Tik Tok se dynamicky rozvíjí. Můžeme zjistit kolik dětí využívá uvedenou síť a jestli jí využívají spíše ke sledování videí, nebo samy sdílejí videa, případně jak často a o čem. Zjistit můžeme, zda pro svůj účet používají své jméno nebo přezdívku. Můžeme se zeptat, kdo si upravil nastavení zveřejněných příspěvků.

Na tuto sociální síť je potřeba dávat pozor především díky výchozímu nastavení, kde je vše veřejné. Proto je důležité si nastavení upravit. Využít můžeme například video: Jak správně nastavit soukromí na Tik Tok na budsafeonline.cz. Vzhledem k tomu, že během výuky nebude dost času, a také nemusí být všechny děti aktivní na této sítí, dáme jim k dispozici odkaz na návod.

- https://www.youtube.com/watch?v=kGw9Yxqhiqc

Pro sdílení videí na Tik Toku platí také pravidla, že bychom neměli zveřejňovat videa, která obsahují nevhodné chování, ubližování, násilí nebo sexuální tématiku. Pozorní musíme být obzvlášť v této době na natáčení v domácnosti. Mnoho uživatelů pořizuje své příspěvky v obývacím pokoji, v koupelně. Uvědomit si musíme, že kromě obsahu

dáváme k dispozici prostor, ve kterém se nacházíme. To může vyvolat nejen závistivé reakce, ale v horším případě také zloděje.

3.6.3 Stahování z internetu

Kromě trávení času na sociálních sítích je další častou aktivitou stahování z internetu. Nemusí se jednat jen o **stahování her a aplikací**, kde musíme sledovat všechna oprávnění, která námi vybraná aplikace či hra požaduje a rozhodnout se, zda budeme souhlasit s udělením oprávnění, ale také o stahování materiálu do školy, např. čtenářský deník, referáty a podobně. Při jakémkoliv stahování si musíme dát pozor, z jakých zdrojů stahujeme. Rizikem je, že si společně stáhneme i nějaký vir. Totéž platí o stahování nelegálních programů nebo her. Proto je vhodné používat vždy legální software. Pro hry platí stejná pravidla. Určitě bychom neměli zapomenout na používání antivirových programů, které poskytují základní ochranu zařízení před škodlivými kódy.

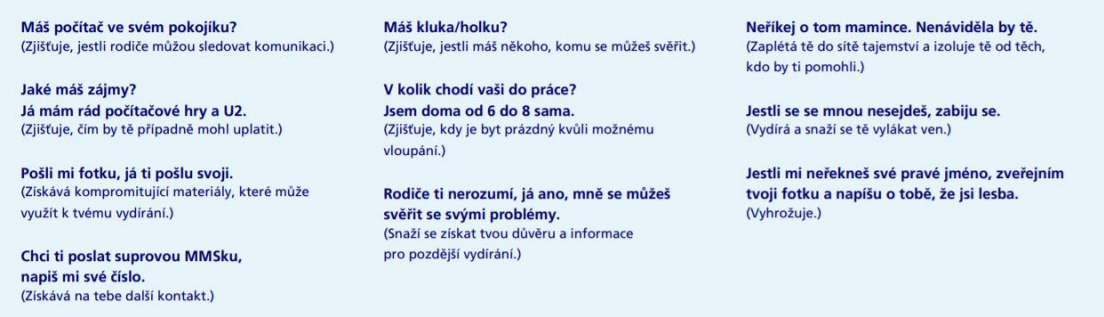
Při stahování musíme pamatovat, že existují **autorská práva**. Nemůžeme libovolně kopírovat cizí díla a vydávat je za své. Autorská práva patří také k filmům, obrázkům nebo písničkám, které mohu použít pro svou potřebu, ale nesmím poskytovat nikomu dalšímu.

3.6.4 Chování na internetu

Pojem kyberšikana všechny děti už slyšely a tuší, co si pod tím představit. U dalších pojmů už tomu tak být nemusí. Proto nejdřív probereme, znají-li přednášené pojmy, případně je vysvětlíme:

- kyberšikana
- kybergrooming
- kyberstalking
- sexting

Obrana proti kybergroomerům spočívá především v tom, že musíme být opatrní, s kým komunikujeme. Útočník bude mít zajímavý profil mladé osoby. Určitě bychom měli zbystřit, pokud se nás někdo začne vyptávat na podobné otázky, které jsou na následujícím obrázku.



Obrázek č. 18: Podezřelá komunikace nových přátel (Zdroj: 36)

Rady, jak se bránit proti kyberstalingu jsme už v podstatě probírali. Jedná se především o to, co dobrovolně sdílíme především na sociálních sítích. Pokud se staneme obětí některého z druhů chování, nesmíme smazat zprávy, které by mohly posloužit jako důkazy. Pokud je to možné, útočníka bychom měli zablokovat.

Stejně jako s mladšími dětmi je vhodné probrat i tématiku **online výzev**.

Fake-news, hoax

Kromě představení těchto praktik se především musíme naučit, jak se proti nim bránit.

Bránit se proti podvodným informacím není nejjednodušší, protože nám zabere určitý čas. Prvním předpokladem je, že vždy musíme myslet na to, že ne vše je pravda. Určitě každé dítě někdy lhalo nebo si poupravilo, co říkalo. To se děje z různých důvodů. Dalšími důležitými aspekty před obranou proti falešným zprávám je, že si musíme přečíst celý článek. Mnoho lidí si čte pouze titulky, které se často díky tomu tvoří, aby byly poutavé a které jsou někdy až zavádějící. Zamyslet se musíme nad tím, jestli jsou informace z článků reálné. Získané informace si pak musíme ověřit u dalších zdrojů.

Dnes je možné ověření pravosti obrázků, případně jestli se neobjevoval v jiném článku s odlišným kontextem. Využít můžeme například www.tineye.com nebo vyhledávání obrázků pomocí Google.

Stránky hoax.cz nebo manipulatori.cz obsahují databázi známých falešných zpráv. Můžeme ověřit, zda nejde už o vyvrácené nepravdivé informace. Kroky, jak se bránit proti těmto zprávám si můžeme snadněji zapamatovat díky následujícímu obrázku.

Obrázek č. 19: Jak si ověřit informace (Zdroj: 37)

Spam a phishing

Phishing

Dříve byly phishingové útoky rozpoznatelné díky špatné gramatice nebo překlepům, které se v nich objevovaly. Dnes se provedení zpráv zlepšilo natolik, že se chyby objevují v mnohem menší míře. Každopádně je důležité pamatovat, že z neznámého e-mailu neklikejme na žádné odkazy. Pokud už ze zprávy klikneme na odkaz, nejlepší ochrana pak je, se vždy podívat do adresního řádku prohlížeče. I když podvržené stránky budou naprosto stejné jako pravé stránky, adresa se nebude shodovat.

