UNIVERZITA PALACKÉHO V OLOMOUCI
PEDAGOGICKÁ FAKULTA
Ústav pedagogiky a sociálních studií

Diplomová práce

Bc. Michal Jančík

Podvodné jednání v prostředí informačních a komunikačních technologií se zaměřením na žáky 2. stupně základních škol

Olomouc 2018 vedoucí práce**:** PhDr. René Szotkowski, Ph.D.

Prohlášení

Prohlašuji, že tuto diplomovou práci jsem vypracoval samostatně a výhradně s použitím literatury uvedené v seznamu literatury.

V Olomouci dne 1.6.2018 Bc. Michal Jančík

Poděkování

Tímto bych velmi rád poděkoval svému vedoucímu diplomové práce PhDr. René Szotkovskému, Ph.D., za odborné vedení, ochotný přístup, cenné rady a připomínky, které mi v průběhu zpracovávání této diplomové práce poskytoval.

ANOTACE

Jméno a příjmení	Bc. Michal Jančík
Katedra	Ústav pedagogiky a sociálních studií PdF UP v Olomouci
Vedoucí práce	PhDr. René Szotkowski, Ph.D.
Rok obhajoby	2018

Název práce	Podvodné jednání v prostředí informačních a komunikačních technologií se zaměřením na žáky 2. stupně základních škol.
Název v angličtině	Fraudulent behavior in the environment of information and communication technologies focusing on pupils of the 2nd grade of elementary schools.
Anotace práce	Diplomová práce Podvodné jednání v prostředí informačních a komunikačních technologií se zaměřením na žáky 2. stupně základních škol je rozdělena na část teoretickou a praktickou. V teoretické části práce vymezuje základní pojmy, popisuje historický vývoj podvodného jednání v daném prostředí po současný stav, zabývá se trestněprávní stránkou a nejrůznějšími podvodnými formami. Zaměřuje se taktéž na oběti, charakteristiku a motivy pachatelů, ale také se zabývá preventivním působením před tímto druhem kriminality na úrovni státu, školy, rodiny a vybraných subjektů. V praktické části zjišťuje aktuální stav dané problematiky se zaměřením na žáky 2. stupně základních škol v Prostějově a pomocí dotazníkového šetření mimo jiné zjišťuje u vybraných žáků 6. a 9. tříd základních škol 2. stupně v Prostějově, zda znají rizika podvodného jednání v prostředí informačních a komunikačních technologií, zda se s vybraným podvodným jednáním setkali a zda mají v tomto prostředí zkušenosti s obchodováním, což je vše zároveň hlavním cílem práce. Diplomová práce poukazuje na vzrůstající trend kyberkriminality, potažmo podvodného jednání a zdůrazňuje na nedostatečné preventivní působení na základních školách v této oblasti.

Klíčová slova	Informační a komunikační technologie, žáci 2. stupně základních škol, podvod, kybernetická kriminalita, prevence, podvodná inzerce, podvodné e-shopy, phishing, vishing, wangiri, smishing, pharming, malware, spam, scam, hoax, skimming, sociální sítě, podvodné profily.
Anotace v angličtině	Diploma thesis fraudulent behavior in the environment of information and communication technologies focusing on pupils of the 2nd grade of elementary schools is divided into the theoretical and practical part. In the theoretical part of the thesis it defines the basic concepts, describes the historical development of fraudulent behavior in the given environment to the present state, deals with criminal law and various fraudulent methods. It also focuses on the victims, characteristics and motives of the perpetrators, but also deals with the prevention of this type of crime at the level of the state, school, family and selected entities. In the practical part, he examines the current state of the given problem focusing on the pupils of the 2nd grade of elementary schools in Prostějov and through a questionnaire survey, among others, he discovers among selected pupils 6th and 9th grades of elementary schools in Prostějov whether they know the risks of fraudulent behavior in the information environment and communication technologies, whether they have met with the selected fraudulent behavior and whether they have experience of trading in this environment, which is also the main goal of the work. The diploma thesis highlights the increasing trend of cybercrime, or fraudulent behavior, and stresses the insufficient preventive effect on elementary schools in this area.
Klíčová slova v angličtině	Information and communication technologies, pupils of 2nd grade primary schools, fraud, cyber crime, prevention, fraudulent advertising, fraudulent e-shops, phishing, vishing, smishing, pharming, malware, spam, scam, hoax, social networks, fraudulent profiles.

Přílohy vázané v práci	**Příloha č. 1** – původní dotazník pro žáky základních škol použitý pro pilotní studii. **Příloha č. 2** – dotazník pro žáky základních škol, finální podoba po úpravě. **Příloha č. 3** – výsledky dotazníkového šetření podrobně. **Příloha č. 4** – dotazník pro školní metodiky prevence. **Příloha č. 5** – doplňující tabulky a grafy k diplomové práci. **Příloha č. 6** – úplné znění zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů a úplné znění zákona č. 251/2016 Sb., o některých přestupcích, ve znění pozdějších předpisů. **Příloha č. 7** - rady a tipy před podvodným jednáním v prostředí informačních a komunikačních technologií.
Rozsah práce	144 stran
Jazyk práce	Český jazyk

Obsah

Empirická část

Úvod

Lidstvo prošlo do současné doby značnou technickou inovací, která dala vzniku moderním informačním a komunikačním technologiím (dále IT), o nichž se nám dříve ani nesnilo. Počítače, tablety, mobilní telefony, navigace a další elektronická zařízení spolu s počítačovými programy a internetem patří mezi nepostradatelné fenomény dnešní doby, na které si mnozí z nás tak zvykli, že si bez nich nedokáží představit snad ani svůj život. Jejich rozvoj nabyl takové rázu, že se v současné době nacházejí na každém našem kroku a jsou implementovány do všech odvětví lidské činnosti. Byly vytvořeny pro nás, aby ulehčovaly a zpříjemňovaly naše životy. Svůj účel jistě splnily, jelikož díky nim máme snadný přístup k ohromnému množství informací, zboží, službám, zábavě, pomoci, můžeme s ostatními sdílet cokoliv, komunikovat s kýmkoliv a to vše během jediného okamžiku. Otevřel se nám svět téměř neomezených možností a znalost těchto technologií se stala klíčovou oblastí pro další rozvoj naší společnost. Nicméně stejně jako každá mince má dvě strany, tak i používání těchto nových vymožeností sebou přináší specifická rizika, která nám do jejich příchodu nehrozila. Jedním z takových rizik je páchání protiprávního jednání právě v tomto prostředí.

Do IT prostředí se přesunula značná aktivita naší společnosti a je logické, že se do něj přenesla i kriminalita. Samotné IT jsou mnohdy velmi snadno ovladatelné a někdy postačuje jediné kliknutí či stisknutí tlačítka k dosažení zamýšleného cíle, např. provedení nákupu, zaslání zprávy, spuštění aplikace, komunikace s cizí osobou apod. Ačkoliv je v jednoduchosti síla, z opačné strany lze na ni nahlížet jako na nebezpečí a riziko. Tedy stejně tak můžeme jedním kliknutí či stisknutím tlačítka přijít do styku s podvodníkem, zlodějem, pedofilem, nebo nebezpečným programem, jejichž zájmem je něco neoprávněně získat. Takovým zájmem mohou být nejen peníze a obecně majetek, ale dnes tolik důležité přihlašovací údaje, bankovní údaje nebo další citlivé údaje a informace. Doba, kdy si před pachateli tak stačilo hlídat *„pouze peněženku v kapse*“, nebo *„dítě v bezpečí domova*“, s novými technologiemi skončila.

Naše děti a mládež si používání IT plně osvojily, tráví s nimi mnoho svého času. Přitom nemají dokončen fyzický ani duševní vývoj, mají méně zkušenosti, jsou zranitelnější, citlivější a důvěřivější než my, dospělí lidé, a proto všechna tato rizika pro ně představují hrozbu ještě větší. Záleží tedy na nás dospělých, abychom naše děti zavčas ochránili před nebezpečím, se kterými se mohou setkat. Měli bychom apelovat na to, aby nejen naše děti a mládež, ale abychom my všichni byli ve virtuálním prostoru značně obezřetní, dodržovali bezpečnostní pravidla, měli kvalitní zabezpečení a znali možná rizika podvodného jednání pachatelů v IT prostředí.

Ke zpracování diplomové práce na téma „*Podvodné jednání v prostředí informačních a komunikačních technologií se zaměřením na žáky 2. stupně základních škol*" mě vedlo několik důvodů. Téma slučuje moji zálibu a orientaci v IT, osobní i rodičovský zájem o danou problematiku a mé současné zaměstnání. Jako policista zpracovávám trestnou činnost, přičemž s podvodnými praktikami se v tomto prostředí setkávám téměř pravidelně a sám vím, že má stoupající tendenci. Navíc jsem povinen se chovat proaktivně a předcházet a zamezovat trestné činnosti, v čemž vidím souvislost s preventivním působením. V neposlední řadě dané téma spojuje i vhodnost tématu daného pro Pedagogickou fakultu, jelikož se zaměřuje právě na žáky základních škol. Navíc se domnívám, že se jedná o velmi aktuální téma, kterému je třeba se zabývat a věnovat mu zvýšenou pozornost.

Diplomová práce je rozdělena na část teoretickou a empirickou. Hlavním cílem v teoretické části práce je vytvořit přehledný, ucelený a aktuální soubor teoretických vstupů o podvodném jednání v IT prostředí z hlediska protiprávního jednání. V empirické části je **hlavním cílem** zjistit u vybraných žáků 6. a 9. tříd základních škol 2. stupně v Prostějově, zda znají rizika podvodného jednání v IT prostředí, zda se s podvodným jednáním setkali a zda mají v tomto prostředí zkušenosti s obchodováním. Oblast obchodování je podstatná z toho důvodu, jelikož se pachatelé v daném prostředí zaměřují zejména na něj.

Teoretická část práce obsahuje šest kapitol a vychází z analýzy poznatků získaných studiem odborné literatury, publikací, článků, zákonných norem, metodických doporučení, dostupných informací orgánů státní správy a dalších relevantních zdrojů. K naplnění hlavního cíle teoretické části byly stanoveny dílčí cíle, které představují jednotlivé kapitoly a podkapitoly.

První kapitola teoretické části tedy vymezuje základní pojmy spojené s IT a podvodným jednáním z hlediska kriminality. Druhá kapitola popisuje historický vývoj podvodů v IT prostředí. Třetí kapitola se zabývá trestněprávní stránkou podvodného jednání z hlediska právní úpravy České republiky. Čtvrtá kapitola popisuje jednotlivé formy podvodných praktik v daném prostředí s přesahem na specifické formy zaměřené na seniory. Pátá kapitola se zabývá samotnými pachateli, jejich oběťmi a odpovědností žáků základních škol za takové jednání. Šestá kapitola je zaměřena na prevenci před tímto druhem kriminality na úrovni státu, školy, rodiny a dalších subjektů. Důvody volby jednotlivých kapitol jsou uvedeny na začátku každé kapitoly, a ačkoliv teoretická část práce zasahuje zejména do oblasti kriminality, je východiskem praktické části, ve které se zaměřuje právě na žáky základních škol.

Praktická část práce obsahuje pět kapitol a vychází z vlastního výzkumného šetření, uskutečněného formou anonymních dotazníků se školními metodiky prevence a vybranými

žáky 6. a 9. tříd 2. stupně základních škol v Prostějově. K naplnění hlavního cíle empirické části, bylo stanoveno 12 dílčích cílů, které jsou uvedeny v kapitole 9.1.1.

První kapitola empirické části, tedy sedmá kapitola seznamuje se současným stavem zkoumané problematiky z dosud provedených výzkumů, výzkumných šetření a dalších relevantních zdrojů. Osmá kapitola charakterizuje realizované kvantitativní pedagogické výzkumné šetření. Devátá kapitola popisuje vlastní výzkumné šetření krok za krokem a mimo jiné popisuje empirické dílčí cíle diplomová práce, deskriptivní problémy, relační problémy a hypotézy. Desátá kapitola obsahuje samotné výsledky výzkumného šetření, názorně graficky a tabulkově zpracované. Závěrečná kapitola předkládá diskuzi i závěry z vlastního výzkumného šetření a porovnává je se zjištěním současného stavu o dané problematice, které je předestřeno v sedmé kapitole.

TEORETICKÁ ČÁST

1 Vymezení základních pojmů

Cílem této kapitoly je vymezit ty základní pojmy, podstatné pro jejich pochopení. Jedná se o pojmy v této práci používané, ale i ty, které s nimi úzce souvisí a jsou stále v různých odborných publikacích používány. Tato kapitola se zabývá třemi základními oblastmi pojmů, kterými jsou informační a komunikační technologie, podvodné jednání a kriminalita v informačních a komunikačních technologií. Při vymezování základních pojmů je kladen důraz na souvislost, návaznost a systém v samotné terminologii.

V této kapitole nejsou některé specifické pojmy vymezeny. Jejich vymezení se z důvodu přehlednosti nachází v těch kapitolách, které se jich přímo týkají.

1.1 Informační a komunikační technologie

Pojem informační a komunikační technologie (dále IT) je v dnešní době velmi často užíván, ale jeho vymezení není jednotné. V literatuře je mnohdy označován jako informační technologie, komunikační technologie, digitální technologie, moderní technologie, nové technologie, výpočetní technika, apod. Proto považuji za podstatné, tyto časté pojmy ozřejmit.

V minulosti byl pro označení těchto veškerých technologií používán pouze termín **informační technologie**. Tento pojem *„zahrnuje veškerá elektronická zařízení, která jsou schopna nějakým způsobem zpracovávat informace,“* ale z tohoto pohledu se jedná pouze o hardwarovou fyzickou část těchto zařízení. Díky technologickému vývoji a pokroku došlo mezi těmito zařízeními ke vzájemné komunikaci a termín informační technologie byl rozšířen o prvek komunikace (Průcha a Veteška, 2014, s. 138).

Organizace OSN pro vzdělání, vědu a kulturu UNESCO (2003) ve svém vydání „*Developing and Using Indicators of ICT Use in Education*“ informační a komunikační technologie rozděluje na dva odlišené pojmy. Informační technologie označují nejen hardwarové části, ale rovněž počítačové programy – software. **Komunikační technologie** označují jako telekomunikační zařízení, jež umožňuje informace vysílat a přijímat.

Průcha a Veteška (2014, s. 138) ve svém Andragogickém slovníku již specifičtěji uvádějí, že **informační a komunikační technologie** pochází z anglického názvu Information and Communication Technologies, odkud pochází zkratka ICT[1] a *„zahrnují veškeré technologie, nástroje a postupy umožňující komunikaci a práci s informacemi. Pojem označuje hardwarové (servery, počítače, komunikační a síťová zařízení, kamera, myš apod.)*

[1] V této práci pro pojem informační a komunikační technologie je však používána zkratka IT.

a softwarové (operační systém, textové editory, grafické programy, síťové protokoly apod.) prostředky pro sběr, přenos, ukládání zpracování a distribuci dat.“

Jelikož se IT integrovaly i do vzdělávacího procesu, lze je definovat i v souvislosti s pedagogikou. Takové vymezení uvádí např. pedagogičtí odborníci Zounek a Šeďová (2009, s. 15), kteří uvádí, že „*pod pojmem informační a komunikační technologie zahrnujeme prostředky moderní didaktické audiovizuální techniky (např. video, televizi, CD přehrávač, datový projektor) a* ***digitální technologie****, které jsou založeny na počítačích a na telekomunikačních službách, umožňujících jejich uživatelům v maximální možné míře zpřístupnit informace a dále s nimi pracovat (např. internet, interaktivní tabule, digitální kamera aj.), ale také různými formami a prostředky komunikovat (email).“*

Ve starším vydání českého Pedagogického slovníku je tento termín označen termínem **nové technologie ve vzdělávání** a je definován takto: „*moderní prostředky didaktické techniky a jimi inspirované nové formy vyučování zahrnující zejména: 1. sítě (lokální počítačové sítě, Internet a jeho prostřednictvím přístupné on-line knihovny, databáze a další zdroje informací, videokonference a jiné), 2. multimédia, která spojují různé formy prezentace informací (hypertext, obraz a animovaný obraz, zvuk atd.) na různých typech nosičů (on-line, CD-ROM), 3. mobilní prostředky a přístupy podporující flexischooling a další formy distančního vzdělávání, zahrnující bezdrátové sítě, notebooky apod*.“ (Průcha et al., 2003, s. 139). Tato definice pak vychází z literatury od Bertranda (1998, s. 89–116).

Zounek a Šeďová (2009, s. 14–15) však k pojmu nové technologie ve vzdělávání uvádějí, že se jedná o nepřesný termín, který nedefinuje, jaké technologie jsou ještě ty staré, a jaké jsou již ty nové, moderní. V aktualizovaném Pedagogickém slovníku (Průcha et al., 2013, s. 103), termín nové technologie ve vzdělávání byl již nahrazen termínem informační a komunikační technologie ve vzdělávání.

Za důležité je rovněž zmínit, že dané technologie ovlivnily téměř všechny odvětví lidské činnosti. Díky jejich rozvoji je naše společnost nazývána **informační společností**, ve které se informace staly hlavním produktem či základem, respektive nutností pro jiné produkty. Úspěch tak závisí na využití informací a jejich zvládnutí, což v praxi znamená závislost na internetu a počítačových procesech. IT se staly nepostradatelnou a důležitou součástí státní, soukromé i podnikatelské sféry, a proto patří získávání a rozvíjení jejich dovedností mezi klíčové kompetence pro osobní rozvoj a uplatnění každého člověka ve společnosti (Průcha a Veteška, 2014, s. 138).

1.2 Podvodného jednání

V pedagogickém slovníku definici tohoto pojmu nenalezneme. Pouze zde nalezneme pojem **jednání,** jenž je definován jako *„takové chování, které je záměrné, motivované, řídí se představou cíle, usiluje o změnu jedince samého, sociální situace nebo věcí a jevů okolního světa.“* (Průcha et al., 2003, s. 95). Synonymem záměru je úmysl, proto jednání můžeme označit i jako úmyslné chování.

Podvod je pojem spojovaný s protiprávním jednáním, respektive kriminalitou, přičemž z tohoto pojetí je Zoubkovou (2011, s. 80) zařazován mezi závažné sociálně patologické jevy.

Sociálně patologické jevy lze obecně definovat jako*„ závažné poruchy chování jedince, které se projevují zejména v porušování sociálních, případně právních norem*.“ (Miovský et al., 2015, s. 167). Jsou to pro společnost *„nechtěné, nežádoucí, nebo až nepřijatelné* “ společenské jevy, mezi něž patří mimo kriminality a delikvence i např. agresivní a násilné chování, suicidální jednání, zneužívání psychoaktivních látek, návykové a impulsivní poruchy, některé nelátkové závislosti, prostituce, záškoláctví, dysfunkční a afunkční rodina (Fišer a Škoda, 2014, s. 15).

Definici podvodného jednání nabízí jeden z nejvýznamnějších českých právníků zabývající se trestním právem Pavel Šámal (2009, s. 1853), který v obecné rovině **podvodné jednání** definuje jako *„uvedení v omyl nebo využití omylu, popř. zamlčení podstatných skutečností, může směřovat nejen vůči poškozenému, ale i vůči jiné osobě. Omyl je rozpor mezi představou a skutečností. O omyl půjde i tehdy, když podváděná osoba nemá o důležité okolnosti žádnou představu nebo se domnívá, že se nemá čeho bát.*“

Pakliže při podvodném jednání je úmyslem se zmocnit cizí věci, což spadá již do oblasti kriminality, pachatel poškozenému neodnímá věc proti jeho vůli, ale poškozený mu ji sám dobrovolně vydá nebo mu dovolí, aby si ji vzal (Smejkal, 2015, s. 140).

Uvedení někoho v omyl a využití něčího omylu lze provést i prostřednictvím technického zařízení, což definuje § 120 trestního zákoníku. *„Uvést někoho v omyl či využít něčího omylu lze i provedením zásahu do počítačových informací nebo dat, zásahu do programového vybavení počítače nebo provedením jiné operace na počítači, zásahu do elektronického nebo jiného technického zařízení, včetně zásahu do předmětů sloužících k ovládání takového zařízení, anebo využitím takové operace či takového zásahu provedeného jiným*.“ (Zákon č. 40/2009 Sb.).

1.3 Kriminalita informačních a komunikačních technologií

Podvod tedy spadá mezi **kriminalitu**[2]. Z užšího legálního juristického pojetí je kriminalita „*souhrn jednání, která trestní právo posuzuje jako trestné činy*“ uvedené v trestním zákoníku. Z hlediska širšího sociologického pojetí, jež je na trestním právu nezávislé, označuje rovněž, jak bylo uvedeno, „*některé závažné sociálně patologické jevy*“ (Zoubková, 2011, s. 80–81). Ačkoliv není kriminalita ze sociologického hlediska dle trestního práva přímo trestná, je stále společensky škodlivá a negativním způsobem ovlivňuje kvalitu naší společnosti. K tomuto pojetí je nutné přistupovat opatrně, protože s kriminalitou nemusí vůbec souviset (Chalupová et al., 2012, s. 13).

Širší pojetí kriminality označujeme termínem **delikvence,** což je „*způsob jednání, kterými jsou porušovány nejen právní, ale i společenské normy.*“ Takové činy nazýváme delikty a patří sem protispolečenské činnosti dětí a přestupky (Kraus a Hroncová, 2010, s. 30).

Kriminalitu dělíme do různých oblastí. Násilná, hospodářská, mravnostní, majetková, počítačová, kybernetická, latentní apod., které se mohou i vzájemně prolínat. Obecně však podvod podle Zoubkové (2011, s. 84) spadá mezi **majetkovou kriminalitu**, která představuje jednání spočívajícím v útoku proti cizímu majetku. Takový útok může být namířen se záměrem získání majetku hlavně krádeží, podvodem, jeho poškození nebo využití trestné činnosti jiného.

Vzhledem k tomu, že se tato práce zabývá kriminalitou v prostředí IT a v odborných publikacích jsou v této souvislosti používány nejčastěji pojmy počítačová kriminalita, kybernetická kriminalita, informační kriminalita, internetová kriminalita, e-kriminalita, které všechny v podstatě lze považovat za její podmnožiny, je vhodné tyto pojmy blíže objasnit.