Spam

Proti praktikám spamových útoků se můžeme bránit tak, že budeme ohleduplní, především ke zprávám z neznámých adres. Dalším znakem může být nepřesná čeština. Z těchto zpráv se nesmí nic stahovat, žádné přílohy a ani klikat na přiložené odkazy. Takovou zprávu můžeme nahlásit jako spam. Důležité je si uvědomit, pokud nám přijde e-mail s informacemi, že se máme přihlásit k určité službě za nějakým účelem, neklikejme na uvedený odkaz. Je lepší si do adresního řádku napsat adresu a přihlásit se pomocí pravých stránek.

Příklad: Dojde nám e-mail od banky, že se máme přihlásit kvůli změně nastavení. Uvnitř zprávy bude také odkaz. V žádném případě nesmíme kliknout na odkaz. Vždy raději pomocí webových prohlížečů vyhledejme stránky naší banky.

Pokud nám dojde zpráva, která se nám zdá podivná, můžeme si na internetu vyhledat, jestli se nejedná o podvodnou zprávu. To můžeme například na stránkách hoax.cz/phishing, kde můžeme zkontrolovat, zda se nejedná o už známý podvodný trik.

3.6.5 Ochrana zařízení a hesla

Nesmíme zapomenout také na to, že děti by mimo to, jak se chovat na internetu, měly vědět, jak chránit svá zařízení. Znát by měly, co je antivirový program a proč ho mají využívat. Pro správnou ochranu je důležité používat legální a aktualizovaný software. V neposlední řadě musíme zmínit účty a oprávnění na počítači. Pokud počítač využívá více lidí, každý by k němu měl mít svůj účet opatřený heslem. Nastavit můžeme i typ účtů. Pro běžnou činnost bychom nikdy neměli používat účet administrátora. Vhodné je provádět pravidelné zálohy dat uložených na počítači. Tím zajistíme, že budeme mít zachovaná důležitá data v případě, že by došlo k jejich smazaní, zablokování nebo poruše zařízení.

Důležité je zmínit problematiku hesel. Jak by heslo nemělo nikdy vypadat a naopak, jak si vytvořit kvalitní heslo.

3.6.6 Veřejná Wi-Fi a veřejný PC

Dětí se můžeme zeptat na následující otázky, abychom zjistili, jestli veřejné sítě nebo počítače využívají. Protože skoro každé dítě využívá veřejnou Wi-Fi, můžeme je nechat zamyslet se, jestli to přináší některá nebezpečí. Využijeme tyto otázky:

- Jak často využíváte veřejnou Wi-Fi?
- Jaké aktivity na nich provádíte?
- Můžou být tyto sítě nebezpečné? Jestli ano, dokázali byste říct čím?
- Co si představíte pod pojmem veřejný počítač?
- Využíváte ho někdy? Myslíte, že má nějaká pravidla používání?

Bezdrátovou síť můžeme rozdělit na více skupin podle toho, kde je provozována a kdo má k ní přístup. Může se jednat o domácí, školní, firemní či veřejnou síť. První tři typy sítě by měly mít nastavené zabezpečení, především, aby se k nim nemohl připojovat kdokoliv. Problémem však jsou veřejné sítě. K těm se může přihlásit kdokoliv. Protože jsou veřejné sítě zadarmo, jsou velmi oblíbené. Málokdo si však uvědomuje rizika spojená s přihlašováním do veřejných sítích.

Problémem je, že stejně jako se přihlásíme k veřejné síti my, tak se k nim může přihlásit i útočník. Útočníci umí odposlouchávat data, která putují mezi zařízením a přístupovým bodem, který vysílá Wi-Fi signál. A získaná data mohou zneužít.

Druhou možností je, že útočník vytvoří veřejnou síť, kterou pojmenuje podle potřeby. Není problém vytvořit síť, která se bude jmenovat škola nebo ponese jméno restaurace. Na těchto sítích je ještě snadnější pro útočníky získat osobní informace.

Ochrana proti zneužití veřejné sítě je taková, že bychom neměli tyto sítě vůbec **používat**. Jako ochranu sice lze využít službu VPN, která nám zabezpečí komunikaci mezi dvěma uzly. Nevýhodou je, že bezpečné služby jsou placené. Ty zdarma bychom také neměli využívat, protože proč by nám někdo dával něco zadarmo… Vhodné doporučení je, že bychom na svém zařízení měli **vypnout automatické přihlašování k Wi-Fi.** Pokud už využíváme veřejné sítě, musíme pečlivě uvažovat nad aktivitami, které provádíme. Není určitě vhodné, abychom se přihlašovali do bankovnictví, ale i do dalších služeb, pokud nechceme, aby nám někdo odcizil přihlašovací údaje.

Veřejný počítač – pod tímto pojmem si můžeme představit počítač, který může být v knihovně, ale i v některých školách a na dalších místech. Jde o to, že uživatelé nemají vlastní účet, pomocí kterého se přihlašují. Když budeme používat takový počítač, musíme na internetu používat následující opatření:

- neukládat přihlašovací údaje v prohlížeči
- přihlásíme-li se, musíme se i odhlásit
- používejme anonymní režim nebo smažme údaje o prohlížení, nikdo tak neuvidí, co jsme navštívili

Pokud vytvoříme nebo stáhneme fotografie, videa, soubory, musíme je smazat. Další uživatel by se pak k nim mohl snadno dostat.

3.7 Pokračování budování bezpečnostního povědomí

Aby bylo budování bezpečnostního povědomí efektivní, nesmíme zapomenout, že se jedná o opakující se proces. Proto by bylo vhodné, aby na každé škole probíhalo podobné vzdělávání o bezpečnosti alespoň jedenkrát ročně. Díky tomu se postupně žáci dozví další a další informace a než opustí docházku základního vzdělávání, mohli by mít slušný základ o informační a kybernetické bezpečnosti.

Kromě vyučování těchto modulů lze u dětí zvyšovat povědomí i jinými aktivitami. Jednat se může například o osobní angažovanost některého vyučujícího, který se dobrovolně bude občas věnovat tomuto tématu, případně využití nástěnek ať už ve třídách nebo na chodbách. Pro tyto aktivity je vhodné využít některého z nepřeberného množství materiálu na internetu. Na ukázku přikládám některé projekty, ze kterých lze čerpat užitečné informace.

3.7.1 O2 chytrá škola

Na stránkách www.o2chytraskola.cz se lze dozvědět spoustu zajímavých informací. Některá témata, např. kyberšikana, rizikové výzvy apod. přímo poskytují rady a tipy pro učitele, jak poznat možné nebezpečné chování a jak se v takových případech zachovat. Dále v rámci projektu mimo jiné najdeme:

- metodické náměty na výukové aktivity spojené z bezpečností
- informační listy, které lze vyvěsit na nástěnku
- krátká videa, ve kterých je vysvětlení daného tématu

3.7.2 E-Bezpečí

Na stránkách projektu e-bezpeci.cz se nachází několik tiskovin pro učitele, včetně metodických návrhů, které byly vytvořeny pro projekt O2 Chytrá škola. Dále zde najdeme výzkumné zprávy, které se týkají bezpečnosti na internetu, odborné studie, monografie, DVD materiály, skládačky nebo přehledové listy, které jsou vhodné pro vložení na nástěnky.

3.7.3 Digitální stopa

NÚKIB, CZ.NIC a Kabinet informačních studií a knihovnictví na Masarykově univerzitě spustili projekt nazvaný digitální stopa, který je zaměřen na žáky pátého a šestého ročníku základní školy. Tento interaktivní kurz mohou žáci projít sami nebo s lektorem. Pro lektory (učitele) jsou k dispozici různé materiály pro větší efektivnost výuky.

3.7.4 Film V SÍTI

Filmové zpracování pojednává o sexuálním zneužívání dětí na internetu. Verze filmu „V SÍTI: Za školou“, je přístupná od dvanácti let, a to i bez doprovodu dospělé osoby. Každopádně v rámci seznámení dětí s riziky komunikace na internetu, hlavně prostřednictvím sociálních sítí, by nebylo od věci, aby tento film žáci starší 12 let viděli.

3.7.5 Přínosy práce

Hlavní přínos této práce je zvýšení bezpečnostního povědomí u žáků vybraných základních škol. Nezabývá se metodickými postupy, jak by měl program budování bezpečnostního povědomí vypadat, ale přináší konkrétní náplně vyučovacích modulů, které jsou vybrané podle technologií a aktivit se kterými přichází žáci základních škol do kontaktu. Kromě návrhů je největší přidaná hodnota této práce v tom, že s pomocí výuky došlo k opravdovému budování povědomí v oblasti informační a kybernetické bezpečnosti.

Díky tomu má práce největší přínos pro zúčastněné žáky, kteří mohli získat základy bezpečnosti. Seznámili se s riziky, která na ně mohou číhat v prostředí internetu nebo při využívání ICT. Důležitým přínosem kromě jiného bylo i téma politiky hesel, především jak vytvořit kvalitní a bezpečné heslo. Tuto část práce určitě využijí všichni žáci, protože hesla využívá každý uživatel v kyberprostoru a jsou jednou z nejdůležitějších částí v bezpečnosti. V neposlední řadě měla tato práce přínos i pro třídní učitele. Pro některé z nich byla účast přínosná a sami si odnesli nové informace pro svůj profesní i osobní život.

3.7.6 Výuka navržených modulů

Praktické plnění této diplomové práce bylo ovlivněno pandemií koronaviru, díky které nemohly být moduly odučeny v plánovaném rozsahu. Výuka se uskutečnila pouze v rámci základní školy Těšany.

Tabulka č. 3: ZŠ Těšany - plán výuky (Zdroj: Vlastní zpracování)

Třída	Datum	Stav
I.	6. 3. 2020	Proběhla
II.	6. 3. 2020	Proběhla
III.	11. 3. 2020	Neproběhla
IV.	11. 3. 2020	Neproběhla
V.	13. 3. 2020	Neproběhla
VI.	10. 3. 2020	Proběhla
VII.	10. 3. 2020	Proběhla
VIII.	18. 3. 2020	Neproběhla
IX.	18. 3. 2020	Neproběhla

Tabulka č. 4: ZŠ Těšany - výuka a její zhodnocení (Zdroj: Vlastní zpracování)

Třída	Datum	Vyhodnocení
I.	6. 3. 2020	Výuka s nejmenšími byla velmi pozitivní. Většina dětí se nebála komunikovat a pokládat různé otázky. Rozdíl mezi jednotlivými dětmi ve znalostech technologií byl výrazný. Proto musela být výuka postavena tak, aby předkládané informace pochopili i žáci s nejmenšími dosavadními znalostmi. Získané informace děti projevily v závěrečné hře. Z nedostatku času jsme nestihli probrat, jak by bylo správné se v situaci zachovat.
II.	6. 3. 2020	Druhá třída nebyla ze začátku tak komunikativní jako první. V průběhu výuky se však děti osmělily a více se zapojovaly do komunikace. Skupina prokázala větší znalosti probíraných technologií, proto jsme se mohli věnovat více rizikům a bezpečnostním radám. Na konci zbylo více času na test, který žáci vypracovali samostatně. Při kontrole projevili, že pochopili vzdělávací modul a většina měla vše dobře. U špatně řešených situací jsme probrali, jak se správně zachovat.
VI.	10. 3. 2020	Ze začátku byla třída ostýchavá, v průběhu se však začala zapojovat do diskuse a přidávat otázky. Nejvíc času jsme se věnovali, proč je důležité přemýšlet o přátelích a sledujících na různých sociálních sítích a jak vhodně sdílet příspěvky. Velký zájem přinesla část věnovaná heslům. Z časových důvodů jsme přehodily závěrečná témata a věnovali se nejdřív veřejným Wi-Fi a veřejnému PC. Z toho důvodu nám nezbylo moc času a nestihli jsme pořádně probrat téma spamu, phishingu a hoaxu.
VII.	10. 3. 2020	Při výuce jsme s žáky sedmé třídy prošli všechny navrhované části. Oblast kyberšikany byla pro třídu rychlým opakováním. O to více jsme debatovali nad tématy využívání veřejných Wi-Fi, přátelé a sledující na sociálních sítích a Tik Tok a jeho využívání, včetně nastavení.