Počítačová kriminalita není jednotně vymezena a definic tohoto termínu lze nalézt celou řadu. Mnozí autoři se však shodují v tom, že se jedná o trestnou činnost, v níž figuruje počítač, který je terčem útoku, přičemž se může jednat o průniky do systémů za účelem krádeže, podvodu, zneužití údajů apod., anebo počítač slouží k usnadnění trestné činnosti, je tedy prostředkem k páchání trestné činnosti (např. Matějka, 2002, s. 6; Matoušková, 2013, s. 154; Smejkal, 2015, s. 21).

Definic pojmu **počítač** existuje rovněž celá řada. V zásadě je to „*každá funkční jednotka schopná provádět výpočty a operace bez lidského zásahu a podle určitého programu, zařízení na zpracování, uchovávání a využívání dat, která převádí na číselné kódy*.“ (Kuchta, 2009, s. 224).

[2] Též kriminální jednání, zločinnost, trestná činnost.

V publikacích se ovšem častěji setkáváme s pojmem **počítačový systém**, což je *„funkční jednotka, která je složena z jednoho nebo více počítačů a přidruženého software, využívající paměťové médium*[3] *pro všechny, nebo pouze část programů a dat, nezbytných pro vykonávání programů.“* Příkladem takového systému je nejen osobní počítač a notebook, ale také počítačová síť, mobilní telefon, tablet, PDA, herní konzole, televize, bankomat nebo jakékoliv technické zařízení umožňující spouštět aplikace (Kolouch, 2016, s. 58).

Odborné publikace často uvádějí definici počítačové kriminality od českého odborníka zabývající se touto problematikou Vladimíra Smejkala (2015, s. 20–21), který počítačovou kriminalitu definuje jako *„páchání trestné činnosti, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité, nebo jako nástroje trestné činnosti.“*

Rada Evropy ve statutu Komise expertů pro zločin v cyberprostoru počítačovou kriminalitu definují však také jako: „*Trestný čin namířený buďto proti integritě, dostupnosti nebo utajení počítačových systémů nebo trestný čin v tradičním slova smyslu, při kterém je použito moderních informačních a telekomunikačních technologií*.“ (Matějka, 2002, s. 5).

Kolouch (2016, s. 32) vhodně uvádí, že počítačová kriminalita se v 90. letech 20. století ustálila jako pojem pro trestnou činnost páchanou za pomocí výpočetní techniky a evokuje představu, že je tato činnost páchána nejčastěji osobním počítačem. Proto se v dnešní době tento termín v odborné literatuře téměř nepoužívá. Namísto pojmu počítač je dnes obecně používán výraz informační a komunikační technologie a tedy tato kriminalita je nazývána **kriminalitou informačních a komunikačních technologií**.

O tom, že **informační kriminalita** je pojmem širším než termín počítačová kriminalita, se zmiňoval již Matějka (2002, s. 3), nebo Musil (2000, s. 8), který zmiňoval, že na tento druh kriminality má být nahlíženo z hlediska informačního pojetí**.** Zájem o informace, byť byly uchovávány, zpracovávány a přenášeny jiným způsobem, byl mnohem dříve, než vznikl pojem počítačová kriminalita. Rozšiřování výpočetní techniky vedlo a vede k vyšší míře jejího zneužívání a zastiňuje klasické formy práce s informacemi a jejich zneužívání.

[3] Paměťové médium slouží jako nosič informací a dat. Může se jednat o pevný disk (HDD), operační paměť (RAM), CD, DVD, Blu-Ray, USB disk, paměťovou kartu, mobilní telefon (Šámal, 2009, s. 2090).

Smejkal (2003, s. 161) uvádí, že informační kriminalita je *„prostředkem nebo cílem zločinného útoku jsou informace, bez ohledu na to, jakým způsobem jsou zpracovávány a jakým způsobem byly k útoku použity,“* jedná se tedy též např. o pomluvu podle trestního zákoníku.

Definici informační kriminality lze nyní taktéž nalézt např. ve Výkladovém slovníku kybernetické bezpečnosti, který ji definuje specifičtěji jako trestnou činnost, *„pro kterou je určující vztah k software, k datům, respektive uloženým informacím, respektive veškeré aktivity, které vedou k neautorizovanému čtení, nakládání, vymazání, zneužití, změně nebo jiné interpretaci dat*.“ (Jirásek et al., 2015, s. 55).

V odborné literatuře i v mezinárodních úmluvách se v dnešní době pro kriminalitu páchanou prostředky informačních a komunikačních technologií nejčastěji používá pojem **kybernetická kriminalita**[4] (Kolouch, 2016. s. 33; Smejkal, 2015, s. 15), která představuje nejširší množinu veškeré trestné činnosti páchané v prostředí IT (Kolouch, 2016, s. 35).

V podstatě neexistuje jednotná definice, která by hloubku a rozsah tohoto pojmu plně postihla, avšak v odborných publikacích je označována jako kriminální jednání, v němž je předmětem útoku samotná informační a komunikační technologie anebo je tato kriminalita páchána za výrazného využití těchto technologií, jakožto prostředku k dosažení cíle (Kolouch, 2016, s. 34; Rak a Porada, 2013, s. 34).

V nejobecnější rovině lze kybernetickou kriminalitu definovat *„jako jednání namířené proti počítači, případně počítačové síti, nebo jako jednání, při němž je počítač použit jako nástroj pro spáchání trestného činu*.“ Aby bylo možné uplatnit tuto definici, je nutné neopomenout skutečnost, že počítačová síť je prostředím a prostorem, v němž se tato činnost odehrává (Kolouch, 2016, s. 34).

V některých zemích je kybernetická kriminalita nazývána kriminalitou počítačovou (Rak a Porada, 2013, s. 34), a ačkoliv i někteří autoři považují počítačovou a kybernetickou kriminalitu za synonymum (např. Jirásek et al., 2015, s. 69, 85), o synonymum se nejedná (Šámala, 2009, s. 2084; Kolouch, 2016, s. 34).

Kybernetická kriminalita je odvozena od pojmu nikoliv kybernetika, ale **kybernetický prostor**[5], který lze označit jako *„nervový systém*“ tvořený propojenými počítači, routery, servery, přepínači, optickými kabely. Jedná se o sběrný termín pro všechno od internetu a světové sítě, až po imaginární a metaforický prostor, který v něm existuje. Tento prostor je tam, kde jsou informace, je to skutečný a zároveň fiktivní prostor, v němž probíhá např. chat

[4] Též kybernetická trestná činnost, kyberkriminalita, Cyber-crime.

[5] Též kyberprostor.

nebo e-mailová komunikace (Šámal, 2009, s. 2084; Kuchta, 2016, s. 7). Předmětem trestné činnosti nebo jeho nástrojem není tedy pouze počítač (Smejkal, 2015, s. 15).

Kybernetický prostor je definován v § 1 zákona o kybernetické bezpečnosti jako „*digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací*." (Zákon č. 181/2014 Sb.).

V současné době je v rámci kybernetické kriminality nejvíce využíváno komunikační rozhraní sítě Internet (Rak, Porada, 2013, s. 34), proto se někdy lze setkat s pojmem **internetová kriminalita**, která kromě počítače jako objektu či nástroje trestné činnosti vyžaduje propojení počítačů lokálními a vzdálenými sítěmi a následné využití internetu (Smejkal, 2003, s. 161).

V neposlední řadě se můžeme setkat i s pojmem **e-kriminalita**[6], který vznikl vzhledem ke konvergenci médií, kdy se v době digitálního zpracování všech druhů informací přestalo rozlišovat, zda jsou obsahem řady bitů, zvuk, obraz nebo počítačová data (Smejkal, 2003, s. 161).

Vzhledem k velkému množství definic v oblasti IT kriminality je tedy téměř nemožné zavést jednotnou definici, která by plně vystihovala její veškeré aspekty.

Podvodné jednání v IT prostředí z hlediska protiprávnosti, na což je tato práce zaměřena, nicméně spadá do oblasti kybernetické kriminality. Mohli bychom tedy definovat, že se jedná o úmyslné kriminální jednání včetně delikvence, jako sociálně patologický jev, při němž za pomoci zařízení pro zpracování informací a komunikaci dochází k uvedení v omyl, využití omylu nebo zamlčení podstatných skutečností včetně zásahu prostřednictvím technického zařízení, vůči někomu nebo něčemu jinému s určitým záměrem. Takovým záměrem může být nejčastěji způsobení škody na majetku nebo získání dat, údajů, informací, či přístupu k nim nebo samotné IT.

[6] Též elektronická kriminalita.

2 Historický vývoj podvodného jednání v informačních a komunikačních technologií

S příchodem informačních a komunikačních technologií (dále IT) začali pachatelé trestné činnosti tyto technologie využívat k páchání tradičního nebo zcela nového protiprávního jednání. S vývojem a rozšiřováním technologií mezi širokou veřejnost tak docházelo i k vývoji a rozšiřování kriminality, která podle Smejkala (2015, s. 73) de facto kopírovala technické a uživatelské možnosti těchto technologií. Pokud tedy chceme pochopit současné podvodné praktiky pachatelů v IT, musíme se podívat do historie, jaký vývoj jim předcházel.

První kriminální případy, které se začaly objevovat se vnikem nových technologií, byly **sabotáže**. Motivace byly politické či proti zaměstnavateli. První taková sabotáž byla spáchána ve Francii v roce 1801, kde zaměstnanci Jaquardova automatizovaného tkalcovského stavu[7] tento záměrně poškozovali z důvodu obavy o budoucnost svého zaměstnání. Kořeny tohoto protiprávního jednání nalezneme v tzv. hnutí Luddistů, v němž řemeslníci protestovali proti změnám výroby způsobeným průmyslovou revolucí a proti strojům, jako původci nezaměstnanosti (Smejkal, 2015, s. 75).

Významnou událostí historie IT kriminality byl následně **vynález telefonu** v 19. stol., jako prvního prostředku elektronické komunikace. Prostředí mezi telefonními přístroji bylo pojímáno jako *elektronické pohraničí*, což ve spojení s počítačem vedlo později ke vzniku kyberprostoru. V 70. letech 19. stol. byly zaznamenány případy, kdy mladí chlapci pracovali v telefonní ústředně, úmyslně přerušovali telefonní hovory, smáli se do nich, nebo uváděli v omyl uživatele tím, že k sobě úmyslně spojovali nepatřící hovory. S rozvojem telekomunikačních zařízení se v 70. letech 20 stol. poměrně rozmohl nový druh kriminality tzv. **phreaking**, který spočíval v tom, že pachatelé díky specifickým technikám využívali nedokonalostí telefonní sítě zejména k nelegálnímu telefonování zdarma. Známý phreaker byl např. John Draper, jenž v roce 1971 díky dětské píšťalce vydávající zvuk o určité frekvenci, použité v telefonní lince, uskutečňoval hovory zdarma (Matějka, 2002, s. 18–21).

Sestrojení prvního elektronického počítače ENIAC v roce 1946 představovalo **zrod počítačového věku**, avšak nová éra pro IT nastala až v roce 1981, kdy společnost IBM uvedla na trh první osobní počítač, čímž se počítače začaly dostávat do běžných domácností. V 80. letech 20 stol. také docházelo k propojování počítačů a telefonní linky do sítí zejména v podobě

[7] Předchůdce počítače.

technologie BBS[8] jako předchůdce internetu, což vytvořilo odrazový můstek pro rozvoj dalšího druhu kriminality, tzv. **hackingu**. Tento spočíval v tom, že pachatelé neoprávněně pronikali do počítačových systémů a prozkoumávali jejich útroby. Vznikaly hackerské skupiny a z počátku to byl prostředek pro nadšence ke slávě, osobnímu vítězství a zviditelnění (Matějka, 2002, s. 20–24).

Termín „*hacker*" pochází již z 50. let 20 stol. a označuje technicky nadanou osobu schopnou nalézat nová, neortodoxní řešení problému (Kolouch, 2016, s. 270). V době vzniku tohoto termínu se jednalo o oprávněné programátory, kteří prováděli zásahy do předchůdců dnešních počítačů za účelem zefektivnění, úpravy nebo opravy, přičemž jejich úloha byla na rozdíl od 80. let 20 stol. pozitivní (Matějka, 2002, s. 20). Většina hackerů též začínala jako phreakři (Smejkal, 2015, s. 129).

S nástupem webových technologií, intenzivním využíváním počítačů a nárůstem informací dostupných na počítačových sítích se hacking začal měnit a profesionalizovat (Jírovský, 2007, s. 48). V 90. letech 20. stol. přestal být zejména cílem k získání slávy a začal být prostředkem k obohacení a páchání škody, zisku, včetně podvodů (Matějka, 2002, s. 27).

První člověk potrestaný za hacking byl Ian Murphy, který v roce 1981 pronikl do počítačové sítě firmy AT & T a pozměnil čas jeho vnitřního systému, čímž se hovory s denní tarifní sazbou účtovaly za tarify noční (Matoušková, 2013, s. 154).

Dalším příkladem je jeden z nejslavnějších a největších hackerů této doby Kevin Mitnick, který v 90. letech 20 stol. pronikal do počítačových systémů různých společností a způsobil škodu 300 mil. dolarů (Jírovský, 2007, s. 58), hacker Kevin Poulsen v roce 1990 pronikl do telefonní sítě amerického rádia a zajistil si konkrétně 102. pozici volajícího, čímž dosáhl podvodné výhry v soutěži o motorové vozidlo značky Porsche 944 S2 (Matoušková, 2013, s. 154), nebo hacker Vladimir Levin, jehož skupina v roce 1994 pronikla do počítačů americké banky Citibank a převedla si na své účty 10 mil. dolarů (Matějka, 2002, s. 27).

Ve druhé polovině 90. let 20 stol. byly masivně rozšířeny osobní počítače s operačním systémem Microsoft Windows, rostl vývoj software, nabýval rozvoj a komercializace počítačové sítě Internet, což vedlo ke zlaté éře dalšího druhu kriminality, tzv. **softwarového pirátství –** porušování autorského práva, spočívajícím zejména v nelegální kopírování, vypalování a prodeji programů, hudby, her, filmů. K šíření nelegálního software začaly vznikat i tzv. warez skupiny (Matějka, 2002, s. 41).

[8] Bulletin Board Systém.

Výrobci software se snažily své produkty před kopírováním či nelegálním užíváním chránit, proto se rozvinul i tzv. **cracking**, jenž spočíval v prolamování nebo obcházení ochranných prvků počítačového systému programů nebo aplikací, s cílem jejich neoprávněného užití (Kolouch, 2016, s. 276).

S rozšiřováním internetu do domácností a firem se aktivity pachatelů rovněž zaměřovaly na podvody s odcizenými platebními kartami, útoky na finanční instituce a začala nabývat na nebezpečnosti rovněž **hrozba počítačových škodlivých programů** – **malware** – virů, jejichž hlavním distribučním kanálem byla elektronická pošta[9] nebo právě nelegální software. Prvním světoznámým internetovým virem byl vir Melissa z roku 1999, který se rozšířil do celého světa. Jeho škodlivost spočívala v tom, že se sám rozesílal prvním 50 uživatelům z adresáře napadeného počítače. Nejednalo se o destruktivní program, ale poukázal, jak mohou viry působit. Dalším obdobným světoznámým virem byl vir *„I Love You"* z roku 2000, maskující se za podvodný milostný vzkaz. Od té doby vznikaly viry nové a nové, z nichž některé také způsobovaly ztrátu dat, mazaly soubory nebo byly vytvořeny s cílem se dostat k určitému obsahu v počítačovém systému (Matějka, 2002, s. 35).

2.1 Historie na území České republiky

V 70.–80. letech 20. stol. byly na našem území typické **sabotáže** proti výpočetní technice, přičemž první ryze počítačový kriminální čin se odehrál v 70. letech, kdy zaměstnanec Úřadu důchodového zabezpečení úmyslně poškozoval magnetem záznamové pásky. Podobný případ se udál rovněž v 90. letech 20 stol., kdy zaměstnanci výpočetního střediska záměrně poškozovali počítač, aby dosáhli jeho výměny za výkonnější (Smejkal, 2015, s. 76–77).

Ještě v době, kdy nebyly IT dostupné, je pachatelé nejčastěji **zneužívali** u svého zaměstnavatele. Účely byly různé. Tisk populárních obrázků na řádkové tiskárně, neoprávněné telefonování, kondiciogramy a výpočty diplomových prací, nelegální podnikání. Konkrétní případ se stal např. v 90. letech 20 stol., kdy spojovatelka telefonní ústředny na monitoru počítače podvodně přepisovala údaje o telekomunikačním hovoru, díky čemuž mohli její známí telefonovat do zahraničí zdarma (Smejkal, 2015, s. 127).

V 80. letech 20 stol. se začaly objevovat tzv. **dokladové delikty**, kde pachatelé měnili a falšovali údaje v dokladech připravených ke zpracování do počítače. Podstatou byly např. podvodné manipulace ve mzdových účtárnách, odbytech, zásobování a jiných pracovištích, kde

[9] Emaily.

měl zaměstnanec možnost manipulovat s penězi, ať už v hotovosti nebo přes čísla účtů, či zboží. Za takové podvody bylo v dané době dokonce 14 osob trestně stíháno (Smejkal, 2015, s. 133).

V 90. letech 20 stol. se začal na našem území vyvíjet bankovní sektor, což v kombinaci se zaváděním výpočetní techniky do bank znamenalo vznik **bankovních počítačových podvodů**, které měly charakter zejména neoprávněné manipulace s bankovními záznamy. Rovněž se začaly rozvíjet úvěrové podvody, pojistné podvody, padělané dokumenty. Historicky známý bankovní podvod s pomocí výpočetní techniky byl spáchán v roce 1991, kde si zaměstnanec České spořitelny převedl nelegálními počítačovými operacemi částku 35 mil. korun na své účty. Dále se např. v roce 1996 pachatel v Union bance pokusil za pomoci výpočetní techniky převést 70. mil korun. V roce 1999 došlo v Komerční bance k podvodnému převodu 60 mil. korun na jiné účty a vkladní knížky, v roce 2002 došlo k podvodnému převodu 190 mil v GE Capital Bank (Smejkal 2015, s. 134–136).

V období druhé poloviny 90. let 20 stol. docházelo na našem území taktéž k **nelegálnímu šíření software**. Pachatelé nelegální kopie softwaru zejména prodávali, přičemž v roce 2000 dosahovala míra používání nelegálního software až 80 % (Matějka, 2002, s. 44).

V oblasti **průniku do systémů – hackingu** se udály taktéž zajímavé případy. Patří mezi ně zejména známý podvod televizní soutěže BINGO z roku 1995, v němž pachatelé modifikovali počítačový program tak, aby finanční hotovost vyhrála konkrétní osoba, nebo také česká a slovenská hackerská skupina CzERT, která od roku 1996 měnila pro zábavu vzhled internetových stránek (Matějka, 2002, s. 44–45).

Kromě pirátství a hackingu se v České republice po revoluci s využitím počítače nebo internetu začaly vyskytovat případy podvodných her typu **letadlo,** ve kterých byli lidé s vidinou vysokého zhodnocení lákáni ke vkladu peněz, avšak ve skutečnosti k žádnému zhodnocení nedocházelo. Také se začalo vyskytovat padělání platebních karet výpočetní technikou nebo výroba věčných telefonních karet. Z počátku 90. let 20 stol. byla známá činnost tzv. Kyjovské buňky, provozující podvodnou hru typu letadlo, do kterých se zapojilo dokonce 10 000 osob, avšak zisk si rozdělilo pouze 15–20 organizátorů hry (Matějka, 2002, s. 47).

S příchodem internetu v roce 1992 a následně jeho postupném rozšiřováním se rozmohly také nejrůznější formy podvodného jednání. Pachatelé v internetu nalezli možnost páchat podvody na dálku, vydávat se za někoho jiného a skrývat svoji identitu (Smejkal, 2015, s. 133–134).

V počátcích pachatelé využívali neopatrnosti a neznalosti samotných uživatelů internetu. Jednalo se o případy **podvodných finančníků**, kteří se neprávem honosili nejlepšími ratingy od různých agentur a slibovali zázračné zisky z obchodů s měnami, komoditami, či

cennými papíry, přitom si vytvářeli vlastní webové stránky a komunikovali přes běžně dostupné emailové adresy (Matějka, 2002, s. 62).

Další prvotní podvody byly spojeny s **nabízením sexuálních služeb** na internetových seznamkách. Pachatelé takových inzerátů pod příslibem těchto služeb požadovali dobíjecí kupony předplacených telefonní karet (Matějka, 2002, s. 61).

S rozrůstající dostupností internetu začaly být páchány podvody, s nimiž se setkáváme do současné doby. S využitím elektronické komunikace začali pachatelé šířit nepravdivé informace – **Hoax**, nebo v emailech rozesílat různé podvodné zprávy o výhrách v loteriích, převodech peněz, nedoplatcích, podnikatelských záměrech, neuhrazených fakturách apod. Jedná se o **Nigerijské dopisy**[10], jejichž cílem je vylákat a zneužít citlivé údaje nebo peníze (Smejkal, 2015, s. 141–142).

S rozvojem nakupování přes internet se rozmohly podvody spojené s nakupování zboží na inzertních stránkách a jeho nedodáním, podvodné internetové obchody – e-shopy nabízející neexistující zboží nebo padělky a díky internetovému bankovnictví vznikly i podvodné metody jako phishing pharming, skimming, vishing, smishing (Smejkal, 2015, s. 137–138), jejichž objasnění je mimo jiné předmětem kapitoly č. 4.

Jakmile se kybernetická kriminalita objevila a rozrůstala, začala mnohdy přesahovat hranice jednoho státu. Pachatelé zjistili, že se tím šance na jejich dopadení snížily, proto v Evropě vznikla myšlenka sjednotit právní regulaci této trestné činnosti.

Dne 23.11.2001 byla vydána na mezinárodní úrovni Úmluva Rady Evropy o kybernetické kriminalitě, kterou Česká republika v roce 2013 ratifikovala a implementovala z ní vycházející závazky do trestního zákoníku[11]. Obsahuje hmotněprávní a procesně právní závazky, přičemž upravuje některé aspekty mezinárodní spolupráce za účelem efektivnějšího a snadnějšího trestního stíhání pachatelů. Úmluva definuje činy, které mají být jednotlivými členskými státy kriminalizovány a stanoví znaky těchto činů (Kolouch, 2016, s. 332–333).