ZÁVĚR

Cílem diplomové práce bylo vytvořit vzdělávací moduly pro žáky základních škol, které budou sloužit ke zvyšování bezpečnostního povědomí. Práce je rozdělená do tří hlavních částí. V první z nich se zabývá teoretickými východisky, ve kterých popisuje pojmy a definice, které jsou nezbytné pro správné pochopení návrhu řešení. Druhá část se zabývá problematikou, proč budovat povědomí o informační a kybernetické bezpečnosti na základních školách. Kromě toho tato část popisuje, jak bude probíhat celý program. Nejdůležitější částí druhé hlavní kapitoly je rozdělení žáků do jednotlivých skupin a stanovení hlavních požadavků, které mají výukové moduly obsahovat. Tyto požadavky byly konzultovány se zástupci vybraných škol.

Nejdůležitější částí je návrh řešení, ve kterém probíhá přesný popis a náplň vzdělávacích modulů, včetně problematiky, jak by měla výuka probíhat. Kromě vlastních návrhů se této části týká samostatná implementace. Ta je úzce spojená s první částí teoretická východiska. Součástí vlastního řešení byla výuka navržených modulů na vybrané základní škole. Výuka byla největším přínosem předkládané práce, protože díky ní došlo ke zvýšení bezpečnostního povědomí u žáků, kteří se vzdělávacích modulů účastnili.

Výuka byla zásadně ovlivněna nečekanou pandemií koronaviru, se kterou souvisí nařízení vlády ze dne 10. 3. 2020, které od 11. 3. 2020 až do odvolání ruší výuku na základních školách. Díky této nečekané situaci nemohlo dojít k implementaci práce v takovém rozsahu, jak bylo plánováno. Výuka tak proběhla pouze v rámci jedné z těchto škol, a to pouze v rozsahu vyučovacích modulů zaměřených pro I. – III. třídu a pro VI. – IX. třídu. Zbytek z plánovaného rozsahu implementace této diplomové práce proběhne, v případě zájmu ze strany škol, až po zrušení opatření, podle kterého jsou školy uzavřeny.

Výuka na jedné škole však částečně proběhla. Ohlasy na vzdělávací aktivity byly pozitivní jak ze strany žáků, tak ze strany pedagogů. Edukace proběhla v rámci několika tříd. Pozitivní bylo vzdělávání těch nejmenších dětí navštěvující první třídu. Tyto děti se teprve učí číst, psát, počítat a další základy, proto se muselo vyučování přizpůsobit jejich dovednostem a chápání. Část vyučování proběhlo při sezení na koberci před

dataprojektorem, na kterém se promítala prezentace s obrázky z pexesa, které děti hrály. K obrázkům, kde poznávaly zařízení, probíhala i debata, k čemu se využívá, případně na co si dát pozor. Na těchto dětech bylo znát, že některé jsou více seznámeny s různými zařízeními a jiné se v nich příliš nevyznají. Také využívání technologií je u každého žáka na odlišné úrovni. Některé děti už byly schopny reagovat i na otázky, jestli je vhodné takové chováni či nikoliv. Dokonce část dětí byla velice komunikativní a sama se vyptávala na různé informace, které je zajímaly. V rámci hry na opakování, kterou jsme procházeli společně a hlasovali o výsledku, děti prokázaly, že pochopily probíranou tématiku a uměly se správně rozhodnout, jestli je situace, chování, správné nebo špatné.

Ve druhé třídě probíhala výuka vzdělávacího modulu velmi podobně. Rozdíl spočíval v tom, že většina účastníků znala probíraná zařízení. Zde se také prokázala odlišnost využívání. Zatímco někteří mají mobilní telefon, jiní ještě ne. Část z nich si může sama stahovat aplikace do telefonu, ostatní k tomu potřebují souhlas odpovědné osoby. Většina využívá počítač pouze pod dohledem rodičů. Výjimky už ho využívají samy bez přítomnosti a stálého dohledu. Zapomenout nesmíme také na ty, kteří dané technologie z různých důvodů nevyužívají vůbec. Část druháků prokázala, že již některé minimální informace ze základů bezpečnosti má. Dokážou říct k čemu je heslo, slyšeli že existují počítačové viry, které napadají počítač, a taky, že na internetu se mohou setkat s nevhodným chováním. To je důsledkem toho, že někteří rodiče si uvědomují potřebu bezpečnosti a rozebírají se svými dětmi i rizika, která přináší kyberprostor. V rámci výuky padlo i více zvídavých dotazů, například „Jak se počítačový vir dostane do počítače?“ nebo otázka, která mě zaujala: „Je možné, že nás někdo sleduje přes kameru?“ V rámci hry na konci, kterou už tyto děti vypracovávaly samy, prokázaly, že pochopily probíranou tématiku a správně rozhodovaly o daných situacích.

Žáky obou tříd tyto vzdělávací moduly zaujaly. Důsledkem bylo, že při setkání během dalších návštěv školy chtěli, abych zase přišel a probíral s nimi další zajímavé informace. Kromě toho při vypracování hry na opakování prokázali, že pochopili probíraná témata a vyznají se v oblastech v míře, která byla od nich požadována při sestavování témat vzdělávacích modulů. Tím došlo ke splnění dílčího cíle, kterým bylo seznámit děti s požadovanými oblastmi.

V rámci modulu pro VI. – IX. třídu se žáci daných tříd nejdříve seznámili s náplní. Z této skupiny je většina účastníků aktivní na sociálních sítích. Velké množství z nich ví o nebezpečích, která jsou spojena s využíváním internetu, ale neřeší je. K problematice přistupují stylem „mě se přeci nemůže nic stát, a tak mě to nezajímá“. Zajímavá byla debata o přátelství nebo sledujících na sociálních sítích. Spousta uživatelů bere tyto počty spíš jako důkaz oblíbenosti či zajímavosti. Podobné je tomu u sdílení, tam někteří berou sdílení příspěvků ve stylu „proč bych se nepochlubil, neukázal kamarádům“. Proto nezbývá než doufat, že díky ukázkám příkladů budou více rozmýšlet, jak se na sociálních sítích, potažmo celém internetu chovat. Co se týče různých aplikací nainstalovaných v telefonu se rozmezí pohybovalo od jednotek až přes desítku. Téměř nikdo se ale nezajímal o to, jaká oprávnění aplikace vyžadují a k čemu mají přístup. Zajímavostí byl uvedený průzkum, který vedl k prozkoumání nainstalovaných aplikací a jejich oprávnění. Kyberšikanu a další typy nevhodného chování žáci této školy díky předešlým vzdělávacím aktivitám znali, proto tato část byla rychlým opakováním, které jistě nikomu neublížilo. Největší diskuse probíhala nad tématy veřejných Wi-Fi a částí zabývající se hesly, hlavně jejich tvoření. Veřejné Wi-Fi využívá každý a nikdo si neuvědomuje rizika s nimi spojená. Část uživatelů dokonce má neustále aktivní nastavení automatického připojování k Wi-Fi sítím. Je jasné, že v rámci jednoho dvouhodinového školení se kompletně přístup k problematice bezpečnosti nezmění. Bylo by vhodné, aby se různými způsoby připomínala i nadále.

V rámci návrhu řešení jsou přiloženy i možné způsoby a náměty, jak dále připomínat a zvyšovat bezpečnostní povědomí u žáků základních škol.

SEZNAM POUŽITÝCH ZDROJŮ

1) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

2) Základní příručka k ochraně údajů. Úřad pro ochranu osobních údajů. uooz.cz [online]. ©2013 [cit. 2020-04-23]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-ochrane-udaju/ds-4744/archiv=0&p1=3938

3) KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

4) NIST SP 800-63B. Digital Identity Guidelines. Authentication and Lifecycle Management. National Institute of Standards and Technology, 2017.

5) Informace: význam. IT Slovník: Počítačový slovník [online]. IT-Slovnik.cz team, ©2008-2020 [cit. 2020-03-26]. Dostupné z: https://it-slovnik.cz/pojem/informace

6) DOUCEK, Petr, Luděk NOVÁK a Vlasta SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 978-808-6946-887.

7) Správa a řízení internetu. CZ.NIC. jaknainternet.cz [online]. ©2020 [cit. 2020-03-29]. Dostupné z: https://www.jaknainternet.cz/page/1703/sprava-a-rizeni-internetu/

8) Počítačové viry, červi a trojské koně. Internetem bezpečně. Internetembezpecne.cz [online]. ©2018 [cit. 2020-03-29]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/virus/

9) Co to je malware. Internetem bezpečně. Internetembezpecne.cz [online]. ©2018 [cit. 2020-03-29]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/co-to-je-malware/

10) Kybernetická šikana. O2 Chytrá škola. o2chytraskola [online]. ©2020 [cit. 2020-03-30]. Dostupné z: https://www.o2chytraskola.cz/clanek/7/kyberneticka-sikana/

11) Jak kyberšikana probíhá. O2 Chytrá škola. o2chytraskola [online]. ©2020 [cit. 2020-03-30]. Dostupné z: https://www.o2chytraskola.cz/clanek/7/kybernetická-sikana/4317

12) KOPECKÝ, Kamil a Veronika KREJČÍ. Rizika virtuální komunikace (příručka pro učitele a rodiče). [online]. NET UNIVERSITY, Olomouc, 2010. [cit. 2020-03-31] ISBN 978-80-254-7866-O. Dostupné z: https://www.zsmalse.cz/phprs/storage/enebezpeci_a5_3.pdf

13) Kybergrooming. Internetem bezpečně. Internetembezpecne.cz [online]. ©2018 [cit. 2020-03-31]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybergrooming/

14) Online challenges (rizikové výzvy). O2 Chytrá škola. o2chytraskola [online]. ©2020 [cit. 2020-04-18]. Dostupné z: https://www.o2chytraskola.cz/clanek/39/online-challenges-rizikove-vyzvy/

15) Falešné profily. Bezpečně v kyberprostoru. Bezpecnevkyberprostoru [online]. ©2020 eStránky.cz [cit. 2020-04-20]. Dostupné z: https://bezpecnevkyberprostoru.cz/clanky/rizika/falesne-profily/

16) NUTIL, Petr. Média, lži a příliš rychlý mozek: průvodce postpravdivým světem. Praha: Grada, 2018. ISBN 978-80-271-0716-2.

17) Computer Scientists' App Measures Our Online Footprints, communications of the ACM, cacm.acm.org © 2015 Information Inc., Bethesda, Maryland, USA [cit. 2020-04-21]. Dostupné z: https://cacm.acm.org/news/183567-computer-scientists-app-measures-our-online-footprints/fulltext?mobile=true?mobile=false

18) KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

19) KOPECKÝ, Kamil. Problém zvaný TikTok. In: E-bezpečí [online]. ©2008–2020 [cit. 2020-04-21]. Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/socialni-site/1403-problem-zvany-tik-tok

20) Autorská práva. CZ.NIC. jaknainternet.cz [online]. ©2020 [cit. 2020-04-22]. Dostupné z: https://www.jaknainternet.cz/page/1191/autorska-prava/

21) NIST SP 800-16. Information Security: A Role-Based Model for Federal Information Technology/ Cyber Security Training. Revision 1 (2nd Draft Version 2). Gaithersburg: National Institute of Standards and Technology, 2013.

22) NIST SP 800-50. Computer Security: Building an Information Technology Security Awareness and Training Program. Gaithersburg: National Institute of Standards and Technology, 2003.

23) TÝDEN. Tyden. *tyden.cz* [online]. ©2006-2020 [cit. 2020-04-27]. Dostupné z: https://www.tyden.cz/rubriky/veda/technologie/internetove-prohlizece-v-cr-google-chrome-prilis-nezaujal_90181.html

24) PCDAYS. PCdays. *pcdays.cz* [online]. [cit. 2020-04-27]. Dostupné z: https://www.pcdays.cz/2012/03/vetsina-lidi-na-internetu-neumi-hledat/

25) ANTIVIROVÉ CENTRUM. Antiviroveventrum. antivirovecentrum.cz [online]. ©1998-2020 Amenit s.r.o [cit. 2020-04-27]. Dostupné z: https://www.antivirovecentrum.cz/akcni-nabidka.aspx

26) COMODO ANTIVIRUS. Comodoantivirus. antivirus.comodo.com [online]. ©2020 [cit. 2019-12-30]. Dostupné z: https://antivirus.comodo.com/blog/comodo-news/how-to-get-rid-of-a-virus/

27) NOVINKY. Novinky. *Novinky.cz* [online]. [cit. 2019-12-30]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/podvodnici-zkouseji-novy-trik-duverivce-lakaji-na-atraktivni-vyhry-40017984

28) SEMAFOR „BEZPEČNĚ NA YOUTUBE“ Národní úřad pro kybernetickou a informační bezpečnost. Nukib.cz [online]. [cit. 2020-04-27]. Dostupné z: https://www.nukib.cz/download/vzdelavani/hry/Hra_Bezpecne_Youtube.pdf

29) Další informace. Anglicko-český offline slovník. play.google.com. [online]. ©2020 Google [cit. 2020-04-27]. Dostupné z: https://play.google.com/store/apps/details?id=com.dic_o.dico_cze_eng