Na vývoj IT kriminality měly značný vliv tedy určité zásadní momenty. Byl to zejména nástup osobních počítačů, vznik počítačových sítí (zejména Internet), vzdálený přístup k počítačům a exponenciální růst možností mobilní telefonie včetně využívání anonymních tzv. předplacených karet (Smejkal, 2015, s. 74), resp. vynález telefonu vůbec (Matějka, 2002, s. 19).

[10] Též Scam 419.

[11] Např. do trestného činu „*Neoprávněný přístup k počítačovému systému a nosiči informací"* podle § 230 trestního zákoníku, trestného činu „*Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat*" podle § 231 trestního zákoníku, nebo trestného činu „Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi" podle § 270 trestního zákoníku.

3 Trestněprávní stránka podvodného jednání

Definici podvodného jednání obecně, nalezneme v kapitole č. 1.2 Podvodné jednání. Z užšího pojetí, z hlediska kriminality a právní úpravy se jedná o jednání proti majetku, které naplňuje již zákonem stanovené znaky. Podle společenské škodlivosti je kvalifikováno buď jako trestný čin podle zákona č. 40/2009 Sb., trestní zákoník (nejčastěji podvod podle § 209), nebo jako přestupek podle zákona č. 251/2016 Sb., o některých přestupcích (nejčastěji podvod podle § 8/2a bod. 3).

Páchání podvodného jednání v prostředí informačních a komunikačních technologií (dále IT) z hlediska kriminality, právní úprava České republiky speciálně neupravuje. Rovněž **ne každé podvodné jednání je** podle právní úpravy České republiky **kvalifikováno přímo jako podvod**, proto jsou v této kapitole uvedeny i další jednání, která do podvodu z hlediska kriminálního jednání přesto spadají, vycházejí z něj, úzce s ním souvisí, nebo jsou jeho nejčastějším cílem. Cílem této kapitoly je tedy seznámit s protiprávními činy, kterých se pachatelé při uvádění v omyl v IT prostředí dopouští z protiprávního hlediska.

3.1 Trestní jednání ve vztahu k podvodu

Trestný čin podle trestního zákoníku je *„protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně*.“ Velmi podstatným znakem trestného činu je, že k *„trestní odpovědnosti za trestný čin **je třeba úmyslného zavinění**, nestanoví-li trestní zákon výslovně, že postačí zavinění z nedbalosti*“, přičemž již *„ pokus trestného činu je trestný podle trestní sazby stanovené na dokonaný trestný čin.“* (Zákon č. 40/2009 Sb., § 13, § 21).

3.1.1 Podvod – trestný čin proti majetku

Trestný čin *„Podvod*“ podle § 209 trestního zákoníku spáchá ten, *„kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou[12], bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.“* (Zákon č. 40/2009 Sb.).

„Uvedení v omyl je jednání, kterým pachatel předstírá okolnosti, které nejsou v souladu se skutečným stavem věci.“ Uvedení v omyl může být spácháno konáním (např. předložení padělku, neoprávněné telefonování), opomenutím (např. zpravidla zamlčení podstatných skutečností) nebo konkludentním jednáním (např. využití služby s úmyslem nezaplatit). Při

[12] Částka přesahující 5.000,- Kč včetně.

uvedení v omyl může jít i pouze o nepravdivou informaci, zvláště když není zvykem v běžném životě si pravdivost podávaných informací ověřovat. V soudní praxi jsou to typické případy osob, které se vydávají za někoho jiného, přičemž mohou předkládat padělané dokumenty (Šámal, 2009, s. 1854).

Při *„využití omylu“* jiného, sám pachatel k takovému vyvolání omylu nepřispěl, ale po rozpoznání omylu jiného jednal v příčinném vztahu k němu tak, aby sebe nebo jiného obohatil ke škodě cizího majetku (Šámal, 2009, s. 1855).

Pachatel *„zamlčí podstatné skutečnosti“*, pokud při svém podvodném jednání neuvede jakékoliv skutečnosti, které jsou zásadní nebo rozhodující pro rozhodnutí poškozeného, příp. jiné osoby. Jedná se o takové skutečnosti, které by vedly k tomu, že pokud by byly druhé straně známy, k vydání věci, nebo jiné majetkové dispozici, by ze strany poškozené nebo jiné podváděné osoby nedošlo, anebo by došlo, ale za značně méně výhodnějších podmínek pro osobu, která tyto skutečnosti zamlčela nebo v jejíž prospěch byly zamlčeny. Při zamlčení podstatných skutečností není třeba prokazovat, že si podváděná strana tyto skutečnosti mohla zjistit (Šámal, 2009, s. 1855).

Pachatelé se mnohdy podvodného jednání dopouští opakovaně, a pakliže *„jednotlivé dílčí útoky vedené jednotným záměrem naplňují, byť i v souhrnu, skutkovou podstatu stejného trestného činu, jsou spojeny stejným nebo podobným způsobem provedení a blízkou souvislostí časovou a souvislostí v předmětu útoku,“* jedná se o pokračující trestnou činnost jednoho daného trestného činu, v němž je celková způsobená škoda součtem všech dílčích jednání (zákon č. 40/2009 Sb., § 116).

Dopustí-li se pachatel podvodu podle trestního zákoníku v prostředí IT nebo v reálném světě, neexistuje rozdíl kvalifikace. Na IT prostředí např. internet, se nahlíží jako na specifické místo spáchání trestného činu a na technologii, z hlediska fyzického zařízení např. počítač, se nahlíží jako pomocný nástroj.

3.1.2 Trestné činy související s podvodem

V těchto podkapitolách jsou uvedeny další trestné činy, kterých se osoba uvádějící v omyl oběť často dopouští, buď s trestným činem Podvod souběžně (je-li způsobena škoda obohacením min. 5.000,- Kč), nebo samostatně (vznikne jiná škoda nebo újma).

Neoprávněný přístup k počítačovému systému a nosiči informací – trestný čin proti majetku

Jak bylo uvedeno v první kapitole, uvést někoho v omyl nebo využít něčího omylu lze provést i prostřednictvím technického zařízení, zejména zásahem do počítačového systému, informací, dat, programového vybavení apod. Takový zásah podle trestního zákoníku sám o sobě ale podvodem není. Jedná se o trestný čin „*Neoprávněný přístup k počítačovému systému a nosiči informací*“ podle § 230 trestního zákoníku (Šámal, 2009, s. 1855).

Šámal (2009, s. 2086) dále uvádí, že tento trestný čin v sobě zahrnuje dokonce pět různých jednání. **Neoprávněný přístup k počítačovému systému nebo jeho části** – odst. 1, („*kdo překoná bezpečnostní opatření*[13]*, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části*“). **Neoprávněný zásah do dat nebo do počítačového systému** – odst. 2 písm. a), b), d), („*kdo získá přístup k počítačovému systému nebo k nosiči informací a neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací….*“). **Falšování údajů související s počítači** – odst. 2 písm. c), („*kdo získá přístup k počítačovému systému nebo k nosiči informací a padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací …*“). **Podvod související s počítači** – odst. 3 písm. a), (spáchá-li čin uvedený v odstavci 1 nebo 2 *„v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, …*“). **Neoprávněný zásah do systému** – odst. 3 písm. b), (spáchá-li čin uvedený v odstavci 1 nebo 2 *„v úmyslu neoprávněně omezit funkčnost počítačového systému …*“).

Neoprávněný přístup je označován termínem „*hacking*,“ u něhož dochází právě k překonání bezpečnostního opatření. Ten může být cílem sám o sobě, přičemž pro naplnění základní skutkové podstaty způsobení škody není rozhodující (Šámal, 2009, s. 2087).

Většinou je průnik do systému přípravou ke spáchání jiného útoku, přičemž pachatel může za účelem neoprávněného užití dat, jejich vložení, poškození (sabotáže), pozměnění, nebo způsobení škody vytvořit a využít škodlivý program, který dokáže sám překonat zabezpečení, nejčastěji jeho slabiny. Takový program nazývaný malware je prostředkem, který musí poškozený stáhnout, nainstalovat, čehož pachatel mnohdy docílí pomocí klamavých postupů (např. podvodným emailem), aby si je poškozený sám nainstaloval nebo stáhnul (Šámal, 2009, s. 2087–2091). Počítačové systémy i nosiče informací spadají do IT a mohou být tedy prostředkem nebo cílem podvodu.

[13] Bezpečnostní opatření je jakékoliv opatření, jehož cílem je zabránit volnému přístupu k počítačovému systému nebo nosiči informací (Šámal, 2009, s. 2088).

Neoprávněné opatření, padělání a pozměnění platebního prostředku – trestný čin hospodářský

Jedním z nejčastějších cílů při podvodném jednání v IT prostředí jsou platební prostředky[14], nebo údaje pro jejich manipulaci (Šámal, 2009, s. 2143). Ten kdo platební prostředek *„sobě nebo jinému bez souhlasu oprávněného držitele opatří, zpřístupní, přijme nebo přechovává“*, se dopustí trestného činu *„Neoprávněné opatření, padělání a pozměnění platebního prostředku*“ podle § 234 trestního zákoníku (zákon č. 40/2009 Sb.). Pro naplnění skutkové podstaty tohoto činu se přitom *„nevyžaduje, aby pachatel platební prostředek použil k placení.“* (Šámal, 2009, s. 2143).

Poškození cizích práv – trestný čin proti právům na ochranu osobnosti, soukromí a listovního tajemství

„Kdo jinému způsobí vážnou újmu na právech tím, že uvede někoho v omyl, nebo využije něčího omylu,“ naplní skutkovou podstatu trestného činu *„Poškození cizích práv*“ podle § 181 trestního zákoníku (zákon č. 40/2009 Sb.).

Tímto podvodným jednáním jsou poškozena tedy jiná práva než majetková, ale musí dojít k úmyslnému způsobení vážné újmy, což je např. větší odliv zákazníků, ohrožení politické kariéry, ztráta větší zakázky při podnikání, neuzavření důležité smlouvy (Šámal, 2009, s. 1640).

Větší odliv zákazníků v oblasti IT kriminality může nastat u poctivého e-shopu, za který se pachatel vydával a zákazníky podváděl např. nedodání objednaného zboží. Kdo si pak objedná u tohoto e-shopu zboží, když má negativní reference, byť neoprávněně?

Porušení tajemství dopravovaných zpráv – trestný čin proti svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství

Mnohdy jsou cílem podvodníka zprávy a informace uložené v IT. Získá-li k nim úmyslně přístup a *„poruší tajemství….b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo* c) *neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data*,“ dopustí se trestného činu

[14] Mezi platební prostředky patří platební karta, elektronické peníze, cestovní šek, šek, záruční šeková karta, směnka, příkaz k zaúčtování ve formě příkazu k úhradě nebo k inkasu (Šámal, 2009, s. 2132).

„*Porušení tajemství dopravovaných* zpráv“ podle § 182 trestního zákoníku (zákon č. 40/2009 Sb.).

V IT prostředí mohu být spáchány také trestné činy „*Úvěrový podvod*“ podle § 211 trestního zákoníku, „*Dotační podvod*“ podle § 212 trestního zákoníku, „*Pojistný podvod*“ podle § 210 trestního zákoníku, „*Padělání a pozměnění veřejné listiny*“ podle § 348 trestního zákoníku nebo prostřednictvím podvodného jednání mohou být naplněny skutkové podstaty dalších trestných činů jako „*Neoprávněné nakládání s osobními údaji*“ podle § 180 trestního zákoníku, „*Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat*“ podle § 231 trestního zákoníku, „*Vydírání*“ podle § 175 trestního zákoníku. Cílem této kapitoly bylo uvést ty trestné činy související s podvodem dle § 209.

3.2 Přestupkové jednání ve vztahu k podvodu

Z hlediska společenské škodlivosti je na mírnější porušení zákona nahlíženo jako na přestupek, který je podle Zákona o odpovědnosti za přestupky a řízení o nich (zákon č. 250/2016 Sb., § 5) definován jako „*společensky škodlivý protiprávní čin, který je v zákoně za přestupek výslovně označen a který vykazuje znaky stanovené zákonem, nejde-li o trestný čin*.“ K odpovědnosti za přestupek obecně, na rozdíl od trestného činu, „***postačí zavinění z nedbalosti,*** *nestanoví-li zákon výslovně, že je třeba úmyslného zavinění*,“ přičemž „*pokus přestupku je trestný, pokud tak stanoví zákon, a to stejně jako dokonaný přestupek.“* (Zákon č. 250/2016 Sb., § 15, § 21).

3.2.1 Podvod – přestupek proti majetku

Podvod v rámci přestupku není blíže specifikován, pouze je v daném zákoně uvedeno, že se daného přestupku dopustí ten, kdo „*úmyslně způsobí škodu na cizím majetku…“* „*podvodem,“* přičemž „*pokus je trestný.“* (Zákon č. 251/2016 Sb., §8). Jedná se o přestupek proti majetku, tedy pokud je u trestného činu vyžadována způsobená škoda 5.000,- Kč včetně, pro naplnění skutkové podstaty přestupku, způsobená škoda nesmí této částky dosáhnout.

Pachatelé se přestupkového podvodu, např. při prodeji zboží, mnohdy dopouští v blízké časové souvislosti se stejným předmětem útoku opakovaně a domnívají se, že veškerá jednání budou kvalifikována pouze jako přestupky. V momentě, kdy však výše škody za tyto stejné přestupky v celkovém součtu přesáhne 5.000,- Kč včetně, věc je kvalifikována jako trestný čin Podvod podle § 209 trestního zákoníku a každé další jednání je považováno za pokračující trestnou činnost.

4 Formy podvodného jednání

Jak se informační a komunikační technologie (dále IT) vyvíjely, pachatelé přicházeli na nové a nové formy páchání protiprávní činnosti. Způsoby provádění podvodů v IT prostředí, které jsou v této kapitole předestřeny, jsou nejen ty nejčastější, ale i ty méně časté. Cílem této kapitoly je tedy tyto formy jednotlivě popsat, vzájemně je od sebe rozlišit, poukázat, jak spolu mohou vzájemně souviset a objasnit, co je vůbec jejich cílem. Budeme-li totiž znát co nejširší paletu páchaných podvodných praktik v IT, byť i jen dílčí část, budeme mít větší šanci se jich vyvarovat nebo vhodně reagovat na formy nové, obdobné, které teprve vzniknou.

Jak uvádí Britz (2013, s. 100–101), podvodníci se vyskytovali v celé historii lidstva, v každých aspektech života a působili v každé společnosti, přičemž podvod je nejběžnější protiprávní čin.

Kyberkriminalita obecně se vyznačuje vysokou úspěšností, jelikož jsou ve virtuálním prostředí potlačeny morální aspekty, provádění operací je snadné a prováděné na dálku, prokázání odpovědnosti konkrétní osobě je mnohdy nemožné, úprava nebo vymazání údajů v tomto prostředí je snazší a nezanechává stopy. To vše, ale zejména značná důvěryhodnost výstupu z počítače, je základním předpokladem úspěšného podvodu. Kromě těchto aspektů je další, který podmiňuje úspěch pachatele. Je jím vysoká kvalifikace pachatele tohoto druhu kriminality, která se projevuje ve vysoké latenci. Pachatelé mají mnohem větší předpoklad k tomu, aby se spáchání protiprávního činu nepodařilo vůbec zjistit, případně aby se nepodařilo zjistit pachatele, příp. trestnou činnost mu prokázat. IT prostředí, zejména internet umožnil páchat podvody na dálku a vydávat se za někoho jiného, skrývat skutečnou identitu. To umožnilo opravdový zlom v možnostech páchání této trestné činnosti (Smejkal, 2015, s. 134).

Páchat IT podvody, potažmo kyberkriminalitu vůbec, proti běžné fyzické krádeži či loupeži, je výhodnější z důvodu nižšího rizika fyzické újmy, mnohonásobně vyššího zisku, nižšího trestního postihu, nižší naděje na odhalení a odsouzení (Jírovský, 2007, s. 30).

4.1 Elektronické obchodování – nejčastější forma podvodu

Největší část podvodů v prostředí IT tvoří podvody páchané na internetu prostřednictvím elektronického obchodování[15], které Sedláček (2006, s. 97) podle OECD[16] vymezuje jako *„formu podnikání prostřednictvím elektronických prostředků*“. Jedná se

[15] Též elektronická komerce, e-comerce.

[16] Organizace pro hospodářskou spolupráci a rozvoj.

o nakupování nebo prodej zboží a služeb včetně těch bankovních, mezi jednotlivci, jednotlivými spotřebiteli, domácnostmi, podnikateli, veřejnými i soukromými organizacemi, vládou. Tato činnost i samotné objednávání zboží a služeb je prováděna pomocí počítačových sítí. Dodání objednaného může být provedeno online v digitální podobě nebo off-line přepravní společností.

Tato forma obchodování je každým rokem stále oblíbenější. Je prováděna prostřednictvím internetových inzercí, bazarů, aukčních portálů, e-shopů[17] i slevových portálů, ale také někdy přímými nabídkami prostřednictvím elektronických komunikací (např. email).

Podvodná jednání, ke kterým zde dochází, jsou klasického charakteru. Jedná se o podvodné nabídky zboží, zvířat, služeb, zaměstnání, půjček, přivýdělku apod. **Společným prvkem je velmi výhodná nabídka a nízká cena**. Samotný podvod nemusí spočívat jen v nedodání zboží nebo služby. Zboží může být doručeno poškozené, zničené, v nižší kvalitě, padělané nebo zcela jiné apod. Cílem pachatele nemusí být jen finanční zisk, ale i citlivé údaje.

Společnosti Gfk FutureBuy zkoumala, co motivuje zákazníky k nákupům na internetu proti nákupům v kamenných obchodech. Z 23 zemí světa, mezi 23.000 nakupujícími osobami staršími 18 let zjistila, že nejdůležitějšími faktory jsou lepší ceny (55 %), snadnější nákup (28 %), větší výběr (26 %), rychlejší nákup a časová úspora (25 %) nebo více informací o produktu (21 %), (Gfk.com, 2016). Mezi výhody také patří možnost nákupu bez omezení otvírací doby obchodu a poskytování 14 denní zákonné lhůty pro vrácení zboží bez udání důvodu.

Při nakupování zboží hraje značný **vliv reklamy**, na kterou jsou daleko náchylnější děti a mládež. Děti od 12 let jsou pro zadavatele reklam na internetu dokonce cílovou skupinou. Podle výsledků průzkumu si až ¾ dětí od 9 let již zakládají na značkách, které se propagují i na sociálních sítích. Děti a mládež se pohybují v sociálních skupinách, ve kterých určité značky představují jakýsi společenský status ke vzájemnému srovnávání a hodnocení. ***„Kdo má iPhone, je IN***“, (Eckertová a Dočekal, 2013, s. 156–158).

Sympatizace s určitou sociální skupinou představuje nátlak. Jelikož jsou děti nevýdělečně činné, nebude pro ně pak snadnější přesvědčit rodiče k zakoupení vysněného mobilní telefonu za velmi výhodnou cenu na inzertních a aukčních portálech?

[17] Elektronický internetový obchod.

4.1.1 Platební možnosti elektronického obchodování

Veškeré instituce přesouvají své aktivity na internet, což pro ně představuje snižování nákladů i časovou úsporu. Neustále tak roste objem nabízených služeb. Podvodníci jdou s dobou, a proto se na něj stále intenzivněji zaměřují (Smejkal, 2015, s. 137).

Podvodníci při elektronickém obchodování využívají důvěřivosti lidí a **preferují zejména platbu zboží předem na účet**. Při komunikaci s oběťmi je ujišťují, že se nemusí ničeho obávat, a že mají špatné zkušenosti se zasíláním dobírky. Po připsání platby přestanou s obětí komunikovat, nebo se vymlouvají, že jim platba nedorazila, nachází se v nemocnici, v zahraničí, neměli čas balík poslat a snaží se oddálit oznámení na Policii ČR. Výjimkou není ani využívání odesílání objednaného zboží dobírkou. Po uhrazení dobírky pak nachází oběti v balících bezcenné věci (mouka, brambory, kuchyňské nádobí, apod.). V současné době také pachatelé **využívají** virtuální **kryptoměny**[18], na které si podvodně získané peníze přeposílají, či **vyžadují zaslání peněz do zahraničí** na bankovní účet, např. pomocí služby Western Union.

Kryptoměna zejména umožňuje snadnější páchání trestné činnosti z důvodu anonymity (Smejkal, 2015, s. 562), ale jelikož se veškeré provedené transakce těchto měn ukládají do veřejně přístupné databáze, tzv. blockchainu, lze prostředky vysledovat.

K možnostem platby za zboží a služby při tomto obchodování patří platba **dobírkou** platební kartou či fyzickou hotovostí, platba při **osobním odběru**, platba bankovním převodem **předem na účet** (pomocí internetového bankovnictví, poštovní složenky, bankovní přepážky), platba **platební kartou** na internetu (pomocí údajů na kartě), platba **elektronickou peněženkou, platební bránou** (např. pomocí účtu na PayPal, Gopay, PayU apod.), **virtuální měnou** – kryptoměny, nebo platba jiným způsobem (na splátky, **mobilním telefonem** – m-platby, dárkovým kuponem, stravenkami).

V ČR jsme se mohli ještě nedávno setkat s tzv. BLESK peněženkou. Jednalo se o předplacenou dobíjecí anonymní platební kartu vázající se k tel. číslu, kterou si mohl zakoupit kdokoliv. Peněženka byla často využívána k internetovým podvodům a její distribuce byla proto ukončena k 30. 4. 2017 (Penezenka.blesk.cz, 2017).

Domnění mnohých, že se zejména platební karty týkají pouze dospělých, je mylná. V současné době nabízí banky platební karty po děti od 8 do 15 let s možností internetového bankovnictví. České banky to odůvodňují tím, že děti chtějí platit kartou jako dospělí a mohou se tak učit hospodařit s penězi. Otázkou je, jak může dítě lépe hospodařit s penězi na platební

[18] Virtuální (digitální) měna, založená na kryptografii, např. Bitcoin, Litecoin, Ethereum, Ripple.

kartě, proti penězům v pokladničce. Nejedná se tedy o produkty spíše výhodné pro samotné banky, těžící na fenoménu IT a psychologické imitaci dospělosti?

O tom, že různé společnosti nabádají děti k platbám přes internet, nasvědčuje i fakt, že videoherní průmysl vydává pro děti a mládež počítačové hry, zaměřené na mikrotransakce[19].