30) VÁCLAVÍK, Lukáš. Avast zkontroloval „svítilny pro Android“. Výsledky jsou děsivé. Cnews.cz. [online]. ©2020 Mladá fronta a.s. [cit. 2020-04-27]. Dostupné z: https://www.cnews.cz/avast-svitilny-flashlight-android-analyza

31) Online Challenges – infolist. O2 Chytrá škola. o2chytraskola [online]. ©2020 [cit. 2020-04-18]. Dostupné z: https://o2chytraskola.cz/data/files/infolist-rizikove-vyzvy-2txoqacr51.pdf

32) Buď v bezpečí – hoax. E-bezpečí. e-bezpeci.cz [online]. © 2008-2020 [cit. 2020-04-28]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/tiskoviny/bud-v-bezpeci/90-bud-v-bezpeci-hoax/file

33) Co je kyberšikana. O2 Chytrá škola. o2chytraskola [online]. ©2020 [cit. 2020-04-18]. Dostupné z: https://www.o2chytraskola.cz/test/4/7

34) Bezpečné heslo – infolist. O2 Chytrá škola. o2chytraskola [online]. ©2020 [cit. 2020-04-18]. Dostupné z: https://www.o2chytraskola.cz/data/files/infolist-bezpecne-heslo-2oe6lzev6f.pdf

35) KALAŠOVÁ, Dominika. Pozor na nové podvodné výzvy k nastavení soukromí na Facebooku. In: blog.avast.com [online]. ©1988-2020 Avast Software s.r.o [cit. 2020-04-28]. Dostupné z: https://blog.avast.com/cs/2015/01/15/pozor-na-nove-podvodne-vyzvy-k-nastaveni-soukromi-na-facebooku/

36) Kyberstalking, kybergrooming - infolist. O2 Chytrá škola. o2chytraskola [online]. ©2020 [cit. 2020-04-18]. Dostupné z: https://o2chytraskola.cz/data/files/v002-o2-infolist-kyberstalking-kybergrooming-a4-v03-nahled-r60xokvyph.pdf

37) Pravda a lež na internetu, metodické náměty na výukové aktivity. O2 Chytrá škola. o2chytraskola [online]. ©2020 [cit. 2020-04-18]. Dostupné z: https://www.o2chytraskola.cz/data/files/v003-o2-fake-news-list-metodika-digital-a4-v06-nahled-a3sinf9dt5.pdf

38) Technika kolem nás. Národní úřad pro kybernetickou a informační bezpečnost. Nukib.cz [online]. [cit. 2020-02-15]. Dostupné z: https://www.nukib.cz/download/vzdelavani/hry/technika_kolem_nas.pdf

39) Connect IT CKB-3010-CS bezdrátová klávesnice, bílá. TSBohemia.cz [online]. ©2020 CyberSoft s. r. o. [cit. 2020-02-15]. Dostupné z: https://www.tsbohemia.cz/connect-it-ckb-3010-cs-bezdratova-klavesnice-bila_d274516.html

40) Lenovo TAB M10 Plus, 4GB/64GB, Iron Grey. CZC. czc.cz [online]. [cit. 2020-02-15]. Dostupné z: https://www.czc.cz/lenovo-tab-m10-plus-4gb-64gb-iron-grey/279348/produkt

41) Obrazek. CZC. czc.cz [online]. [cit. 2020-02-15]. Dostupné z: https://iczc.cz/cep9sdnnb4irbborru90h08og9-1_7/obrazek

42) MARKETING NA SOCIÁLNÍCH SÍTÍCH, SPRÁVA PROFILŮ A REKLAMNÍCH KAMPANÍ. SEO Web. Seoweb.cz. [online]. [cit. 2020-02-15]. Dostupné z: https://www.seowebu.cz/socialni-site-sprava-uctu-a-reklamy/

43) Chytré hodinky Xiaomi Amazfit GTS černé (A1914-OB). Datart. datart.cz [online]. © 2020 HP TRONIC Zlín, spol. s r.o. [cit. 2020-02-15]. Dostupné z: https://www.datart.cz/chytre-hodinky-xiaomi-amazfit-gts-obsidian-black-a1914-ob.html

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

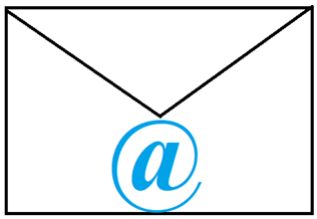
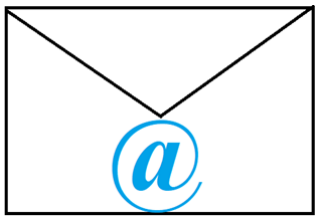
ICT	Informační a komunikační technologie
IS	Informační systém
DDoS	Distributed denial of service
IoT	Internet of Things
OS	Operační systém
ČR	Česká republika
ZŠ	Základní škola
HW	Hardware
SW	Software
GDPR	General Data Protection Regulation
NUKIB	Národní úřad pro kybernetickou a informační bezpečnost
ČSN	České technické normy

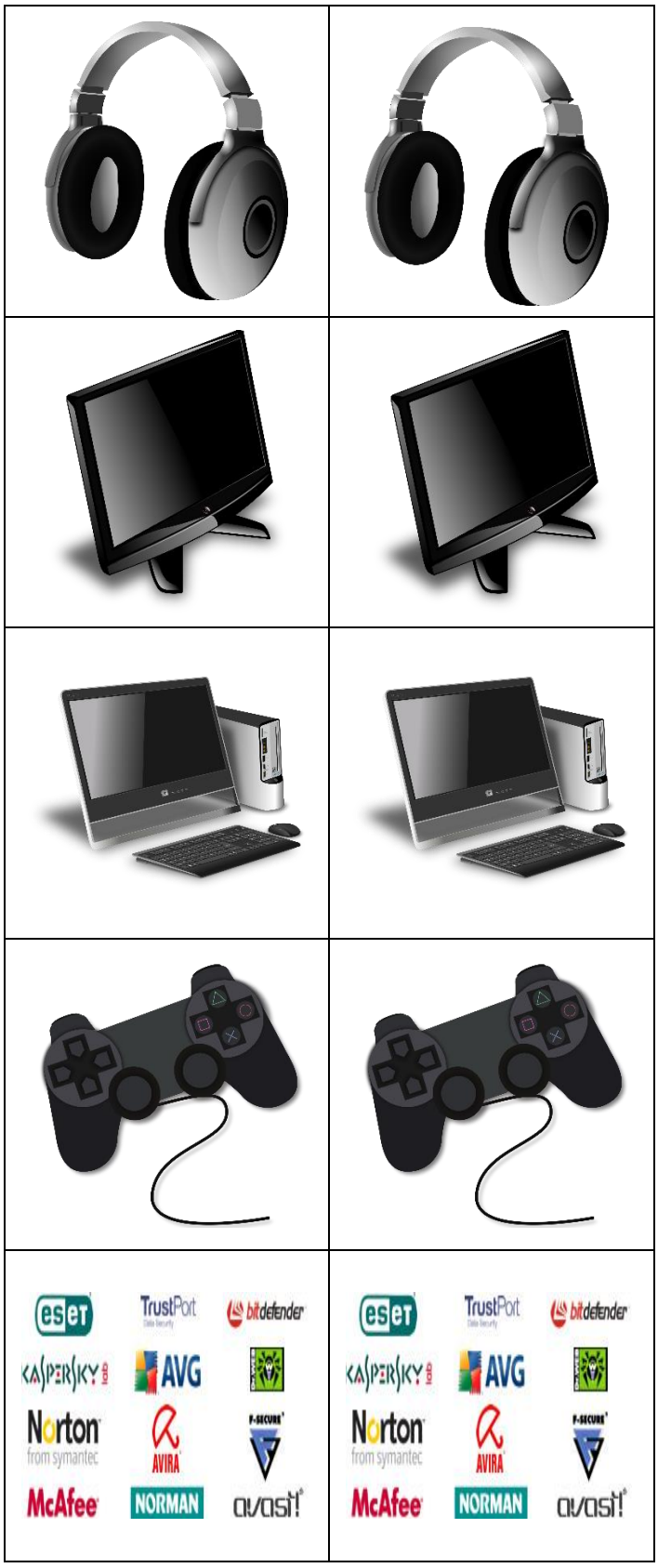
SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Příloha 1: Pexeso (Zdroj: Vlastní zpracování dle 23, 24, 25, 38, 39, 40, 41, 42, 43)

<table>
<tr><td>  </td><td>  </td></tr>
<tr><td>  </td><td>  </td></tr>
<tr><td>  </td><td>  </td></tr>
<tr><td>  </td><td>  </td></tr>
<tr><td>  </td><td>  </td></tr>
</table>


eset
TrustPort
bitdefender
KASPERSKY
AVG
Norton
from symantec
AVIRA
F-SECURE
McAfee
NORMAN
avast!


12:26
08/09
10°/15°
12:26
08/09
10°/15°

Příloha 2: Šablona pro vyplnění hry (Zdroj: Vlastní zpracování dle 28)

Moji kamarádi vymysleli novou hru, která se jmenuje „Na šneky“. Při této hře se rozběhnete a jedním skokem rozšlápnete šnečí ulitu. Holky říkají, že je to nechutné a týrání zvířat, ale pro nás kluky je to velká zábava, a proto natočím video, aby se pobavili i ostatní.	
Na každém počítači by mělo být heslo pro přihlášení.	
Používat antivirový program je zbytečné a nepomůže nám.	
Když chceme hrát hru na počítači nebo telefonu, zeptáme se rodičů.	
Potkám na ulici někoho, koho neznám. On bude chtít, abych mu dal své telefonní číslo. Já mu své číslo dám.	
Vyfotím svého kamaráda, a ten na fotce vypadá směšně. On bude chtít, abych fotku smazal. Ale já ji budu ukazovat ostatním a smát se mu.	
Jdu na kroužek, a aby mi cesta rychle utekla, nasadím si sluchátka a budu po cestě poslouchat muziku.	

Začnou mi chodit zprávy, kde mě bude někdo napadat, vyhrožovat nebo urážet. Nahlásím tyto informace rodičům.	
Najdu si novou hru a chci si ji zahrát. Ptát se rodičů, jestli si jí můžu stáhnout je zbytečné, protože se mi nemůže nic stát.	
Na internetu píšou články různí lidé, proto nesmím věřit všemu, co si přečtu, a také dělat vše, co mě někdo radí.	
Při hraní her na mě vyskočí stránka, že jsem vyhrál. Mám vyplnit nějaké informace. Chci vyhrát, a tak vyplním své jméno, příjmení, bydliště a další informace.	
Jdu do školy a najdu na zemi USB flash disk. Jsem zvědavý, co je na něm, a tak ho vložím do počítače, abych to zjistil.	
Jsem v pokoji se svým sourozencem. Ten se chce učit a já poslouchat hudbu. Abych ho nerušil, použiji sluchátka.	

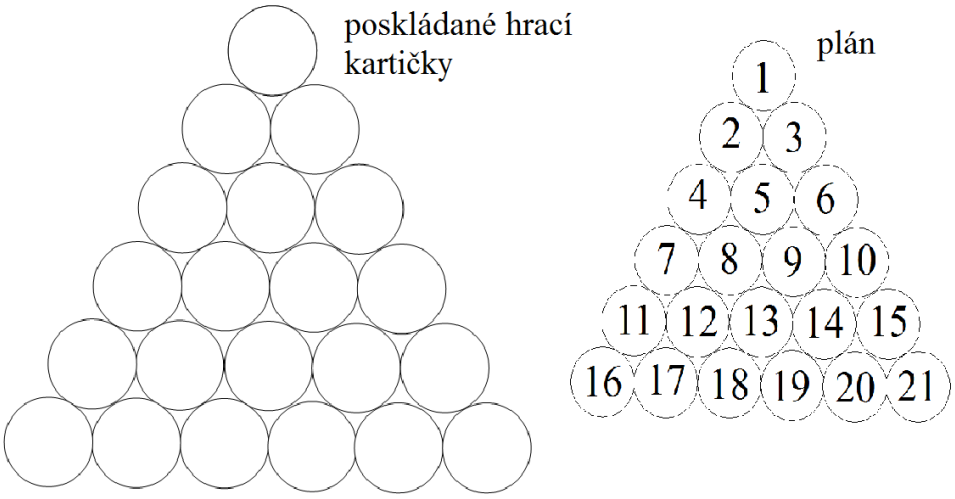
Příloha 3: Hra pro IV. – V. třídu

Hra pro IV. – V. třídu

Hra obsahuje otázky převážně z oblastí a pojmů, které obsahovala výuka vzdělávacího modulu. Součástí jsou otázky z témat, které by měli žáci IV. – V. třídy znát, a také část otázek ze základních pojmů, které se nevešly do náplně a měly by roztřídit děti podle jejich předchozích znalostí.