4.1.2 Internetové inzerce a bazary

V České republice je nejznámější a nejvyužívanější internetový bazar užívaný k páchání podvodů Bazoš.cz. Existují však i další bazary, jako např. sBazar.cz, Hyperinzerce.cz, Annonce.cz, i-Bazar.cz, Letgo.cz, kde hrozící riziko není o nic menší. Tyto internetové bazary jsou zaplněny mnohdy velmi výhodnými nabídkami zboží a službami, proto je někdy již při prvotním seznámení se s inzerátem prakticky nemožné zjistit, zda jde o podvod. Pachatelé nevyužívají jen bazary pro své nabídky, ale také všemožné specificky zaměřené internetové stánky např. na finanční půjčky, podnájmy, práci, zvířectvo apod., na kterých je možné vložit nabídku či poptávku. Zapomínat nesmíme ani na inzerci na sociálních sítích nebo aplikace k tomuto účelu určené na mobilní telefony a tablety.

Založit si podvodný inzerát nebo se na internetovém bazaru zaregistrovat za účelem podvodného obchodování je velmi snadné. To prakticky vyžaduje pouze základní uživatelské znalosti, což je bezesporu jedním z důvodů, proč jsou tyto podvody nejrozšířenější. Poté stačí napsat text inzerátu, vložit případně obrázek zboží nalezený na internetu, nastavit cenu zboží na neodolatelnou a čekat, kdo se ozve.

Kazuistika

Pachatel na Bazoši zveřejnil inzerát s nabídkou prodeje herní konzole za tehdy velmi výhodnou cenu 4.600,- Kč. Na inzerát reagovali poškození, kterým pachatel přislíbil zaslat zboží po uhrazení ceny předem na účet. Po odeslání peněz však pachatel poškozeným nic neodeslal a přestal s nimi komunikovat. Škoda přesáhla 5.000,- Kč, čímž se dopustil trestného činu podvodu (Usnesení Nejvyššího soudu, 2015b).

Pachatelka masivně inzerovala na webovém serveru www.jobs.cz a v deníku Metro fiktivní kampaň na obsazování do komparsů k filmům, natáčení filmů, reklam, modelingu, hostesingu. Podmínkou bylo zaslání menší hotovosti předem na účet, kdy poté se odmlčela. Všem poškozeným způsobila škodu 772.300,- Kč (Usnesení Nejvyššího soudu, 2015c).

[19] Jedná se o drobné platby ve hrách za různá vylepšení nebo urychlení herní činnosti.

Podvodník na internetu inzeroval nabídku přivýdělku spočívajícím v naplňování obálek. Za jednu naplněnou obálku sliboval až 30,- Kč, ale kdo měl o přivýdělek zájem, musel uhradit poplatek 660,- Kč. Po jeho uhrazení se pachatel odmlčel. Tímto způsobem podvedl přes 17 tisíc osob, čímž si vydělal přes 7,5 mil. korun (Honus, 2016).

Velkou část podvodů tvoří také velmi výhodné nabídky nebankovních půjček. Podmínkou pro jejich poskytnutí je uhrazení příslušného poplatku. Po jejich uhrazení se inzerent odmlčí a půjčku neposkytne (Žídek, 2018).

4.1.3 Aukční portály

Aukční portály slouží taktéž k nakupování a prodeji použitého nebo nového zboží či služeb, formou aukce. Cena se určuje během dražby a dochází k soutěži kupujících, kolik jsou ochotni za nabízený produkt zaplatit.

Existují čtyři podvodná jednání při aukci. Nedoručení zboží, nepravdivé údaje o stavu zboží skladem, skryté poplatky a vlastní příhozy pod jinou identitou kvůli zvýšení ceny zboží. V USA tvořily v roce 2004 aukční podvody 71,2 % všech podvodů. Tento počet se snížil o více než 10 % v roce 2010, jelikož si spotřebitelé více uvědomili možných rizik podvodu, dražební společnosti z obavy o ztrátu zákazníků učinily ochranná opatření a rostoucí diverzifikace kriminality na internetu poskytla více příležitostí pro kriminálníky (Britz, 2013, s. 101).

V ČR je nejvyužívanějším aukčním portálem Aukro.cz, na kterém bylo v roce 2016 registrováno 3,8 milionů uživatelů (Aukro.cz, 2003–2018). Existují i méně známé portály např. Avízo.cz, Portalaukci.cz, A.cz, iKup.cz, Miniaukce.cz, Odklep.cz. V zahraničí je nejznámější eBay.com. Jelikož lze Aukro již považovat za značně rozšířenou obchodní síť, v následující části je na něj blíže zaměřeno.

Aukro vzniklo v roce 2003, spolupracuje s Policií ČR, garantuje profesionální služby a uvádí, že na něm již probíhá 99,98 % bezproblémových nákupů. Dochází zde nejen k prodeji a nákupu zboží v rámci dražeb, ale rovněž za pevné ceny (Kup teď). Nabízené zboží je rozděleno do několika kategorií, např. Elektronika, Děti, Móda, Sport, atd., nalezneme zde téměř cokoliv včetně zboží, které se v českých obchodech ani neprodává. Podstatným krokem Aukra bylo v roce 2008 zavedení služby tzv. „*Ochrany kupujících*," která spočívá v tom, že pokud registrovaný kupující na Aukru zakoupí od registrovaného uživatele zboží, které mu nedodá nebo s ním není spokojen, Aukro kupujícímu proplatí plnou výši ceny zboží, včetně poštovného. U každého registrovaného uživatele je vedena veřejně přístupná historie prodejů zboží včetně jejich hodnocení od kupujících. Ověřeným a garantovaným obchodníkům je udělováno osvědčení „*Aukro+"* (Aukro.cz, 2003–2018).

Kazuistika

Pachatel se zaregistroval na Aukru, aby mohl prodávat zboží a pod svým uživatelským účtem zde nabízel mobilní telefon Apple Iphone 4S 16Gb za tehdy výhodnou cenu 11.420,- Kč. Telefon vydražil poškozený, ale po odeslání peněz na bankovní účet pachatele, tento poškozenému nic neodeslal a stal se nekontaktním (Usnesení Nejvyššího soudu, 2015a).

4.1.4 Podvodné e-shopy

Podvodné elektronické obchodování probíhá také prostřednictvím falešných obchodů, respektive e-shopů. Elektronický obchod je založen na totožné myšlence jako obchod kamenný, jen existuje v kyberprostoru. Od obvyklých internetových stránek se odlišuje nabídkou zboží, které lze vkládat do virtuálního nákupního košíku, v němž se zobrazuje celkové množství a cena zboží. E-shopy mnohdy podporují vyhledávání zboží podle stanovaných parametrů (cena, značka, kategorie apod.), které si lze nastavit. U jednotlivého zboží se mnohdy zobrazuje jeho dostupnost, hodnocení uživatelů nebo možnost porovnání s jiným zbožím. Pro dokončení odeslání objednávky je vyžadováno vyplnění doručovací adresy, zvolení způsobu dodání a platby. Potvrzení o objednávce s její rekapitulací bývá odesíláno automaticky na námi zadaný email. Mezi typické poctivé e-shopy patří např. Alza.cz, Mall.cz, CZC.cz, přičemž některé kamenné obchody také mívají i své e-shopy na internetu, např. Euronics.cz, Okay.cz.

Podvodné e-shopy vznikají za účelem vylákání velkého množství finančních prostředků a po krátké době zanikají. Zboží nabízejí za velmi nízkou cenu a vyžadují úhradu platby předem na účet, což mívají jako jediný způsob možnosti platby. Získané peníze zpravidla vyvádějí mimo území ČR za účelem anonymizace finančních toků, nebo využívají kryptoměny (Policie ČR, 2017), jak již bylo uvedeno.

Obvykle v těchto e-shopech chybí či nefungují kontaktní údaje, mají negativní nebo smyšleně pozitivní reference, mohou mít neúplné či podezřelé obchodní podmínky, příp. nemají žádné (Szotkowski, 2016).

Kazuistika

Dvojice pachatelů ve věku 37 a 39 let z Přelouče si na internetu z Dominikánské republiky založili dokonce několik takových podvodných, avšak regulérně vypadajících e-shopů s elektronikou, kuchyňským vybavením, televizory apod. Tyto e-shopy opatřili nepravdivými kontaktními údaji a obchodními podmínkami a podvodně získané prostředky si převáděli expresními službami právě do Dominikánské republiky, čímž minimálně 1000 poškozených okradli o bezmála 4.000.000,- Kč (Matzner, 2016).

4.2 Sociální inženýrství

Pro úspěšný podvod v IT prostředí bývá mnohdy využívána technika tzv. sociálního inženýrství. V zásadě jde o přesvědčování, ovlivňování nebo manipulaci lidí, s cílem je přimět k určité činnosti nebo získat informace, které by však tito lidé neposkytli. Smyslem je navodit dojem, že situace, ve které se nacházíme, je odlišná oproti skutečnosti. Hlavní podstatou této techniky je nevyužívání technických nástrojů či přístupů, např. k prolomení hesla. V podstatě je jednodušší pro pachatele, když jim heslo prozradí sama oběť (Kolouch, 2016, s. 186).

Právě díky promyšlené manipulaci dochází pomocí této techniky ke zneužití nejslabšího článku počítačového systému, kterým je důvěřivý člověk. Počítačový systém je závislý na lidech, což představuje bezpečnostní slabinu v selhání lidského faktoru, využití podvědomého zvyku či vlastnosti jedince. Sociální inženýrství lze též označit za „*umění klamu*“ (Jírovský, 2007, s. 195–196).

McCarthy a Weldon Siviy (2010, s. 57) uvádí, že tato technika je mnohdy využívána ke vpravení malwaru do počítačového systému a „*používá obecné znalosti lidského chování k přesvědčení uživatelů, aby porušili svá vlastní bezpečnostní pravidla*.“ Je využívána při phishingu, pharmingu, podvodných emailech, telefonických hovorech, elektronické komunikaci, prohledávání webu apod.

4.2.1 Phishing

Phishing[20] je podvodná metoda, při které pachatel odesílá smyšlenou zprávu, často email, v němž se vydává za banku, správce sítě apod., přitom využívá mnohdy tzv. spoofingu[21] a požaduje sdělení konkrétních údajů, nebo provedení operace, např. kliknutím na odkaz. Cílem je získat citlivé údaje jako hesla, přihlašovací údaje k internetovému bankovnictví, osobní údaje, PIN platební karty nebo údaje k dalším finančním službám nebo obchodování na internetu. Díky fiktivní emailové adrese vytváří představu věrohodnosti. Takové zprávy rovněž mohou obsahovat odkaz na podvodnou webovou stránku např. banky, která vypadá vzhledově totožně jako originální a slouží ke sběru údajů o klientech a přístupových údajů. V počátcích byly tyto emaily psány špatnou češtinou a nesrozumitelnými formulacemi, v dnešní době jsou na vysoké jazykové i grafické úrovni (Smejkal, 2015, s. 138). V současné době jsou cílem phishingu také přihlašovací údaje např. k sociálním sítím nebo herním účtům[22].

[20] V překladu rybaření.

[21] Změna záhlaví emailu, přičemž se útočník vydává za někoho jiného.

[22] Např. Steam, Microsoft Store, PlayStation Network, Xbox Live, Google play, App store, apod.

Podvodné stránky využívají mnohdy nepozornosti samotných uživatelů a místo originální stránky např. www.mojebanka.cz, odkazují na falešnou stránku www.mojebanka.cn, což zaznamená málokdo (Kopecký et al., 2015, s. 97).

Příchozí podvodná phishingová zpráva mnohdy obsahuje malware, který si ale údaje může získat sám. Phishing se šíří pomocí elektronické komunikace, nejen emaily, ale i pomocí instant messaging (Facebook Messenger, Whatsapp, Viber), sociálních sítí samotných, SMS a MMS zprávami, falešnými aplikacemi, chatovacími místnosti, resp. veškerou cestou, která umožňují oslovit obrovské množství uživatelů (Kolouch, 2016, s. 246–247).

Kopecký et al. (2015, s. 97–98) upozorňují, že tvůrci phishingových stránek se zaměřují i na chytré mobilní telefony a tablety. Pomocí podvodných kódů, které jsou integrovány přímo do www stránek, se snaží přimět uživatele, aby si do těchto zařízení nainstalovali různé aplikace. Jedná se však o nebezpečný malware běžící na pozadí, který ovládá přijímání sms zpráv, tedy i autorizační zprávy z internetového bankovnictví.

Tvůrcem phishingové stránky může být v současné době téměř kdokoliv, jelikož na internetu lze nalézt mnoho návodů, jak takové stránky vytvořit.

Kazuistika

V roce 2006 vytvořil 14 letý chlapec z Japonska podvodnou webovou herní stránku, díky které ukradl identitu 94 osob. Jednalo se o prvního obviněného nezletilce z phishingu (McCarthy a Weldon-Siviy, 2010, s. 127).

V České republice proběhly v období 2014–2016 čtyři masivní phishingové útoky. Prostřednictvím emailů byly zasílány falešné výzvy k zaplacení dluhu s hrozbou exekuce nebo obyčejné zprávy s Vánočním přáním, které vyzývaly k otevření přílohy obsahující malware, jenž si získával citlivé údaje. Dále byly zasílány falešné oznámení od „*České pošty*“ o dodání zásilky, obsahující odkaz na stažení takového malwaru a také byly zasílány falešné zprávy vyzývající k nainstalování bezpečnější a jednodušší aplikace pro práci s emailovou schránkou v mobilních telefonech, po jejichž nainstalování měli pachatelé k mobilnímu telefonu plnou kontrolu (Kolouch, 2016, s. 250–261).

V roce 2012 se na sociální síti Facebook nacházel odkaz na phishingovou stránku novamaturita.kvalitne.cz, která slibovala výsledky státních maturit ihned. I když se prokazatelně jednalo o podvod, během 24 hodin tyto stránky navštívilo 2632 návštěv, které provedly celkem 4145 zobrazení (Voříšek, 2012). Pakliže tedy žáci středních škol tento podvod nedokázali již v prvopočátku odhalit, jak by asi reagovali na podobnou situaci žáci základních škol?

4.2.2 Vishing, Wangiri, Smishing, Pharming

Vishing je podvodná metoda s využitím telefonického rozhovoru. Jde o telefonický phishing, pomocí něhož se pachatel snaží od klienta získat citlivé údaje. Obvykle se používá nikoliv klasické hlasové telefonie, ale VoIP[23], případně namísto autentického hlasu pachatel mnohdy využívá hlasu generovaného počítačem nebo automatického záznamníku (Smejkal, 2015, s. 138).

Pachatelé se prostřednictvím mobilních telefonů taktéž někdy pokouší o získání finančních prostředků formou nevyžádaných hovorů ze zahraničí (**wangiri**[24]). Útočník jen prozvoní telefonní číslo oběti a čeká, pokud oběť zavolá zpět. Hovor se neuskuteční, je přesměrován na volání za cenově vysoký tarif, přičemž podvodník profituje z propojovacích poplatků (Echo24.cz, 2017).

Smishing je SMS phishing probíhající obdobně jako vishing. Pachatel zašle oběti SMS zprávu s informací, že byla zjištěna podezřelá transakce na jeho bankovním účtu. V této SMS zprávě je uvedeno tel. číslo, na které má oběť zatelefonovat. Na daném tel. čísle se představí útočník jako pracovník banky, přičemž pro získání důvěry požádá oběť o kontrolní údaj nebo kód doručený v příchozí podvodné SMS. Následně od oběti získá údaje za účelem podvodného získání peněz z jeho účtu. Novější metoda má v SMS zprávě přímo odkaz na internetové stránky, kam se má oběť přihlásit, na což navazuje pharming (Smejkal, 2015, s. 138–139).

Příchozí podvodné nevyžádané SMS zprávy nabádají ke kliknutí na odkaz. Jde např. o podvodné výzvy k vyzvednutí zásilky, podvodné výhry a další záminky jako u phishingu.

Pharming[25] je podvodná metoda využívající malware, který uživatele v případě záměru přihlášení do svého internetového bankovnictví přesměruje na podvodné stránky, vypadající jako stránky banky, kde klient zadává přihlašovací údaje a heslo. Pharming se realizuje na dvou úrovních. Útočník neoslovuje přímo klienty banky, ale napadne konkrétní server banky. Pokud se mu podaří změnit záznam bankovního serveru, tak všichni, kdo jsou napojeni na daný server a zadají správnou internetovou adresu bankovnictví, dostanou se namísto správné stránky na stránku falešnou, daného podvodníka. Nebo útočník provádí útok na konkrétní počítačový systém, kde je upravená tabulka (s názvem „*hosts*“ u operačního systému MS Windows), obsahující dvojici IP adres a odpovídajících domén, kdy poté opět po zadání konkrétní internetové adresy (URL) je zobrazena stránka podvodná (Smejkal, 2015, s. 138).

[23] Voice over Internet Protocol.

[24] Wangiri je zkratka „*one ring and cut*“ (jednou prozvonit a típnout).

[25] V překladu farmaření.

4.3 Malware

Malware je jakýkoliv škodlivý software využívaný buď k narušení obvyklé činnosti počítačového systému, zisku dat nebo informací, nebo získání přístupu k samotnému systému (Kolouch, 2016, s. 204). Aby plnil svoji naprogramovanou funkci mnohdy skrytou, musí být vpraven do počítačového systému. Je mnoho způsobů, jak toho docílit, podvodnými praktikami nevyjímaje. Podvody v obecném slova smyslu spolu s malware v prostředí IT hrají významnou roli a jsou hojně využívány. V podstatě stačí uvést uživatele v omyl zprávou, informací, sdělením, s cílem jediného kliknutí na určité místo, soubor, odkaz nebo nainstalovat program.

Tyto škodlivé programy jsou distribuovány ***prostřednictvím přenosných paměťových médií***[26]; ***staženého nebo nainstalovaného programu/aplikace*** z neznámého zdroje, v němž je implementován; ***kancelářských dokumentů***[27], v němž je implementován; ***prostřednictvím emailu*** v příloze; ***přiloženého přímého odkazu na webové stránky***. Mnohdy je přiložen u phishingové zprávy, hoaxu, spamu, nebo se nachází ***ve falešném antiviru***, v němž je implementován a nabízí se sám zdarma k vyzkoušení a stažení (Kolouch, 2016, s. 211–214).

Malware může mít celou řadu podob a mnohé druhy jsou pojmenovány podle své činnosti (Kolouch, 2016, s. 204). Jedná se o hackerské programovací nástroje (Jírovský, 2007, s. 59), kterými jsou např. viry, červi, Trojské koně, Rootkity, Ransomware, Adware a další. Existuje ale i např. malware, který skrytě těží kryptoměny nebo snímá stisk jednotlivých kláves.

Viry potřebují hostitele, šíří se jako viry biologické, bez vědomí uživatele (Šámal, 2009, s. 2091). Jejich následkem může být neškodné vyhrávání melodie, zahlcení systému, změna dat nebo jejich zničení, smazání, nebo celková destrukce systému (Kolouch, 2016, s. 207).

Červi dokáží automaticky rozesílat kopie sebe samých, hostitele nepotřebují. Umožňují útočníkovi částečnou nebo plnou kontrolu nad počítačovým systémem, mohou jej i vyřadit z provozu. Mohou rozesílat automaticky samy sebe, způsobují rozsáhlé síťové přenosy, které mohou zahltit počítačové sítě (Šámal, 2009, s. 2092).

Trojské koně skrývají část programu fungující určitým způsobem, kterým si přeje útočník. Jsou využívány k zachytávání informací při přihlašování, shromažďují uživatelská data, hesla, platební transakce, která vzápětí odesílají útočníkovi (Britz, 2013, s. 38, 137). Mohou být využívány také k modifikaci, mazání, blokování, narušování běhu počítačového systému či sítí, kopírování dat, usnadnění ovládnutí počítače na dálku (Kolouch, 2016, s. 208).

[26] CD, DVD, USB disky.

[27] Dokumenty a soubory např. s koncovkou doc, dosx, xls, avi.

Rootkity škodlivé nejsou, ale slouží k maskování samotného malware. **Adware** způsobují nepříjemné zobrazování a vyskakování reklamy, různých sdělení, fiktivních výher, mění domovskou stránku, shromažďují informace a historii (Kolouch, 2016, s. 205–222).

Ransomware je vyděračský a **podvodný druh malware**. Omezuje nebo zabraňuje uživateli v řádném přístupu k počítačovému systému, celému nebo jen části do doby, než je útočníkovi zaplaceno výkupné. Tento druh malware se objevuje i na mobilních zařízeních s operačním systémem (Smejkal, 2015, s. 148). Náhled na známý ransomware je v příloze.

Malware působí prakticky v jakémkoliv operačním systému, pro který byl vytvořen. Z hlediska mobilních zařízení je nejčastěji zaměřen právě na Android z důvodu vysoké rozmanitosti a dále jeho neaktualizace, přičemž v roce 2016 bylo 85 % smartphonů vybaveno Androidem. Většina zařízení s tímto systémem totiž neumožňuje aktualizovat na aktuální verzi, která opravuje chyby předchozí verze (Statista – The portal for statistics, 2017).

4.4 Spam, Scam, Hoax

Na spam lze nahlížet jako na zneužití elektronických komunikací, spočívajícím v náhodném nebo nahodilém zasílání nevyžádaných zpráv prostřednictvím elektronických komunikací. Mohou být nápomocny k internetovým podvodům (Britz, 2013, s. 82). Emailové adresy jsou získávány z různých zdrojů, např. marketingovými firmami, z internetové diskuse nebo z registrací různých služeb zdarma (Matějka, 2002, s. 69–70).

Pro spam je typické hromadné šíření. Nejčastěji obsahuje informace z oblasti: ***obchodního nebo reklamního sdělení***, ***medicíny a zdraví*** – nabídky produktů k redukci váhy, léčivých a kosmetických přípravků; ***edukace*** – nabídky kurzů, tréninků; ***financí*** – nabídky půjček, možnosti přivýdělku; ***hoax*** – řetězové zprávy; ***pornografie*** – nabídka přípravků ke zvýšení potence, odkazy na pornografické stránky; ***náboženství***, ***politiky***, ***kriminality*** – odkazy na stránky s malware, nebo jej přímo v příloze obsahují (Kolouch, 2016, s. 232).