Před zahájením hry:

Žáci se rozdělí do dvojic. Každá dvojice dostane hrací plán a soutěžní kartičky, které nesmí prohlížet. Zamíchané kartičky naskládají do pyramidy podle plánu. Dvojice si vezme tři pastelky, černou a další dvě barevné dle výběru, pro každého hráče jednu.



Průběh:

Hráč A si zvolí pole např. 10. Hráč B odpočítá desátou kartičku a přečte otázku. Pokud hráč A odpoví správně, vybarví si políčko na hracím plánu svou barvou. Pokud hráč A odpoví špatně, políčko se označí černým puntíkem. Poté si volí kartičku hráč B a hráč A čte otázku. O neuhádnutá políčka s černým puntíkem se bude hrát hra „kámen, nůžky, papír“, vítěz si vybarví pole a poražený pokračuje v dalším výběru.

Konec hry:

Vítězem se stane ten, kdo spojí tři strany pyramidy. Dle časových možností se může hra upravit a vítězem se stane hráč s větším počtem získaných políček.

Hrací kartičky:

Mělo by být na každém zařízení, aby se k němu nepřihlásil někdo cizí...

Heslo

Speciální program, který pomáhá chránit zařízení se jmenuje...

Antivirový program

Před stažením aplikace bych měl zjistit, jaké vyžaduje...

Oprávnění

Sítě, mezi které řadíme například Facebook, YouTube, Tik Tok nazýváme...

Sociální sítě

Ke každému dílu (například fotka, dokument) se vztahují práva. Jak se jmenují?

Autorská práva

Na internetu nás někdo vyzývá, abychom splnili nějaké úkoly. Tyto hry se jmenuji...

On-line výzvy

Je bezpečné při jízdě na kole používat sluchátka?

Není

Publikování ponižujících fotografi je nevhodné chování, které se nazývá...

Kyberšikana

Seznam, Google, Atlas jsou webové prohlížeče nebo vyhledávače?

Vyhledávače

Může si někdo vytvořit na sociálních sítích falešný profil?

Může

Trashtag Challenge je pozitivní nebo negativní výzva?

Pozitivní

Jsou všechny informace na internetu pravdivé?

Nejsou

Kolik znaků je doporučená délka hesla?

8 znaků

Přenosné zařízení, na které lze ukládat data nazýváme...

USB Flash disk

Heslo123, je takové heslo bezpečné?

Není

Malware je označení pro...

Škodlivé kódy (programy)

Zařízení, pomocí kterého dostaneme obrázek do počítače nazýváme...

Skener

Nevyžádané zprávy označujeme slovem...

Spam

Název pro elektronickou poštu...

E-mail

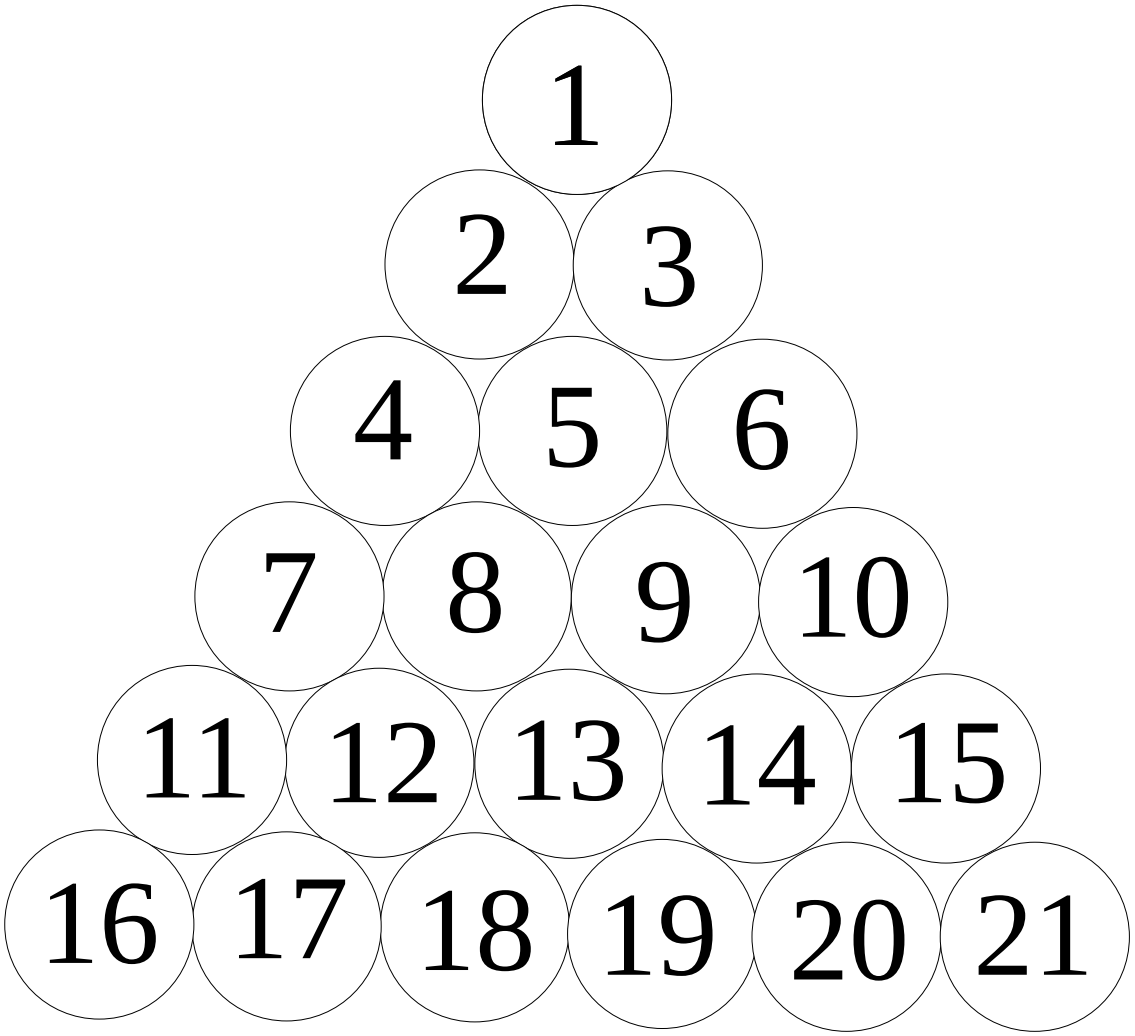
Informace o určité osobě (jméno, rodné číslo, bydliště) označujeme jako...

Osobní údaje

Označení pro bezdrátové připojení k síti je...

Wi-Fi

Hrací plán:



X