Pokud spam obsahuje kriminální nebo jiný podvodný obsah, je označen termínem **scam**, jehož účelem je získat důvěru adresáta díky sociálnímu inženýrství a přimět jej k vykonání požadovaného, např. navštívení webové stránky, otevření emailu, zaslání finančních prostředků. Mezi scam lze zařadit i phishing, podvodné nabídky a loterie, malware, hoax, dárcovský scam, facebookový scam, scam 419 (Kolouch, 2016, s. 235).

Předmětem scamu jsou velmi výhodné podvodné nabídky práce, zaměstnání, pronájmu bytů, seznámení s osobou opačného pohlaví, která se do oběti vzápětí zamiluje[28], informace

[28] Romance scam.

o vysokých výhrách, sdělení že byl na nás najat nájemný vrah[29], ale také prodeje automobilů, vzácných zvířat apod. (Root.cz, 1998–2017). Některé scamy bývají velmi sofistikované a k jejich účelu mohou být vytvořeny webové stránky neexistujících bankovních institucí, společností apod. Obětem také mohou být útočníkem zasílány falešné dokumenty, fotografie, certifikáty k podpoření důvěryhodnosti (Hoax.cz, 2000–2017). Pokud ještě k samotné škodě nedojde, může být scam kvalifikován jako pokus podvodu, vydírání apod.

Známými scamy jsou **Nigerijské dopisy**. Nástupem elektronické komunikace se tato forma masově rozrostla a umožňuje v krátkém čase oslovit milióny uživatelů. Odesílatel většinou vystupuje jako osoba z Nigerie, ale nejsou výjimky osob z jiných zemí a ve zprávě nás informuje, že získala, zdědila nebo spravuje majetek nebo peníze a potřebuje pomoc při jejich převodu ze země, s příslibem vysoké odměny. Následně požaduje finanční prostředky za nečekané administrativní poplatky, čímž se převod majetku oddaluje (Hoax.cz, 2000–2017).

Tyto zprávy jsou zasílány v cizím jazyce nebo v češtině, kdy mohou být gramaticky chybné, některé věty nelogické s nesprávným slovosledem. Pachatelé požadují posílat peníze do zahraničí, jejichž majitelé bývají bílými koňmi. S konkrétními případy včetně těch nejnovějších scamů se lze seznámit na webové stránce hoax.cz.

Hoax patří mezi formu spamu, příp. scamu a v překladu znamená žert, smyšlenka, novinářská kachna. Jedná se o řetězové sdělení „*pošli dál, pokud to nepošleš dalším 20 lidem, stane se…*“, obsahující nepravdivé, zavádějící, zkreslení nebo jiné informace. Mnohdy uvádějí prosby o pomoc, varují před útoky, popisují nebezpečí, posílají petice, pyramidové hry, výzvy, dopisy štěstí, prohlášení slavných, žertovné zprávy, prezentují obrázky a videa, hrají si na zvířátka (Kolouch, 2016, s. 240).

Na internetových stránkách E-Bezpečí uvádí Kopecký (2008), že přibližně 80 % dětí ve věku 6–15 let tyto zprávy přeposílají dál a umožňují jejich šíření. Tyto zprávy čtou a v kombinaci s jejich nekritickým přístupem u nich mohou vyvolávat obavu, strach, nedůvěru čímž působí na jejich psychiku.

Kazuistika

V dubnu 2017 se objevil nebezpečný hoax zaměřený na děti a mladistvé. Jednalo se o hru vyzývající plnit destruktivní úkoly až následně sebevraždu. Jako důkazy byly předestírány informace o stovkách údajných sebevražd, ke kterým mělo dojít v Rusku v období 2015–2016.

[29] Příchozí zpráva, že byl na nás najat nájemný vrah, který požaduje peníze, mnohdy kryptoměnu, lze kvalifikovat dokonce jako trestný čin vydírání podle § 175 odst. 1 trestního zákoníku.

Když se informace o hře dostaly do České republiky, začaly se následně šířit mezi uživateli sociálních sítí. Jednalo se však o hoax a marketingový tah, jehož cílem bylo nalákat do určitých sociálních skupin (Kopecký, 2017a).

Jako podvodný scam lze uvést příchozí email. *„ Ahoj drahý, Jsem Advokát Victoria Josef, mám pro vás zprávu týkající se mého zemřelého klienta, který nese stejné příjmení jako vy, ... On odešel za částku ve výši 2.700.000 $. Mezitím, jeho banka chce převést výhody na některou z jeho rozšířené člena rodiny… Advokát Victorie Joseph.“* (Kolouch, 2016, s. 237).

4.5 Skimming

Jedná se o metodu podvodného kopírování platebních karet pomocí speciálního nainstalovaného kopírovacího zařízení na čtečkách karet umístěných v bankomatech, restauracích, obchodech, apod., prostě všude tam, kde je možno platit platební kartou (Smejkal, 2015, s. 138).

Jde o složitější metodu krádeže dat, která zahrnuje čtení a nahrává osobních informací zakódovaných na magnetickém proužku karty. Získané údaje jsou po uložení pachatelem znovu zakódovány na magnetický proužek sekundární nebo fiktivní karty, který je přesnou kopií originálu. Kopírovací zařízení existují v různých tvarech a velikostech a obsahují v sobě i miniaturní kamery, díky kterým pachatel získá PIN kód (Britz, 2013, s. 132).

4.6 Sociální sítě a podvodné profily

Sociální sítě se staly velmi oblíbeným prostředkem současné komunikace. Lidé zde navazují přátelství, sdružují se zde do skupin, shromažďují a sdílejí informace, vyměňují si zkušenosti nebo se zde jen setkávají a udržují sociální kontakt. Zároveň ale představují našeho „*velkého virtuálního bratra*“, jenž je bankou našich údajů, dat a informací. Pakliže jejich uživatelé nedodržují bezpečnostní pravidla nebo prozrazují a zveřejňují na sebe velké množství informací, představuje to výživnou půdu pro zloděje, podvodníky, sociální inženýry.

Sociální sítě jako Facebook nebo Google + jsou zaměřeny univerzálně pro všechny. Existují i sítě zaměřené přímo na studijní skupiny (Spolužáci), profese (Linkedln), sdílení videosouborů (Youtube), online komunikaci (messengery, Skype, WhatsApp,), seznamování a chat (Lidé.cz, Líbimseti.cz, Badoo.cz), blogování (Twitter), pokládání otázek (Ask.fm).

Na sociálních sítích, zejména Facebooku, který je nejoblíbenějším, se začal rozšiřovat nový druh podvodu ohrožující jak děti tak dospělé. Pachatelé si zakládají fiktivní profil konkrétní osoby naklonováním a požádají oběť o „*znovupřidání*“ mezi přátele, což oběť

zpravidla učiní. Následně pachatel oběť pod smyšlenou legendou požádá o pomoc při obnově fiktivně zablokované služby, účtu, emailu nebo při zapomenutí PINU k bankovnímu účtu a přesvědčí ji, aby mu poslala své tel. číslo, na které si odešel kód nebo PIN k obnovení přístupu k zablokované službě. Ve skutečnosti je to potvrzovací kód k provedení platby u mobilního operátora, tzv. m-platba (Kopecký, 2013). Takový falešný přítel nám může také poslat odkaz na zavirované stránky, fotografie, video nebo na phishingové stránky (Kopecký, 2017c).

Kazuistika

Pachatel si založil falešný profil ženy a přes sociální síť zaslal žádost o přátelství oběti. Ta v domnění, že se jedná o její známou, žádosti vyhověla a pachatel ji požádal o zaslání drobné platby 40,- Kč. Společně však s touto žádostí o platbu jí poslal formulář k platbě, do něhož oběť vyplnila nutné údaje pro platbu platební kartou, díky čemuž pachatel získal údaje a poté odčerpal z účtu oběti více než 7.000,- Kč (Perdoch, 2014).

4.7 Podvodné formy zaměřené na seniory

V IT prostředí využívají pachatelé i podvodné formy, které jsou zaměřeny primárně na seniory. Počty seniorů, kteří se stávají terčem podvodů, každý rok strmě narůstá. Pachatelé je kontaktují pomocí nevyžádaných emailů, mobilních telefonů, inzerátů, sociálních sítí a nabízejí jim různé **předražené zboží a nevýhodné smlouvy**. Navíc stále častěji k podvodnému jednání vůči nim využívají citového vydírání (MVČR, 2015, str. 62).

Rozšiřování internetových služeb, diskutování a obchodování na internetových aukcích, vyhledávání informací a práce s emaily jsou důvody, proč jsou senioři na internetu stále aktivnější. Proto se také stále častěji stávají obětí kybernetické kriminality (Kopecký, 2015a), vzhledem ke stárnoucímu obyvatelstvu lze nadále předpokládat zvyšování kriminality vůči nim.

Senioři se také setkávají na internetu s podvodnými e-shopy, podvodnými elektronickými aukcemi, podvodnými inzeráty, podvodnou reklamou, scamem, podvodnými objednávkami, hoaxem, podvodnými m-platbami, phishingem a malwarem **(**Kopecký a Szotkowski, 2013), další rizika představují nejrůznější podvodné smlouvy, výhodné hypotéky a úvěry uzavírané prostřednictvím internetu (E-Bezpečí, 2017).

4.7.1 Vnuk

Tato forma podvodu se objevila již v roce 2003, následně se rozšířila a je užívána i v současné době. Pachatelé si touto metodou mnohdy vydělají statisícové částky.

Podvodníci se při ní zaměřující na seniory, pod smyšlenou identitou navážou důvěrný vztah a poté se z nich snaží vylákat peníze (MVČR, 2015, str. 62).

Problematice této trestné činnosti je věnována zvýšená pozornost. Záměrem pachatelů je vždy získat finanční hotovost či adekvátní majetkovou hodnotu tak, aby při páchání nezanechali žádné stopy. Pachatelé si totiž velmi dobře uvědomují nevýhodu vysokého věku, který hraje významnou roli při dokazování trestné činnosti (MVČR, 2017, str. 24–25).

Podvod spočívá v tom, že si pachatel v telefonním seznamu vybere typická jména seniora jako Cecílie, Františka, apod. Následně mu zatelefonuje a vydává se za příbuzného, nejčastěji vnuka. Vzápětí požaduje půjčit narychlo co nejvíce peněz na nutné výdaje, např. na koupě bytu, vozidla apod. Pokud senior rozpozná, že mu nevolá ten, kdo se představuje, pachatel s omluvou, že jde o omyl, zavěsí. Jakmile seniora přesvědčí, mnohdy díky výmluvnosti, sdělí, že pro peníze pošle svého známého, kterému senior vzápětí peníze skutečně předává. Konverzace probíhá následujícím způsobem. Pachatel: *„Ahoj babi.“* Senior: *„Kdo volá? To jsi ty Filípku?“* Pachatel: *„Ano babi, tady je Filip,*“ a dále pokračuje (Sasínová, 2003).

4.7.2 Romance scam

Specifickým druhem scamu, kterému senioři podléhají je Romance scam. Cílem pachatele je v tomto případě s obětí navázat romantický vztah a vylákat od ní peníze. Mnohdy je tato podvodná nevyžádaná zpráva podpořena fiktivní atraktivní fotografií osoby opačného pohlaví. Tento podvod neohrožuje pouze seniory, ale prakticky veškeré uživatele internetu. Podvodné příběhy, s nimiž se oběť seznamuje, jsou zaměřeny na případy, kdy scammer potřebuje půjčit nebo darovat peníze na vyřízení pasu nebo letenky; na přílet nebo na cestu k oběti; na převod peněz na účet oběti; na zaplacení daní; na náklady spojené s léčbou; na poplatky za telefon/internet, aby mohl pokračovat v komunikaci; na urgentní léčbu rodičů; na nečekaný zdravotní problém, kdy je hospitalizován apod. (Kopecký, 2016).

Tento scam se šíří nejen tradičním emailem, ale rovněž sociálními sítěmi a online seznamkami. V minulosti byly tyto zprávy převážně v anglickém jazyce, dnes bývají lokalizovány do češtiny, což umožňuje oslovit značné množství osob (Kopecký, 2016).

Kazuistika

Seniorka Martina: *„Na Facebooku jsem se seznámila s přítelkyní. Moc dobře jsme si povídaly a občas i zavolaly. Najednou se odmlčela a já pak s hrůzou zjistila, že je vážně nemocná. Požádala mě o padesátitisícovou půjčku, kterou jsem jí ráda poskytla. Pak už se neozvala a telefon nebere*." (Janouš, 2014).

5 Pachatelé a oběti

Bez pachatelů a jejich obětí by kriminalita v prostředí infomačních a komunikačních technologií (dále IT) neexistovala. K pochopení tohoto druhu kriminality a následné ochraně před ní, je třeba se zabývat i tím, kdo je jejím pachatelem, jaká je jeho charakteristika, jaké jsou jeho motivy a kdo jsou jeho oběti, což je cílem této kapitoly. Jelikož je práce zaměřena na žáky základních škol, je důležité se zabývat i jejich odpovědností za protiprávní jednání.

5.1 Charakteristika pachatele

V současné době jsou nové technologie snadno dostupné a masově rozšířené, proto stoupá i počet těch, kteří se této trestné činnosti dopouští. Získávají jako celá společnost určité znalosti a dovednosti v IT oblasti. Pachatelem se může stát za určitých okolností každý, pokud k tomu dostane příležitost, má úmysl a motiv a přijde s technologiemi do styku, děti a mladiství nevyjímaje. Lze však stanovit určitou charakteristiku pachatele, a to podle motivace, oblastí činnosti, vlivu vnějšího okolí a osobních schopností a předpokladů (Kuchta, 2016, s. 12–13).

Jedná se většinou o vzdělaného a inteligentního člověka, který ovládá potřebné dovednosti s určitou mírou přizpůsobivosti. **Může jím být ale kdokoli** z jakékoliv společenské vrstvy. Navenek se od ní neodlišuje, nevzbuzuje pozornost a jeho osobnostní rysy nevykazují patologii. Trestnou činnost páchá sám v izolaci, obvykle nemá záznam v trestním rejstříku. Mnohdy pracuje na pozici, ve které vzbuzuje respekt i důvěru společnosti (Kuchta, 2016, s. 13).

Většina pachatelů kyberkriminality využívá IT jako prostředek k páchání trestné činnosti. To pro někoho může představovat jediný impulz, díky němuž se takové činnosti dopustí. Gottfredsonova a Hirchiho obecná teorie, zabývající se příčinami vzniku kriminality předpokládá, že nebude-li mít pachatel podmínky nebo příležitost vůbec ke spáchání protiprávního jednání, nedojde k němu (Válková a Kuchta, 2012, s. 112–115). Z dané teorie vyplývá, že pachatelem se může stát kdokoliv, kdo by bez IT k páchání trestné činnosti ani nepřistoupil a může se tedy odlišovat od jakéhokoliv typu pachatele trestného činu.

Typologie pachatelů IT kriminality se podle Matějky (2002, s. 7) značně liší od pachatelů tradiční kriminality[30], v níž je typickým pachatelem člen podsvětí, mnohdy s vazbami na jiné kriminální živly. Pachatelé IT kriminality bývají lidé mimo běžné zločinecké struktury.

Dle rozborů této trestné činnosti vyplývá, že se jedná o osoby často s vyšším vzděláním, mohou to být někdy až geniální samoukové, nadprůměrně vynalézaví v určité oblasti. Jsou

[30] Tradiční krádeže, vloupání, ublížení na zdraví, výtržnosti.

psychicky silní, sebevědomí, někdy ale taktéž duševně labilní s komplexy. Jejich jednání však postrádá prvky násilí a tradiční trestné činnosti (Válková a Kuchta, 2012, s. 607).

Významnou roli hrají psychologické charakteristiky při pohybu na internetu, kterými jsou anonymita, změněné vnímání pachatele, vnímaná malá rizika, časová a místní flexibilita (pachatel má víc času na přemýšlení), snazší překonávání ostychu a plachosti do míry porušení zákona (Kuchta, 2016 s. 13–14).

Obecně bychom se mohli domnívat, že se bude jednat spíše o mladší pachatele, kteří více inklinují k novým technologiím a inovacím. Gřivna a Polčák (2008, s. 48–53) však uvádí, že věk pachatelů kyberkriminality je čím dále širšího spektra a není výjimkou pachatel starší 40 let. Tito lidé získali znalosti již před desítkami let, věnují se technologickému rozvoji a jdou s dobou. Většina pachatelů bývají muži z důvodu obecného zájmu o techniku, vyšších ambic nebo z důvodu, že kyberprostor chápou jako loveckou výpravu nebo nedobytné území.

V odborné literatuře rozděluje Smejkal (2015, s. 488) pachatele IT kriminality do 5. kategorií. **Zaměstnanci** poškozené organizace. **Průnikáři –** hackeři, počítačoví odvážlivci s anarchistickým cílem. **Příslušníci organizovaného zločinu**, využívající počítače zejména k výrobě padělků, skryté komunikaci, praní špinavých peněz. **Profesionálové**, převážně pracující za peníze, kteří pronikají nebo odhalují státní a obchodní utajované informace, útočí na infrastrukturu jiného státu. **Osoby blízké věku dětí a mladistvých**, příliš nepřemýšlející o svém jednání a následcích, nepředpokládají odhalení.

V současné době se komunita pachatelů kyberkriminality významně změnila. Již se nejedná o jednotlivce, ale o profesionály, kteří svoji činnost páchají s cílem profitu či jsou zapojeni do organizovaného zločinu (Kolouch, 2016, s. 183). Důkladnější znalosti a dovednosti v IT prostředí jsou pro pachatele jistě výhodnější z důvodu nižšího rizika odhalení. S vývojem technologií se i pachatelé vyvíjí, zdokonalují, přizpůsobují a vymýšlí nové taktiky k páchání trestné činnosti. Obecně můžeme ty, kteří páchají tuto trestnou činnost sofistikovaně a nelze je běžnými policejními postupy odhalit, označit za profesionály. Na druhé straně může být pachatelem trestného činu i neprofesionál, tedy ten, kdo nemá vůbec široké znalosti a je běžným uživatelem takových technologií, anebo jím může být někdo mezi těmito mantinely.

5.1.1 Motivy pachatele

Motivy pachatelů kybernetické kriminality se mění především s ohledem na jejich věk a osobnostní vyspělost, příležitost, vědomosti a dovednosti pachatele. Podvodné jednání je z hlediska práva přiřazováno k majetkové kriminalitě, ve které je převažujícím motivem obvykle peněžní zisk a osobní obohacení (Smejkal, 2015, s. 486–487).

Porada a Straus (2013, s. 512) pak motivy pachatelů kyberkriminality rozdělili na ***motivy zištné,*** pohnutkou je finanční zajištění pachatele, vidina snadného a relativně bezpečného zisku; ***touha po výsadním postavení –*** v podnikatelském prostředí jde o snahu zlikvidovat konkurenci; ***touha dokázat svou intelektuální převahu –*** např. nad tvůrci ochranných programů nebo zaměstnavatelem, ***touha překonat pocit nedocenění svých schopností –*** neúspěšnost v reálném životě, neschopnost navazovat kontakty, pocit odloučení od svých vrstevníků apod. vede k nutkání kompenzace těchto nedostatků; ***krycí motivy k utajení jiné trestné činnosti –*** obavy z odhalení jiného trestného činu, který ani nemusí mít povahu počítačové kriminality, mohou vést k „*zametání stop*"; ***politické nebo jiné ideologické motivy***.

Rak a Porada (2013, s. 22–23) opět motivy páchání v závislosti na samotném vývoji této trestné činnosti rozdělili do třech období. V první polovině 90. let 20 století byla motivem pachatelů zejména zvědavost, nuda, hravost, pomsta, nespokojenost, touha překonat technologie, bezpečnostní opatření nebo sám sebe. Ve druhé polovině 90. let 20. století se k uvedeným motivům navíc přidala vidina velkého finančního prospěchu a začátkem 21. století dále dosahování politických cílů s využitím technologií až vedení informační války.

Podněty vedoucí k páchání protiprávního jednání v IT prostředí se také zabývala z řad zahraničí americká odbornice na počítačové technologie Debra Littlejohn Shinder (2002, s. 112–119), která mimo peněžního zisku a politických motivů uvádí z důvodu zábavy, hněvu, pomsty a dalších emocí, sexuálního impulzu nebo psychické nemoci.

5.2 Odpovědnost žáků 2. stupně základních škol za podvodné jednání

Žáky II. stupně základních škol můžeme podle Zákon o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže označit za děti a mladistvé. Tento zákon uvádí, že *„dítě je osoba do 15 let věku a osoba mladistvá je osoba od 15 let věku do 18 let věku. Od 18 let věku je osoba považována za osobu dospělou.“* (Zákon č. 218/2003 Sb., § 2).

Dopustí–li se dítě trestného činu, resp. činu jinak trestného, není podle § 11 trestního řádu trestně odpovědné. Policejní orgán po provedeném prověřování trestní věc podle § 159a trestního řádu odloží (zákon č. 141/1961 Sb.). Po skončení prověřování ale může dítěti na návrh státního zástupce „*soud pro mládež uložit, a to zpravidla na základě výsledků předchozího pedagogicko-psychologického vyšetření, tato opatření: výchovnou povinnost, výchovné omezení, napomenutí s výstrahou, zařazení do terapeutického, psychologického nebo jiného vhodného výchovného programu ve středisku výchovné péče, dohled probačního úředníka, ochrannou výchovu, ochranné léčení.“* (zákon č. 218/2003 Sb., § 93).

Dopustí–li se mladistvý trestného činu, resp. provinění, trestní odpovědnosti se nevyhne. Policejní orgán po provedeném prověřování proti mladistvému zahájí trestní stíhání a za přítomnosti obhájce vyslechne mladistvého jako obviněného. Po skončení vyšetřování předloží policejní orgán státnímu zástupci spis s návrhem na podání obžaloby (zákon č. 141/1961 Sb., § 160, § 166). Mladistvému soud pro mládež podle zákona o soudnictví ve věcech mládeže uloží buď *„**výchovné opatření**: dohled probačního úředníka, probační program, výchovné povinnosti, výchovná omezení, napomenutí s výstrahou*“, *„**ochranné opatření**: ochranné léčení, zabezpečovací detence, zabrání věci, zabrání části majetku, ochranná výchova*“, nebo *„**trestní opatření**: obecně prospěšné práce, peněžité opatření, peněžité opatření s podmíněným odkladem výkonu, propadnutí věci, zákaz činnosti, vyhoštění, domácí vězení, zákaz vstupu na sportovní, kulturní a jiné společenské akce, odnětí svobody podmíněně odložené na zkušební dobu (podmíněné odsouzení), odnětí svobody podmíněně odložené na zkušební dobu s dohledem, odnětí svobody nepodmíněné.“* (Zákon č. 218/2003 Sb. § 15, § 21, § 24).

*„V trestním řízení proti mladistvým je třeba dbát toho, aby vyšetřování, projednávání a rozhodování jejich trestních věcí bylo svěřováno takovým osobám, jejichž znalost otázek souvisících s výchovou mládeže zaručí splnění výchovného účelu řízení. Orgány činné podle tohoto zákona také spolupracují s příslušným orgánem sociálně-právní ochrany dětí a Probační a mediační službou.“ „**Trestní sazby** odnětí svobody stanovené v trestním zákoníku **se u mladistvých snižují na polovinu**, přičemž však horní hranice trestní sazby nesmí převyšovat pět let a dolní hranici jeden rok.“* (Zákon č. 218/2003 Sb., § 36, § 31).

Dopustí–li se dítě přestupku, policejní nebo správní orgán takový přestupek odloží, nezjistí-li jiné skutečnosti. **Dopustí–li se mladistvý přestupku** odpovědnosti se nevyhne (zákon č. 250/2016 Sb., § 76, § 56).

Za přestupky lze mladistvému uložit správní trest *„napomenutí, pokuta, zákaz činnosti, propadnutí věci nebo náhradní hodnoty, zveřejnění rozhodnutí přestupku*“ nebo *„ochranná opatření: omezující opatření a zabrání věci nebo náhradní hodnoty*“. *„Horní hranice sazby pokuty se u mladistvého snižuje na polovinu, přičemž však nesmí přesahovat částku 5000 Kč.“ „Při ukládání správního trestu mladistvému se přihlíží k jeho osobnosti včetně jeho věku a rozumové a mravní vyspělosti, jakož i k jeho osobním poměrům tak, aby jeho další vývoj byl co nejméně ohrožen.*“ (Zákon č. 250/2016 Sb., § 35, § 51, § 56, § 57).

Policejní orgán, správní orgán, respektive všechny *„**státní orgány**, pověřené osoby, školy, školská zařízení a poskytovatelé zdravotních služeb, popřípadě další zařízení určená pro děti, jsou povinni oznámit obecnímu úřadu obce s rozšířenou působností skutečnosti, které*

nasvědčují tomu, že jde o děti…“ , „*…které spáchaly trestný čin nebo, jde-li o děti mladší než patnáct let, spáchaly čin, který by jinak byl trestným činem, opakovaně nebo soustavně páchají přestupky podle zákona upravujícího přestupky nebo jinak ohrožují občanské soužití*.“ (Zákon č. 359/1999 Sb., § 6, §10). Toto oznámení se podává orgánu sociálně právní ochrany dětí, který řeší všechny oblasti života dítěte, tedy nejen trestněprávní, ale také výchovné, sociální, výukové, zdravotní i rodinněprávní

Dětem a mladistvým je třeba věnovat zvláštní péči, což stanovuje LZPS[31] čl. 34 (Usnesení č. 2/1993 Sb.), proto se k nim musí přistupovat vždy specificky, individuálně a s výchovným záměrem. Způsobu přistupování k nim, se věnuje dokument OSN „*Úmluva o právech dítěte*“ nebo na mezinárodní úrovni dokument č. 11 z roku 2008, „*Doporučení výboru ministrů členským státům o evropských pravidlech pro mladistvé pachatele.“*[32]

5.3 Oběti

Z pohledu zákona se na oběť nahlíží jako na fyzickou osobu „*které bylo nebo mělo být trestným činem ublíženo na zdraví, způsobena majetková nebo nemajetková újma nebo na jejíž úkor se pachatel trestným činem obohatil.“* (Zákon č. 43/2013 Sb., § 2). Pokud tato újma byla uzpůsobena fyzické osobě, fyzické osobě podnikající, právnické osobě nebo státu, považuje se podle trestního řádu za poškozeného v trestním řízení (zákon č. 141/1961 Sb.). Pro účely této práce budeme dále termín oběť a poškozený užívat jako synonyma.

Raka a Porada (2013, s. 22–23) uvádí, že dopady na ty, proti kterým byla kyberkriminalita namířena, kopírovaly její historický vývoj. V počátcích to byly velké firmy, státní instituce, později i menší firmy a země s rozvinutou infrastrukturou, následně banky, telekomunikační společnosti, až nakonec byla namířena na samotné občany.

Oběti kybernetické kriminality jsou mnohdy ve značné míře neochotni oznamovat takové protiprávní jednání orgánům činným v trestním řízení nebo jej ani vůbec nezjistí. Poškozené organizace, podniky, banky, apod., kterým byla újma způsobena, mají větší obavy z veřejnosti. Pokud by se o jejich zranitelnosti a neomylnosti dozvěděla, mohlo by to poškodit jejich ekonomický úspěch a zvýšit nedůvěru v bezpečnosti jejich služeb (Kshetri, 2010, s. 42).

[31] Listina základních práv a svobod.

[32] V originálním názvu „*Recommendation CM/Rec (2008) 11 on the European Rules for juvenile offenders subjject to sanctions or measures*.“

Pakliže ale není kyberkriminalita oznamována, dochází ke zkreslování evidované kriminality a odborných publikací. V neposlední řadě to ztěžuje prověřování policejních orgánů, jelikož více zjištěných poznatků k trestné činnosti znamená vyšší šanci na dopadení pachatele.

Dnes nejčastěji využívané podvodné praktiky jsou zaměřeny primárně na jednotlivce a **potencionálními oběťmi jsou všichni uživatelé IT**, přičemž **ohroženou skupinou obětí jsou děti**, které mají k těmto technologiím běžný přístup. „*Děti jsou online v tak raném věku, že si už kolem jedenácti let osvojily technické dovednosti dospělých. Jenže si stále nevytvořily odpovídající intelektuální a emocionální zralost potřebnou ke správným rozhodnutím, kterým musí na internetu čelit*.“ Protiprávní jednání nemusí rozpoznat, mohou jej podcenit či zanedbat bezpečnostní pravidla, o nichž ani nemusí vědět (Krčmářová, 2012, s. 57).

Druhou ohroženou skupinu tvoří senioři. Pachatelé si seniory vybírají záměrně proto, že nejsou schopni se ubránit útoku, jejich svědectví není přesné, čímž se snižuje riziko dopadení, obávají se svěřit, jsou osamělí a odhalení trestného činu by trvalo dlouho (Nováková, 2013)

Stane-li se senior obětí, mnohdy neví, jak má vůbec reagovat, postupovat, zda má kontaktovat polici. Mnohdy vzhledem k nízké úrovni IT gramotnosti také nezná způsoby, jak si např. zablokovat nežádoucí obsah, jak si nastavit antispamovou a antivirovou ochranu, jak využívat help linku, jak si někoho zablokovat, kdo jej obtěžuje v komunikaci apod. Proto je nutné na tento stav reagovat, především preventivním opatřením, přičemž nejefektivnější způsob prevence, zejména představuje přímá edukace seniorů (Kopecký a Szotkowski, 2013).

Rovněž Venglářová (2007, s. 1–2) v příloze časopisu Policista zmiňuje důvody, které seniorům brání oznámit trestný čin. Jsou to poruchy smyslů (nepřečtou si informace o pomoci, nemohou dobře telefonovat), zdravotní stav (snížená pohyblivost), stud, izolace (sami nemají možnost nikam zajít, jsou sledováni), neochota svědčit proti blízkým osobám, strach ze sekundární viktimizace. Dalšími důvody jsou podle Smolíka a Kajanové (2012) a Tomáška (2010) strach z pomsty, vzniklou škodu senioři považují za zanedbatelnou, neznají možnosti odborné pomoci, nedůvěřují soudům a policii.

Vzrůstajícímu trendu kyberkriminality je potřeba věnovat pozornost. Obecně ji charakterizuje vysoká latentnost, vysoká míra tolerance společnosti včetně lhostejnosti k hrozbám, skutečná i domnělá anonymita pachatele, obtížná identifikace a celý proces dokazování. Proto je třeba nejen represivního působení na pachatele, ale je třeba se zabývat otázkou prevence trestné činnosti v této oblasti, stejně jako otázkou možné ochrany společnosti před touto činností (Kolouch, 2016, s. 14).

6 Prevence kriminality informačních a komunikačních technologií

Šestá kapitola se věnuje preventivnímu působení proti podvodnému jednání v prostředí informačních a komunikačních technologií (dále IT), potažmo kriminalitě v tomto prostředí, zaměřené na žáky základních škol, což je velmi klíčové téma. Cílem této kapitoly je odpovědět na otázku, jakou roli hraje škola, rodina, stát a další subjekty v boji proti tomuto druhu kriminality.

Prevence je velmi častý pojem, s nímž se nesetkáváme pouze v lékařské ordinaci, proto jistě téměř každý ví, že jeho synonymem je ochrana. Prevenci můžeme definovat jako *„souhrn opatření zaměřených na předcházení nežádoucím jevům.“* Prevenci dělíme na **primární prevenci** (zabraňuje vzniku nežádoucím jevům), **sekundární prevenci** (nežádoucí jevy se snaží včas odhalit a pracovat s nimi v rané fázi vzniku) a **terciální prevenci** (snaží se zabránit dalším komplikacím, když nežádoucí jevy běží), přičemž primární prevence se dále dělí na nespecifickou a specifickou (Průcha et al., 2013, s. 219).

Nespecifická primární prevence podporuje žádoucí formy chování bez důrazu na konkrétní riziko. Aktivity se zaměřují na efektivní využívání volného času, zdravého životního stylu, upevňování zdraví. Vedou ke zdravému rozvoji osobnosti a k odpovědnosti za své jednání. Součástí je budování a rozvoj bezpečného prostředí snižující riziko nebezpečných situací. Nejpřirozenějším prostředím pro realizaci tohoto druhu prevence je prostředí kvalitní rodinné výchovy, respektive rodina vůbec a dále škola (Miovský et al., 2015, s. 144).

Specifická primární prevence se zaměřuje na předcházení konkrétních rizik a měla by mít komplexní, holistický charakter. Měla by být doménou základních škol, které po rodině představují klíčové edukační činitele, které zásadně formují osobnost dítěte. Specifická primární prevence se dělí na všeobecnou, selektivní a indikovanou (Miovský et al., 2015, s. 144–146).

Všeobecná primární prevence *„je zaměřena na běžnou populaci dětí a mládeže bez rozdělování na méně či více rizikové skupiny, zohledňuje pouze její věkové složení a případná specifika daná např. sociálními nebo jinými faktory*.“ Jde o programy pro větší počet osob, např. celá třída nebo menší sociální skupina. Pro tuto prevenci postačuje vzdělání školního metodika prevence (Miovský et al., 2010, s. 42).

Selektivní primární prevence *„se zaměřuje na skupiny osob, u kterých jsou ve zvýšené míře přítomny rizikové faktory pro vznik a vývoj různých forem rizikového chování, tj. jsou více*

ohrožené než jiné skupiny populace.“ Pracuje se s menšími skupinami nebo jednotlivci, přičemž je kladen důraz na odpovídající vzdělání preventisty (Miovský et al., 2010, s. 43).

Indikovaná primární prevence „*je zaměřena na jedince, kteří jsou vystaveni působení výrazně rizikových faktorů, případně u kterých se již vyskytli projevy rizikového chování. Snahou je zde podchytit problém co nejdříve, správně posoudit a vyhodnotit potřebnost specifických intervencí a neprodleně tyto intervence zahájit*.“ Tento stupeň prevence vyžaduje konkrétní vzdělání preventisty (Miovský et al., 2010, s. 43).

Prevenci v oblasti kriminality lze obecně definovat jako „*zabránění trestné činnosti ještě předtím, než k ní dojde.*“ **Primární prevence kriminality** je zaměřena na předcházení, odvrácení a snižování příležitostí k samotnému páchání kriminality. Směřuje k obecné populaci a místům, které nejsou kriminalitou zatíženy. Usiluje o aktivní podporu společensky akceptovatelného chování. **Sekundární prevence kriminality** zahrnuje intervenci vůči osobám nebo místům, která byla identifikována jako riziková, náchylnější ke kriminalitě. Adresáti této prevence jsou vymezeni konkrétněji, např. podle teritoria, věku, způsobu ohrožení apod. **Terciální prevence kriminality** je zaměřena nejen na pachatele, oběti a na místa, kde se kriminalita již odehrává. Jejím cílem je zabránění dalšího páchání kriminality (Chalupová, 2012, s. 11–16).

Matějka (2002, s. 77–80) uvádí, že boj proti IT kriminalitě se v podstatě neliší od boje proti ostatním formám kriminality obecně. V boji proti této kriminalitě považuje preventivní strategii za stejně důležitou, jako strategii represivní. „*Ačkoli se názory na žádoucí poměr těchto složek liší, je pravdou, že jedna bez druhé nemůže dost dobře existovat, a že žádný boj proti kriminalitě nemůže být efektivní bez působení prevence i represe zároveň.“* Samotnou prevenci IT kriminality rozdělil na psychologickou a technologickou a dodává, že aby bylo možno nad touto kriminalitou zvítězit, musí působit obě preventivní složky současně.

Psychologickou prevenci definuje jako „*taková opatření, která napomáhají vytvářet povědomí o nemorálnosti a společenské nepřijatelnosti právem zakázaných činů.*“ Smyslem je zvyšování stupně společenské akceptace práva (Matějka, 2002, s. 78).

Technologická prevence zahrnuje v první řadě zabezpečení samotného IT proti virům, hackerům, crackerům, zejména instalováním aktualizací programů nebo používáním aktualizovaných antivirových programů. Dokonalá technologická ochrana však neexistuje, protože je otázkou času, kdy bude nový ochranný systém prolomen (Matějka, 2002, s. 80).

V zásadě lze konstatovat, že při trestné činnosti hrají klíčovou roli tři faktory – lidé, místa a situace, které musíme při prevenci komplexně zohledňovat (Chalupová, 2012, s. 17).

6.1 Prevence ve školství

IT kriminalitu lze zařadit mezi sociálně patologický jev. Ve školním prostředí se však užívá pojem **rizikové chování**. Miovský et al. (2015, s. 144) rizikové chování definuje jako *„takové vzorce chování, v jehož důsledku dochází k prokazatelnému nárůstu zdravotních, sociálních, výchovných a dalších rizik pro jedince a společnost*.“ Vzorce takového chování je soubor fenoménů, které je možno podrobit vědeckému zkoumání a lze jej ovlivňovat intervencemi preventivními i léčebnými. Rizikové chování dokonce nahrazuje v minulosti častěji užívaný pojem sociálně patologické jevy, který klade přílišný důraz na společenskou normu, je normativně laděný a stigmatizující.

Děti jsou skupinou, která je sociálně patologickými jevy ohrožena nejvíce a prevence bývá mnohdy ve společnosti podceňovaná, jelikož se její výsledky dostavují s časovým zpožděním. Obtížné je obzvlášť měřit, jak ji skutečně ovlivňují konkrétní preventivní programy (Kopecký et al., 2012, s. 44–45).

Základní legislativní dokument upravující ve školách a školských zařízeních primární prevenci rizikového chování je **zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání** (dále školský zákon), který pro předcházení vzniku rizikového chování ukládá povinnost vytvářet podmínky pro zdravý vývoj dětí, žáků, studentů (MŠMT, 2013, s. 15).

Stěžejní roli v primární prevenci rizikových projevů chování u dětí a mládeže má **Ministerstvo školství, mládeže a tělovýchovy** (dále MŠMT). V oblasti této prevence plní několik stěžejních úkolů. Stanovuje základní strategie v daných oblastech, stanovuje priority na budoucí období, podporuje vytváření vazeb a struktur se subjekty, které realizují nebo se spolupodílejí na vytyčených prioritách a dále podporuje vytváření materiálních, finančních a personálních podmínek nezbytných pro samotnou realizaci prevence ve školství, včetně nezbytné metodické podpory subjektů působících v primární prevenci. MŠMT si uvědomuje, že při formování osobnosti mladého člověka je velmi významné právě období školního vzdělávání, protože to, co se v tomto období nepodaří, se v dospělosti velmi obtížně napravuje (MŠMT, 2013, s. 3).

V roce 2001 byl vypracován ze strany MŠMT významný koncepční dokument **Národní program rozvoje vzdělávání**, tzv. Bílá kniha, ve které bylo zmiňováno preventivní působení pouze v obecné rovině. V rámci zvyšování kvality vzdělávání zde byla zmíněna důležitost posilování prevence v oblasti rizikového chování, přičemž byly mimo jiné zmíněny i zvyšující

se počty dětí s delikventním až kriminálním jednáním (Kotásek et al., 2001, s. 40). Prevence IT kriminality zde tedy nemá privilegované postavení.

S vývojem doby, zejména v kontextu technologickém, ekonomickém a politickém bylo třeba vymezit a přizpůsobit aktuální strategii vzdělávacího systému. Přestože platnost Bílé knihy nebyla formálně ohraničena a její účinnost nebyla oficiálně ukončena, období pro naplnění jejich deklarovaných cílů uplynulo. Vznikl tedy nový koncepční a strategický dokument na vysokém stupni obecnosti, **Strategie vzdělávací politiky České republiky do roku 2020,** kterým Bílá kniha pozbyla platnost (MŠMT, 2014a, s. 3–4).

Tento dokument poukazuje, že ve světě a vzdělávání stále významnější místo zastávají IT, přičemž je koncipován jako rámec vzdělávací politiky vymezující prioritní cíle[33] a k jejich dosažení rámcově určuje směry intervence. K tomuto účelu využívá jednotlivé strategické dokumenty nižšího řádu, mající těsnější vazbu na prováděná opatření (MŠMT, 2014a, s. 25, 43).

Jedním ze strategických dokumentů nižšího řádu Strategie vzdělávací politiky České republiky do roku 2020, který je v souladu s jejími cíli a konkrétně již reaguje na progresivní vývoj IT, je **Strategie digitálního vzdělávání do roku 2020** (dále Strategie digitálního vzdělávání)**.** Zde nacházíme zmínku o rizicích kybernetické kriminality v rámci cíle podpory kvalitní výuky. Je zde uváděno, že využívání digitálních technologií má významný sociální aspekt a základní vliv na rozvoj informační společnosti. Jedním ze zásadních předpokladů pro život v této informační společnosti je schopnost rozlišit přínosy a rizika využívání digitálních technologií, a to jak v osobní, tak ve společenské rovině. Proto se musí nastavit nová pravidla, která s využíváním digitálních technologií bezprostředně souvisejí (legislativa, etická pravidla, doporučená sbírka pravidel a zásad – netiketa, autorská práva, obchod s osobními daty, ***prevence kyberkriminality***, online bezpečí, kybernetické bezpečí). (MŠMT, 2014b, s. 14–15).

Strategie digitálního vzdělávání má jasnou vizi, aby vzdělávací systém zajišťoval každému jedinci výbavu takových kompetencí pro uplatnění v informační společnosti a využívání nabídky otevřeného vzdělávání v průběhu celého života (MŠMT, 2014b, s. 11). Jejími prioritními cíli je zapojovat moderní technologie do vyučování, rozvíjet tzv. **digitální**

[33] Snižování nerovnosti ve vzdělávání včetně posilování celoživotního vzdělávání, odpovědné a efektivní řízení vzdělávacího systému, podpora kvalitní výuky učitele.

kompetence[34] a **informatické myšlení**[35] žáků i učitelů a podporovat vývoj inovací a jejich šíření (MŠMT, 2014b, s. 15–16). Do vzdělávání tak byly zavedeny pojmy jako digitální vzdělávání[36], digitální kompetence respektive digitální gramotnost nebo informatické myšlení.

Primární prevence IT kriminality vzhledem k uváděné strategii digitálního vzdělávání a samotné rostoucí kybernetické kriminalitě je tedy v současné době velmi aktuální téma, kterým je třeba se zabývat a implementovat jej do výchovy a vzdělávání. Rovněž odborník na IT kriminalitu Kolouch (2016, s. 15) uvádí, že je výchova a vzdělávání v IT oblasti nezbytná. Proto je důležité budování gramotnosti a vzdělávání v této oblasti, respektive seznámení s hrozbami, riziky a negativy, by mělo být součástí výuky na všech úrovních školství.

V oblasti primární prevence rizikového chování u dětí a mládeže pak vydalo MŠMT konkrétnější dokumenty, a to **Národní strategii primární prevence rizikového chování na období 2013-2018** (dále Národní strategie primární prevence) a **Metodické doporučení k primární prevenci rizikového chování u dětí, žáků a studentů ve školách a školských zařízeních** (dále metodické doporučení) vedené pod č.j. 21291/2010-28. Oba dokumenty se zaměřují na předcházení rozvoje rizikového chování, konkrétně na rizikové formy komunikace prostřednictvím multimedií (MŠMT, 2010, s. 1), delikventní chování a další trestné činy a přečiny (MŠMT, 2013 s. 9), do čehož lze zařadit i IT kriminalitu.

Národní strategie primární prevence je základní koncepční dokument v oblasti primární prevence rizikového chování dětí a mládeže, v němž jsou vyjádřena základní východiska a cíle, v souladu se současným poznáním a praxí v dané oblasti. Vychází z jednání s krajskými školskými koordinátory prevence, metodiky prevence, ale také z cílů stanovených Strategiemi meziresortních orgánů a ze zkušeností předchozích koncepcí. Jejím hlavním cílem je minimalizovat vznik rizikového chování u dětí a mládeže, přičemž jako cílovou skupinu

---

[34] **Digitální kompetence (digitální gramotnost)** je pojmem ve smyslu klíčových kompetencí. Jedná se o „*soubor vědomostí, dovedností, schopností, postojů a hodnot, které jedinec potřebuje, aby využil digitální technologie a digitální média k činnostem, jako je: řešení úkolů, komunikace, nakládání s informacemi, řešení problémů, spolupráce, vytváření a sdílení obsahu a budování znalostí.“* Tyto kompetence se v dnešní době uplatňují při práci, v zaměstnání, ve volnočasových, občanských a společenských aktivitách, ale také k učení a osobnímu růstu, při zajišťování životních potřeb, a to přiměřeně, efektivně, k danému či zamýšlenému účelu, samostatně, kriticky, pružně a eticky (MŠMT, 2014b, s. 47).

[35] **Informatické myšlení** je „*způsob uvažování, který používá informatické metody řešení problémů, a to včetně problémů komplexních či nejasně zadaných. Rozvíjí schopnost žáků analyzovat a syntetizovat, zevšeobecňovat, hledat vhodné strategie řešení problémů a ověřovat je v praxi. Vede k přesnému vyjadřování myšlenek a postupů a jejich zaznamenání ve formálních zápisech, které slouží jako všeobecný prostředek komunikace. Pracuje se základními univerzálními pojmy, které přesahují současné technologie: algoritmus, struktury, reprezentace informací, efektivita, modelování, informační systémy, principy fungování ICT.“* (MŠMT, 2014b, s. 48).

[36] **Digitální vzdělávání** je „*takové vzdělávání, které reaguje na změny ve společnosti související s rozvojem digitálních technologií a jejich využíváním v nejrůznějších oblastech lidských činností. Zahrnuje jak vzdělávání, které účinně využívá digitální technologie na podporu výuky a učení, tak vzdělávání, které rozvíjí digitální gramotnost žáků a připravuje je na uplatnění ve společnosti a na trhu práce, kde požadavky na znalosti a dovednosti v segmentu informačních technologií stále rostou*.“ (MŠMT, 2014b, s. 3).

nestanovuje pouze děti a mládež, ale také rodiče, veřejnost a pracovníky v dané oblasti. Věnuje se oblastem koordinace, legislativy, vzdělávání, financování a evaluaci primární prevence včetně certifikace programů primární prevence (MŠMT, 2013, s. 3–10).

Metodické doporučení jasně stanovuje systém organizace a řízení primární prevence rizikového chování žáků, zmiňuje činnost MŠMT, Krajských úřadů, Krajských školních koordinátorů prevence, Metodiků prevence v pedagogicko–psychologických poradnách, dále ředitelů škol a školských zařízení, školních metodiků prevence a také třídních učitelů (MŠMT, 2010, s. 3–7).

Oblast primární prevence konkrétně rozpracovávají školy do svých školních vzdělávacích programů. Většina škol má vypracovaný samostatný dokument, **Minimální preventivní program**, který primární prevenci a její samotnou realizaci na škole popisuje z hlediska cílů a priorit (MŠMT, 2013, s. 15). Jedná se o hlavní nástroj školní prevence (Miovský et al., 2015, s. 146).

Náležitosti Minimálního preventivního programu pak stanovuje opět předmětné metodické doporučení. Na jeho tvorbě a realizaci se podílejí všichni pedagogičtí pracovníci, avšak **školní metodik prevence** koordinuje jeho tvorbu a kontroluje realizaci. Tento program podléhá rovněž kontrole České školní inspekci a je průběžně vyhodnocován (MŠMT, 2010, s. 8–9).

Standartní činnosti školního metodika prevence jsou uvedeny v příloze vyhlášky č. 72/2005 Sb., o poskytování poradenských služeb ve školách a školských poradenských zařízeních. Ten tak při své činnosti mimo jiné může spolupracovat nejen s orgány státní správy a samosprávy, které mají danou problematiku v kompetenci, ale také s dalšími zařízeními a institucemi působícími v dané oblasti (vyhláška č. 72/2005 Sb.).

6.1.1 Edukace žáků

Přestože problematika prevence rizikového chování má být začleněna do osnov tak, aby se stala přirozenou součástí výuky jednotlivých předmětů a školních osnov, přičemž není pojímána jako nadstandartní aktivita škol (MŠMT, 2010, s. 7–8), edukace žáků ve škole spadá zpravidla na bedra školního metodika prevence. Ten je ale zatížen mnohými oblastmi sociálně patologických jevů, přičemž svoji činnost vykonává pouze na částečný úvazek, a proto je výhodnější využívat **externího lektora**, který se určitým tématem intenzivně zabývá a je schopen zodpovědět případné dotazy. Nejefektivnější edukace u dětí spočívá pak zejména v **představování modelových kazuistik**. Preventivní a edukační efekt se znásobuje při použití fotografií, které je lépe prezentovat z případů ze zahraničí (Kopecký et al., 2012, s. 44–45).

Pozitivní výsledek prevence rizikového chování spojeného s užíváním internetu lze dosáhnout ideálním způsobem kombinací přímé edukace zaměřené na ohroženou cílovou skupinu a osoby spolupracující s touto skupinou, ale také s mediálními kampaněmi zaměřenými na jednotlivé fenomény. Podle autorů je **přímá terénní edukace** základním funkčním nástrojem prevence a základním prostředkem pro šíření informací o rizikovém chování. Další funkční formy prevence představují **nabízení alternativ k rizikovému** chování, např. nabídka volnočasových aktivit. Taktéž je důležitá prevence realizovaná předkládáním pozitivních vzorců chování rodiči, učiteli, vrstevníky (Kopecký et al., 2012, s. 44–45).

6.1.2 Edukace učitelů

Stejně jako žáci, musí být i učitelé informování o sociálně patologických jevech v oblasti IT. V případě učitelů již není nutné pracovat s kazuistikami, ale musí získat nejen základní teoretické informace (pedagogika, psychologie, IT aspekty), ale také informace o možnostech řešení jednotlivých situací v souladu s právními normami. Je podstatné jim vysvětlit, jak v jednotlivých případech postupovat. Autoři dále uvádí, že je pramálo organizací v České republice, které takový výcvik učitelům nabízejí. Jedním z mála projektů, který takový výcvik provádí je projekt E-Bezpečí (Kopecký et al., 2012, s. 47).

Aby byla realizace primární prevence efektivní, je nezbytné ji realizovat v úzké spolupráci s dalšími subjekty (např. školy, školská poradenská zařízení, zákonní zástupci, neziskové organizace pracující s dětmi a mládeží, OSPOD, Policie ČR, vysoké školy a další), které musí mít v dané oblasti dostatečné vědomosti, znalosti a zkušenosti, což dokazují výzkumy, šetření i praxe. To se týká všech, kteří přicházejí či mohou přicházet s rizikovým chováním do styku (MŠMT, 2013, s. 10, 17).

6.2 Prevence v rodině

Rodina je možná považována za základ státu, ovšem pro účely této práce lze rodinu považovat za základní jednotku, která ovlivňuje vývoj dítěte a podílí se nejen na vytváření jeho budoucnosti, ale také na samotném získávání vědomostí, dovedností a zkušeností. Dominantní vliv na mladého člověka mají bezesporu rodiče, kteří své dítě od narození vychovávají.

Pro rodiče je důležité, aby pochopili roli, kterou IT hraje v životě jejich dětí a vedli je ke správnému chování a **dodržování bezpečnostních pravidel** na internetu. Mezi důsledky nesprávné výchovy v IT prostředí lze pak uvést např. zavirování počítače spamy, hoaxy, sociální inženýrství – phishing, hacking, vyzvídání a zisk informací – krádeže identity na

sociální síti nebo zde sdílení informací, vedoucí např. ke vloupání do bytů během dovolené (Krčmářová et al., 2012, s. 56–57), ale také např. podvody při elektronickém obchodování.

Bezpečnostní pravidla v souvislosti s IT kriminalitou spočívají zejména v nesdělování osobních údajů svých ani rodinných příslušníků prostřednictvím internetu bez souhlasu rodičů; nezasílání fotografií, údajů k platební kartě a bankovnímu účtu, ani jiné osobní údaje prostřednictvím internetu bez porady rodičů; nesdělování nikdy nikomu přihlašovacích údajů ani hesel ke své internetové stránce nebo počítači, apod.; nedomlouvání schůzky s osobou, se kterou jsme se seznámili přes internet bez souhlasu rodičů, doma musí vědět, kam jdeme a proč; neklikání a neotvírání na soubory přiložené v elektronických zprávách doručených od neznámých odesílatelů; dodržování předem dohodnutých pravidel k používání počítače a internetu; pamatování pravidla, že lákavá nabídka na internetu nemusí být pravdivá; oznámení rodičům nalezení nelegálního obsahu (Krčmářová et al., 2012, s. 59). Zařadit lze také používání dostatečně silných hesel nebo používání antivirových programů.

Nejlepší prevencí v rodině je pak **proaktivní výchova**. Rodiče by si měli uvědomit, že děti přijímají celkem bez problémů to, že jsou věci, které nesmějí zatím vůbec dělat, pokud ale většinu toho, co dělat chtějí mohou – byť s určitým omezením. Efektivnější je užívání počítače s konkrétními pravidly, než striktní zákaz, který mohou navíc obejít ve škole, u kamaráda, v knihovně (Krčmářová et al., 2012, s. 59).

Počítačová gramotnost dětí je však mnohdy lepší než u **rodičů** a pokud budou rodiče za dětmi zaostávat, nemohou děti řádně kontrolovat v tom, co tam dělají, jaké weby navštěvují, čeho jsou schopné. Efektivní prevencí je tak rovněž od prvopočátku rodičovská znalost IT, povědomí o rizicích a bezpečnostních pravidlech (Krčmářová, 2012, s. 56).

Edukace rodičů v oblasti IT je ale velmi problematická, jelikož rodiče jsou často pracovně vytíženi a příliš volného času ke vzdělávání jim nezbývá. Proto je vhodná forma prevence zaměřená na rodiče realizovaná **pomocí masmédií** (videospoty, televizní pořady, kampaně na internetu). Nejlepší by bylo, pokud by rodiče při prevenci rizikového chování v IT spolupracovali přímo se školou, čehož se v praxi dosahuje zřídka (Kopecký et al., 2012, s. 47).

Aby školy v této oblasti s rodiči spolupracovali, ukazovali jim vzdělávací potenciál IT a vysvětlovali, proč je tak důležité u dětí rozvíjet digitální kompetence a informatické myšlení, včetně seznámení negativních stránek a možných slabin IT, tak tento dílčí cíl klade na školy i uváděná digitální strategie vzdělávání (MŠMT, 2014b, s. 8).

6.3 Prevence kriminality v České republice – Ministerstvo vnitra

Prevence kriminality spadá primárně pod Ministerstvo vnitra České republiky (dále MVČR). Jeho stálým hlavním orgánem, který se touto problematikou zabývá od roku 1993 je **Republikový výbor pro prevenci kriminality** (Chalupová, 2012, s. 37), který *„vytváří a sjednocuje koncepci preventivní politiky vlády České republiky na meziresortní úrovni a metodicky napomáhá při její realizaci na všech úrovních veřejné správy*." (MVČR, 2018a).

Oblast prevence kriminality v České republice dělíme na tři hlavní okruhy – sociální prevence[37], situační prevence[38], prevence viktimnosti a pomoc obětem trestných činů[39]; na tři základní stupně – primární, sekundární, terciální; a tři úrovně organizace – meziresortní úroveň, rezortní úroveň, místní úroveň (Chalupová, 2012, s. 38–40).

Činnost Republikového výboru pro prevenci kriminality zajišťuje **Odbor prevence kriminality** (dále OPK), který je součástí sekce vnitřní bezpečnosti a policejního vzdělávání Ministerstva vnitra. Jeho hlavním úkolem je tvorba, koncepce a koordinace prevence kriminality, přičemž hlavním výstupem je dokument Strategie prevence kriminality v České republice na určité období (MVČR, 2018b)

Globálním cílem aktuální **Strategie prevence kriminality v České republice na léta 2016 až 2020,** je při zajišťování bezpečnosti a veřejného pořádku v ČR podporovat preventivní přístupy a vytvářet k nim vhodné systémové, finanční a organizační předpoklady (MVČR, 2016, s. 6). Jako strategické cíle pak stanovuje mimo jiné rozvíjet systém prevence kriminality, posilovat spolupráci včetně té mezinárodní, opírat se o vědecké poznatky, poskytovat a zkvalitňovat pomoc a poradenství obětem trestných činů, zaměřovat se práci s pachateli trestné činnosti včetně recidivy, komplexně přistupovat k sociálně vyloučeným lokalitám, ale také zejména reagovat na nové hrozby kriminality a předcházet jim (MVČR, 2016, s. 8).

V reakci na nové hrozby tato aktuální strategie prevence upozorňuje na přesun kriminální aktivity do IT prostředí, kdy je zaznamenáván její strmý nárůst cca o 1/3 každým rokem. Zmiňuje zde i majetkovou trestnou činnost (podvody, phishing, obchodování na

[37] Sociální prevence představuje aktivity, které ovlivňují socializaci, sociální integraci a dále aktivity zaměřené na změnu nepříznivých ekonomických a společenských podmínek, jež jsou považovány za hlavní příčiny páchání kriminality.

[38] Situační prevence je zaměřena na majetkovou kriminalitu a vychází z toho, že v určité době, za určitých okolností a na určitých místech se objevují určité druhy trestné činnosti.

[39] Prevence viktimnosti a pomoc obětem trestných činů je založená na bezpečném chování, diferencovaného z hlediska na rozdílné kriminální situace a psychickou připravenost ohrožených lidí.

internetových aukcích, krádeže identity), která se vyznačuje velmi vysokou latencí (až 90 %), je mnohdy velmi sofistikovaná a mezi oběťmi se nachází všechny skupiny obyvatelstva i právnických osob. Proto v přístupu k prevenci kyberkriminality klade za cíl zejména včasnou a prakticky zaměřenou „*informovanost o existujících rizicích a možnostech ochrany před nimi, stejně jako přijímaní nejrůznějších technických opatření v zabezpečení systémů, aby nemohlo docházet ke zneužívání tohoto virtuálního prostředí a komunikace v něm činěné.“* (MVČR, 2016, s. 55).

OPK rovněž **provozuje internetový portál prevencekriminality.cz,** jehož cílem je v oblasti kyberkriminality poskytovat užitečné informace, vzdělávací materiály, doporučení, kontakty na domácí a zahraniční instituce nebo organizace, které se zabývají různými aspekty a oblastmi kybernetické kriminality a kybernetické bezpečnosti určené pro širokou i odbornou veřejnost. Jelikož existuje mnoho samostatných webových stránek věnující se různým aspektům tomuto druhu kriminality, slouží webový portál zejména jako uživatelsky přívětivý a přehledný rozcestník. Poskytuje taktéž seznam certifikovaných[40] poskytovatelů primární prevence v oblasti kyberkriminality MŠMT (Prevence kriminality v České republice, 2018).

OPK je partnerem projektu E-Synergie – vědeckovýzkumné sítě pro rizika elektronické komunikace Centra prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci (dále Pdf UPOL), který je zaměřený na boj proti kyberkriminalitě a rizikovému chování spojenému s virtuálním prostředím. Tato síť propojuje jak teoretickou oblast (teoretické ukotvení problematiky, výzkumy), tak praktickou oblast (vzdělávání, intervence, implementace znalostí do komerční sféry, trestněprávní řešení problematiky). Projekt nabízí všem studentům Pdf UPOL účast na přednáškách, seminářích, workshopech a odborných stážích, realizovaných jednotlivými aktéry projektu (E-SYNERGIE, 2011).

6.3.1 Policie České republiky

Pod MVČR spadá **Policie České republiky** (dále Policie ČR), která se také zabývá prevencí kriminality. To je dáno i zákonem č. 273/2008 Sb., o Policii České republiky, kde je v § 2 uvedeno, že jejím úkolem je „*předcházet trestné činnosti*.“ (Chalupová et al., 2012, s. 51).

[40] Databázi všech certifikovaných poskytovatelů programů primární prevence rizikového chování, kterou lze i filtrovat např. podle krajů, typů rizikového chování, cílové skupiny, lze nalézt na webových stránkách Národního ústavu pro vzdělání (Národní ústav pro vzdělání, 2018).

Policie ČR se zaměřuje zejména na prevenci primární, sekundární, sociální, situační a prevenci viktimnosti, včetně pomoci obětem trestné činnosti (MVČR, 2016, s. 16).

Na nejvyšším stupni Policie ČR, tedy na úrovni Policejního prezidia České republiky řídí prevenci kriminality republikový koordinátor prevence kriminality a odpovídá za celou preventivní činnost celé Policie ČR. Na úrovni útvarů s celostátní působností a úřadu služby kriminální policie a vyšetřování řídí preventivní činnost koordinátor prevence kriminality těchto útvarů a úřadu. Na úrovni krajů, řídí prevenci kriminality krajský koordinátor prevence kriminality a na úrovni jednotlivých územních odborů řídí tuto činnost koordinátor prevence kriminality příslušného územního odboru (Chalupová et al., 2012, s. 55–56).

Prevence kriminality v rámci Policie ČR je svěřena do působnosti specializovaných pracovišť – **oddělení tisku a prevence** na územní, krajské i celorepublikové úrovni (MVČR, 2016, s. 16). V oblasti prevence tito policisté na základních školách vedou tematické besedy.

Policie ČR také v oblasti prevence kriminality spolupracuje s různými subjekty, kdy pro účely této práce lze představit společný inovativní projekt Policejního prezidia ČR a Univerzity Palackého v Olomouci (projekt E-Bezpečí) „***Buď v bezpečí***“ z roku 2016, zaměřený na kyberšikanu[41], ale rovněž rizika sociálních sítí a podvodné praktiky v IT prostředí. Jeho hlavním cílem bylo vytvořit systém informování pedagogů prostřednictvím měsíčně vydávaného „*Newsletteru*“ a přinášet tak novinky z oblasti výzkumu a vývoje dané problematiky. Dalším cílem bylo vybudovat vazbu mezi školami, školskými zařízeními a Policií ČR. Cílovou skupinou jsou děti, mládež a jejich rodiče (Policie ČR, 2016). Bohužel v roce 2016 vyšlo těchto Newsletterů jen 10 a v současné době již aktualizován není.

Na webových stránkách Policie ČR jsou důležité odkazy s informacemi o kybernetické kriminalitě, jsou zde popsány nejčastější projevy této kriminality, jednotlivé druhy včetně internetových podvodů a rad jak se nestát obětí nebo je zde policejní Hotline s možností nahlášení závadového obsahu a aktivit v síti Internet. Oznámení o jakémkoliv podezření na protiprávní jednání lze podat samozřejmě také na kterémkoliv obvodním oddělení Policie ČR.

6.4 Preventivní působení vybraných subjektů a vybrané projekty

V České republice se osvětou činností, vzděláváním a preventivním působením v oblasti kybernetické kriminality zabývá nejen mnoho státních, ale i nestátních subjektů. Existuje množství projektů, které tvoří základnu ochranné sítě, umožňují nahlášení nelegálního

[41] Forma šikany, která probíhá v kybernetickém prostředí s využitím IT.

obsahu, spolupracují s dalšími složkami záchranné sítě, nebo nabízejí informace o možnostech řešení situace, rizicích a preventivních opatřeních. Mezi takové projekty patří aktuálně např. E-Bezpečí, Bezpečný internet.cz, S@fer internet.cz nebo linkabezpečí.cz (Krčmářová, 2012, s. 65).

6.4.1 E-Bezpečí

Jedná se o velmi uznávaný celorepublikový a časově neohraničený projekt zaměřený zejména na prevenci, vzdělávání, intervenci, výzkum a osvětu spojenou s rizikovým chováním na internetu a fenomény, které s ním souvisejí. Je realizován Centrem prevence rizikové virtuální komunikace Pdf UPOL ve spolupráci s dalšími organizacemi. Projekt je podporovaný např. MŠMT, MVČR či Policií ČR. Je zaměřen na kyberšikanu, sexting[42], kybergrooming[43], kyberstalking[44] a stalking[45], rizika sociálních sítí, hoax, spam, scamy, zneužívání osobních údajů, ale také právě na internetové podvody (E-bezpečí, 2008–2018).

Východiskem projektu jsou terénní práce s cílovými skupinami, mezi něž patří všichni žáci od 1. stupně základních škol, učitelé, vychovatelé, studenti, preventisté sociálně patologických jevů, metodici prevence, pracovníci OSPOD, policisté, manažeři prevence kriminality a v neposlední řadě také rodiče. Kromě vzdělávacích akcí provádí celorepubliková výzkumná šetření v oblastech, na které je zaměřen, provozuje online poradnu, vydává řadu článků a dokumentů pro žáky a učitele, nebo informuje o novinkách v daných oblastech (E-Bezpečí, 2008–2018).

Na jejich stánkách nalezneme mnohé rady. V případě podvodných praktik pak např. podává informace, na co si dávat pozor při nakupování na aukčních portálech, bazarech a e-shopech, abychom nebyli podvedeni.

Preventivní aktivity zaměřené na žáky 2. stupně ZŠ mají formu interaktivních besed, v nichž se žáci seznamují s rizikovými formami chování, kazuistikami, metodami ochrany a obrany apod. Žáci poté vyvozují řešení konkrétních krizových situací, navrhují bezpečnostní pravidla a preventivní opatření. Aktivně se tedy zapojují do činnosti (Kopecký et al., 2015, s. 121).

[42] Sexting – elektronické rozesílání zpráv, fotografií či videa se sexuálním obsahem.

[43] Kybergrooming – komunikace s neznámými uživateli internetu vedoucí k osobní schůzce.

[44] Kyberstalking – nebezpečné pronásledování s použitím IT.

[45] Stalking – nebezpečné pronásledování.

6.4.2 Národní centrum bezpečnějšího internetu

Národní centrum bezpečnějšího internetu (dále NCBI) je neziskové nevládní sdružení, jehož cílem je přispívat ke zvyšování bezpečnosti užívání internetu a IT, zvyšovat povědomí o nebezpečí na internetu, přispívat k osvojování etických norem v online prostředí, napomáhat předcházet a snižovat rizika spojená s užívání IT včetně sociálních sítí. Cílem centra je také vytvořit a provozovat odborné pracoviště pro osvětu, vzdělávat a chránit uživatele před nelegálním a ohrožujícím obsahem na internetu. NCBI podporuje výzkumy, vytváří a publikuje výukové odborné metodické dokumenty pro dané oblasti. Realizuje řadu projektů, které se rovněž zabývají kyberkriminalitou a ve spolupráci s partnery pořádá různé semináře, konference, přednášky a školení zaměřené nejen obecně na oblast bezpečného užívání internetu, ale i na prevenci internetové kriminality. Na svých stránkách přináší aktuální informace o trendech a rizicích spojených s užíváním internetu a taktéž vydává doporučení, jak těmto rizikům předcházet (NCBI, 2012).

NCBI provozuje výchovné webové stránky **bezpečně–online.cz**, které se zaměřují na děti a dospívající, s cílem podpory bezpečného a sebejistého používání internetu, IT, finančních online služeb a aktivní ochrany soukromých informací před zneužitím. Stránky poskytují vzdělávací materiály, metodickou podporu, videa a další materiály určené učitelům a rodičům. Konkrétně poskytují informace např. o internetovém bankovnictví a jeho rizicích, phishingu, podvodných e-shopech a podvodných online nákupech včetně jejich předcházení. Lze jejich prostřednictvím ohlásit kyberkriminalitu nebo nezákonný obsah (Bezpečně-online.cz, 2018).

Nejdůležitějším projektem NCBI je v současné době národní platforma **S@fer internet.cz**, která poskytuje služby linky hlášení nezákonného obsahu (**STOP online.cz**), internetovou poradnu pro pomoc v případě násilí a IT kriminality (**POMOC online.cz**) a jako osvětové centrum se zaměřuje rovněž na prevenci online kriminality a vzdělávání uživatelů internetu. Nabízí vzdělávání v oblasti bezpečnosti na internetu pro děti a mládež, rodiče, širokou veřejnost, ale také pro pedagogy, sociální pracovníky, metodiky IT nebo koordinátory prevence kriminality policie. V Praze je pak realizován konkrétní projekt „*Praha bezpečně online*“ (Saferinternet.cz, 2018).

6.4.3 Bezpečný internet.cz

Cílem tohoto nekomerčního projektu je ukázat na různá rizika spojená s používání internetu a na způsoby obrany. Oslovuje různé cílové skupiny (děti, rodiče, školy, začínající a pokročilé uživatele internetu) a na názorných příkladech napomáhá vytvářet ty správné návyky chování na internetu. Poskytuje rady např. při nakupování na internetu, návody

a zkušenosti, drží se zásady osvěty, že čím větší povědomí o rizicích máme, tím rychleji např. na podvodné nabídky, viry, či emaily budeme umět vhodně reagovat (bezpečný internet.cz, 2018).

6.4.4 Linka bezpečí

Linka bezpečí poskytuje snadnou a dostupnou pomoc dětem, mládeži, studentům do 26 let, ale i rodičům. Prostřednictvím telefonu, emailu a chatu radí a pomáhá s řešením v náročných životních situacích, každodenních problémů a starostí. Jelikož nestále stoupá počet dětí, které se na linku bezpečí obrací kvůli kyberšikaně, sextingu, lákání na schůzku nebo podvodným výzvám na internetu, zabývají se i problémy s tímto nebezpečím (linkabezpeci.cz, 2018).

6.4.5 CSIRT

Jedná se o národní bezpečnostní sdružení v oblasti kybernetické bezpečnosti, které na území České republiky řeší a koordinuje bezpečnostní incidenty, provádí osvětovou, preventivní a školící činnost v oblasti kybernetické bezpečnosti, informuje o aktuálních hrozbách, udržuje zahraniční vztahy se světovou komunitou CERT/CSIRT týmů včetně organizací podporující tuto komunitu a taktéž spolupracuje s nejrůznějšími subjekty na území ČR, např. banky, bezpečnostní složky, poskytovatelé internetového připojení, akademický sektor, úřady státní správy a další instituce. Rovněž zveřejňuje statistiky druhu řešených incidentů např. phishingu, spamu, pharmingu, malware. Rovněž informuje také o bezpečnostních chybách v softwaru, nových aktualizacích a phishingu (CSIRT.CZ, 2018).

6.4.6 Kraje pro bezpečný internet

Tento projekt je výsledkem Asociace krajů ČR a Národního úřadu pro kybernetickou a informační bezpečnost a jeho úsilím je zvýšit celkovou informovanost o rizicích internetu, nabídnout pomoc a možnost prevence. V rámci tohoto projektu vznikly online kurzy a kvíz pro děti a studenty, rodiče, pedagogy, veřejnost, pracovníky Policie ČR a pro sociální pracovníky. Online kvíz a obsah kurzů byly vytvořeny odbornými partnery projektu. V roce 2016 také vznikly rovněž videospoty pro seniory. Na realizaci projektu se podílí např. společnosti Microsoft a Gordic. Organizačně a finančně se na projektu podílí všech 14 krajů České republiky (**Kraje pro bezpečný internet, 2018**).

Pro děti daný projekt konkrétně nabízí kurzy v oblasti např. sociálních sítí, kyberšikany, kybergroomingu, sextingu, sociálního inženýrství, ale také bezpečných hesel, zabezpečení mobilů, online nakupování atd. (**Kraje pro bezpečný internet, 2018**).

Prevencí kyberkriminality se tedy zabývá celá řada subjektů, rovněž také např. společnost Seznam.cz, CESNET, sdružení CZ.NIC. Paradoxně však tato kriminalita, potažmo podvody, neustále narůstá. Proto je důležité si položit nejen otázku, zda školy na tuto oblast nabízí preventivní programy. V oblasti prevence kriminality je rovněž klíčová podle Chalupové (2012, s. 9) kvalitní evaluace, která by pak měla určit další směr takového preventivního projektu. Je-li účinný a funkční, měl by dál působit, ale je-li neúčinný a zbytečný, měl by být zrušen nebo přetvořen.

Zda existují na základních školách preventivní programy zaměřené na podvodná jednání v IT prostředí a zda jsou evaluovány se zabývá praktická část, stejně jako tím, zda žáci základních škol v Prostějově vůbec znají v tomto prostředí rizika podvodného jednání, zda se s takovým jednáním setkali a zda mají v tomto prostředí zkušenosti s obchodováním. Jak již bylo uvedeno, oblast obchodování je podstatná z toho důvodu, jelikož se na něj zaměřují pachatelé podvodů v daném prostředí nejčastěji, jak je doloženo v následující kapitole.

EMPIRICKÁ ČÁST

7 Současný stav zkoumané problematiky

Diplomová práce je zaměřena na kriminalitu v informačních a komunikačních technologií (dále IT) se zaměřením na žáky 2. stupně základních škol. V této kapitole je cílem zjistit a představit ty výzkumy, statistické údaje, výzkumná šetření absolventských prací i další relevantní zjištění, kterým bude nastíněn co nejlépe současný stav zkoumané problematiky. To je důležité pro komplexní účely práce i východiska vlastního výzkumného šetření.

Využívání počítače, internetu a mobilního telefonu

V současné době má podle Českého statistického úřadu ¾ domácností počítač (stolní počítač, notebook nebo tablet) a k internetu má přístup 77 % domácností. Počítače a internet se tedy staly běžnou součástí českých domovů. Trendem je přechod od stolních počítačů k přenosným, přičemž v domácnostech s dětmi dominují notebooky (81 % z domácností s počítačem) a poté tablety (46 % z nich). **Nejčastěji jsou k internetu připojeni** bezdětné domácnosti se členy rodiny mladšími 40 let (97 % z celkového počtu připojení k internetu) a právě **rodiny s dětmi** (96 % z připojených osob), (Český statistický úřad, 2017b, s. 22).

Z Čechů připojených k internetu jej 95 % využívá alespoň jednou týdně. Přičemž 80 % uživatelů se připojuje každý nebo skoro každý den. Nejvíce jej využívá věková skupina mezi 16–24 lety, a to 97 %. Evropský průměr uživatelů připojených k internetu činí 82 % (Český statistický úřad, 2017b, s. 43).

Děti se setkávají s počítačem a internetem od nejútlejšího věku. Na prvním stupni základní školy se učí s počítačem, na druhém stupni s internetem, vyhledávači a mailem. Podle výsledků výzkumu Kids Online 2010 bylo zjištěno, že **¾ českých dětí ve věku 9–16 let používá internet denně nebo téměř každý den**. České děti jsou tak na internetu velmi aktivní, přičemž kolem 11 let mají osvojeny technické dovednosti dospělých (Krčmářová, 2012, s. 57).

Mobilní telefon používá v současné době 98 % Čechů starších 16 let (Český statistický úřad, 2017b, s. 49), přičemž podle průzkumu *České děti a mládež* 2011/2012 jej **vlastní 95 % dětí starších 11 let** a 80 % dětí ve věku 7–10 let. Nejdůležitějším médiem pro dívky od 11 let je mobil, pro kluky internet (Eckertová a Dočekal, 2013, s. 157).

V roce 2017 v ČR využívalo emailovou komunikaci 73 % osob ve věku 16 let a více. 63 % osob mezi 16–24 lety pak využívalo zejména internetové aplikace pro zasílání zpráv (messengery, WhatsApp apod.). (Český statistický úřad, 2017b, s. 60). Pro děti se pak mobilní telefony, emaily a sociální sítě již staly primárními zdroji každodenní komunikace (Kopecký et al., 2015, s. 21)

Kriminalita informačních a komunikačních technologií a podvodné jednání

Veškerých podvodných jednání (tedy nejen v kyberprostoru) podle § 209 trestního zákoníku v ČR registrovaných Policií ČR za rok 2017 bylo celkem 5074 (Policie ČR, 2018b)

Statistiky všech trestných činů spáchaných v kybernetickém prostoru v prostředí internetu Policie ČR zveřejňuje od roku 2011 a **je zaznamenáván neustále vzrůstající trend**. Od 1502 spáchaných trestných činů v roce 2011, po 5654 trestných činů v roce 2017. Z celkového počtu trestných činů v kyberprostoru každým rokem **nejvyšší počet tvoří podvodná jednání**[46] kolem 60 %. V roce 2017 byl tento podíl 56 % a konkrétní počet podvodných jednání činil 3140. Ostatní strukturu této kriminality tvořil hacking v roce 2017 kolem 10 %, mravností delikty v roce 2017 kolem 10 %, dále autorské delikty, násilné projevy a ostatní trestná činnost. Proto je IT kriminalitě věnována stále větší pozornost (Policie ČR, 2018a). Graf s vývojem kybernetické kriminality je přiložen v příloze.

Pro účely této práce byly z Policejního prezidia České republiky vyžádány informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, kolik dětí a kolik mladistvých za období od roku 2011 do 2017 včetně, spáchalo (bylo objasněno) v kyberprostoru přestupek proti majetku kvalifikovaný jako podvod podle přestupkového zákona a trestný čin Podvod podle § 209 trestního zákoníku.

Poskytnutí údajů přestupkového podvodného jednání v kyberprostoru dětí a mládeže za dané období poskytnuto nebylo, ale údaje ohledně trestního jednání ano. Zveřejněné údaje uvádím v následující tabulce:

Tabulka č. 1 – protiprávní činy děti a mladistvých v kyberprostoru (Policejní prezidium ČR).

Protiprávní činy dětí a mladistvých spáchané v kyberprostoru	2011	2012	2013	2014	2015	2016	2017
Podle § 209 zákona č. 40/2009 Sb., trestního zákoníku, věk 1-14 let	1	1	1	3	2	2	3
Podle § 209 zákona č. 40/2009 Sb., trestního zákoníku, věk 15-17 let	5	11	13	12	15	28	33

Jelikož se mnozí odborníci kyberkriminality shodují, že značná část IT kriminality není vůbec na Policii ČR oznamována a dále výše uvedené údaje neobsahují podvodná jednání v kyberprostoru v rámci přestupku, nemohou být tato čísla ještě vyšší?

[46] Policie ČR mezi podvodné jednání zařazuje podvodné inzeráty, podvodné e-shopy, Nigerijské podvody a další scamy, phishing, ale jen ty trestné činy kvalifikované jako Podvod podle § 290 trestního zákoníku (Policie ČR, 2017).

Internetové nakupování

V souladu s nejčastějšími podvody při nakupování na internetu, v ČR každým rokem **roste obliba elektronického nakupování**, což dokládají statistiky Českého statistického úřadu. Za posledních 12 měsíců nakoupilo na internetu v roce 2005 jen kolem 5 % osob starších 16 let, v roce 2012 to bylo téměř 31 % a v roce 2017 nakoupilo již 52 % jednotlivců. Alespoň jednou v životě nakoupila věková skupina mezi 25–34 lety (v roce 2017 – 89 %), dále věková skupina mezi 35–44 (v roce 2017 – 84,5%) a věková skupina mezi 16–24 lety (v roce 2017 – 79 %). Nejčastěji přitom nakupují ženy na rodičovské dovolené (v roce 2017 – 77,6 %), studenti (v roce 2017 – 68,4%) a lidé v zaměstnání (v roce 2017 – 66,5 %). V porovnání se zahraničím, ale nejvíce na internetu nakupují Britové – 83 % (Český statistický úřad, 2017b, s. 108–111). V uvedených statistikách nejsou zahrnuty děti a mládež do 16 let, ale lze předpokládat i z důvodu cílené reklamy na mládež, že i tato věková skupina bude nákupy provádět, zejména prostřednictvím rodičů, kteří se v případě podvodu obvykle stávají poškozenými, což potvrzuje McCarthy a Weldon-Siviy (2013, s. 143), že **osoby mladší 18 let si online zboží sami vyberou, ale zaplatí je rodiče**.

Důkazem obliby elektronického nakupování jsou také veřejné informace Asociace pro elektronickou komerci[47], která uvádí, že v roce 2013 tvořil obrat e-komerce v ČR 58 miliard korun, v roce 2015 81 miliard korun a v roce 2017 již 115 miliard korun (APEK.cz, 2017).

S růstem nakupováním na internetu roste podíl i používání internetového bankovnictví, které v roce 2017 využilo 52 % Čechů, což představuje 2/3 osob využívající internet. V severských zemích internetového bankovnictví používá dokonce 80 % osob (Český statistický úřad, 2017b, s. 96), čímž nelze vyloučit vzestup používání internetového bankovnictví i v ČR.

Společnost ESET zabývající se antivirovou ochranou společně se společností Seznam.cz realizovala v prosinci 2017 průzkum, v němž bylo zjištěno, že čtyři z deseti Čechů nakupujících na internetu, nakupuje i v čínských e-shopech a 13 % nakupuje také v amerických e-shopech. 4 % z 1030 respondentů uvedla, že byli při internetovém nakupování podvedeni (ESET, 2017).

Ve své bakalářské práci prováděla Hejduková (2017, s. 36–40) výzkumné šetření i mimo jiné mezi 92 žáky 8. a 9. tříd základní školy Slatiňany, v němž se zabývala vlastnictvím platebních karet. Zjistila, že **z daného vzorku vlastní platební kartu 15,2 % žáků ZŠ**,

[47] Asociace pro elektronickou komerci vydává ověřeným internetovým obchodům certifikát o spolehlivosti.

většinou mají limit do 1.000,- Kč, přičemž 43 % žáků považuje internetové bankovnictví za nebezpečné.

Eibensteiner (2015, s. 36, 39) ve své diplomové práci zabývající se komunikací žáků na internetu zjistil od 118 žáků 8. a 9. tříd základních škol v Uherském Hradišti, že **5,1 % žáků využívá internet mimo jiné i k nakupování**.

Sociální sítě

Výzkumy bylo zjištěno, že české děti a mládež patří mezi nejaktivnější uživatele sociálních sítí v Evropě. Děti ve věku 11–15 let si nejvíce oblíbily Facebook s více než 80 % uživateli, Google + s více než 44 % uživateli, Lidé.cz s více než 27 % uživateli (Kopecký a kol, 2015, s. 73), přičemž podle výsledků výzkumu Kids Online 2010, má 72 % mládeže profil na nějaké sociální síti (Krčmářová, 2012, s. 57).

V současné době má Facebook 68 % 12 letých, 83 % 13 letých, 92 % 14 letých a 94 % 15 letých dětí (Kopecký, 2017b). Děti si oblíbily zejména Facebook z důvodu komunikace s ostatními, udržení kontaktu s kamarády, skupinového tlaku, hraní online her, seznamování, sdílení fotografií, z důvodu modernosti a rozvoje virtuální prezentace (Kopecký, 2015b, s. 11–15).

Riziko setkání dítěte s falešným přítelem (podvodným profilem) umocňuje fakt, že 36,6 % dětí na Facebooku nezná všechny své přátele (Kopecký, 2015b), 31,10 % dětí vyhoví žádosti o přátelství, aniž by si ověřily identitu dané osoby a 49,49 % dětí si neověřuje identitu svých spolužáků, kteří je o přátelství žádají (Kopecký, 2017c).

Spam, scam

Jírovský (2007, s. 104) uváděl, že v elektronické poště se nachází až 90 % spamu, což odpovídalo i výsledkům antivirové společnosti Symantec z roku 2009 (Kshetri, 2010, s. 5).

Průměrný globální **výskyt spamu v emailech** však postupem času klesal, kdy v roce 2012 činil 75 %, v roce 2015 činil 54 % (*Statista – The portal for statistics, 2018a*), ale do konce **roku 2017** mírně vzrostl na **necelých 60 %** (*Statista – The portal for statistics, 2018b*).

Společnost Kaspersky Lab, která se zabývá kybernetickou bezpečností, vydává zprávy ohledně globálních trendů malware, spamu a phishingu. Uvádí, že z celosvětově odeslaných emailů bylo v roce 2017 průměrně 56,63 % spamu a nejčastější škodlivým programem ve spamu byly Trojské koně (Securelist.com, 2018).

Společnost Intel ve svém průzkumu zjistila od více než 1000 uživatelů, že 74 % Čechů včetně seniorů, někdy obdrželo prostřednictvím internetu podvodnou zprávu (Janouš, 2014).

Hoax

Na internetových stránkách E-Bezpečí uvádí Kopecký (2008), že přibližně **80 % dětí ve věku 6–15 let hoax přeposílají dál** a umožňují jeho šíření. Tyto zprávy čtou a v kombinaci s jejich nekritickým přístupem u nich mohou vyvolávat obavu, strach, nedůvěru čímž působí na jejich psychiku.

Phishing

Podle studie společnosti Google má dobrý **Phishing až 45 % úspěšnost**, přičemž tato metoda se neustále rozšiřuje a vylepšuje (Buckley, 2014). To koresponduje se stále narůstající statistikou množství řešeného druhu phishigu organizace CSIRT, která v ČR řešila 65 druhů v roce 2008, 175 v roce 2013 a 409 v roce 2017. Celkem od roku 2008 do 2017 včetně řešili 2580 druhů phishingu *(CSIRT.CZ, 2018).*

Na celosvětový **stálý nárůst phishingových útoků**, upozorňuje i společnosti Kaspersky Lab. Ze všech jejich uživatelů antivirové ochrany byl v roce 2017 zaznamenán pokus o přesměrování na phishingové stránky u 16 % jejich uživatelů. Nejčastěji se útočníci zaměřovali na bankovní organizace, platební systémy, online obchody a sociální sítě (Securelist.com, 2018).

Malware

Orel (2016, s. 33, 40) se ve své bakalářské práci zabýval ve výzkumném šetření ověřením znalostí o škodlivých programech mezi 241 **žáky 3–6 tříd základních škol**. Zjistil, že ačkoliv více než 50 % žáků správně definovalo pojem malware, mylně jej označovali za synonymum počítačového viru. Na dotaz k termínu červ odpovídali žáci většinou špatně, nebo termín neznali, Trojského koně žáci považovali mylně za pirátskou verzi placeného software, pojem hoax většinou definovali správně. Úspěšně na tom byl také pojem antivirus, který žáci znali a uměli jej správně definovat. Celkovým zjištěním bylo, že žáci nejsou na tak dobré úrovni, jak by být měli, přičemž **dosahují nízké úrovně znalostí o této problematice**.

Organizace CSIRT rovněž uvádí, že od roku 2008 do 2017 včetně, řešila v ČR 953 druhů Malware, 439 druhů Trojských koní *(CSIRT.CZ*, 2018).

Bezpečnostní expert antivirové společnosti ESET Václav Zubr uvedl zjištění, že „*zatímco u počítačů a notebooků je míra zabezpečení zařízení před kybernetickými útoky nad*

90 procenty, u mobilních zařízení se stále pohybujeme lehce nad 40 procenty.“ Obzvláště nebezpečné je pak zejména internetové bankovnictví v mobilech. *„Mobilním telefonům svěřujeme stále více důvěrných dat a to si žádá jejich adekvátní zabezpečení*.“ (Potůček, 2017).

V současné době se v České republice nejčastěji šíří malware tzv. JS/CoinMiner běžící na pozadí internetových stránek, který zneužívá výpočetního výkonu počítačového systému pro těžbu kryptoměn. Na začátku ledna 2018 dokonce dosahoval téměř 50 % ze všech detekcí, v dubnu 2018 již jeho detekce klesla na 11 %. Mezi další často vyskytující se druhy malware tvoří také např. SMB/Exploit.DoublePulsar (detekcí 6 % v dubnu 2018), vyvinutý americkou Národní bezpečnostní agenturou NSA. Infikuje počítače s operačním systémem Windows a stahuje do nich další druhy malwaru, přičemž má dokonalou kontrolu nad systémem. „*V květnu 2017 tento malware pomáhal šířit ransomware WannaCry, což byl doposud největší útok ransomwaru v historii*.“ Další častým druhem malware je trojský kůň JS/Redirector, který přesměrovává prohlížeč na konkrétní URL adresu, z něhož stáhne další malware (ESET, 2018).

Wangiri

V dubnu 2018 informovala společnost Vodafone, že „*zaznamenali vyšší počet prozvánění z různých telefonních čísel se zahraniční předvolbou. Jde o různá telefonní čísla s předvolbami exotických zemí (například +225, +247, +211, +678 a další).“* Jedná se o podvodné prozvánění Wangiri, kterému se nelze nijak vyhnout (Vodafone.cz, 2018).

Skimming

Policie ČR (2018c) taktéž zveřejňuje každým rokem statistiky výskytu zjištěného skimmingu, kterých v roce 2017 bylo 83, tedy obdobně jako v roce 2014 (74), což je podstatně méně než v roce 2016 (329), v roce 2015 (277) nebo v roce 2013 (366).

Preventivní programy primární prevence majetkové kriminality na internetu na středních a základních školách

Vyhlídal (2014, s. 45) se ve své bakalářské práci věnoval majetkové kriminalitě na internetu a výzkumným šetřením mezi školními metodiky prevence ověřoval, zda existují preventivní programy zaměřené přímo na primární prevenci dané problematiky na středních školách a gymnáziích v okrese Olomouc. Ve druhé fázi výzkumného šetření provedl i zjištění na základních školách v okrese Olomouc, aby ověřil, zda nemohou mít studenti potřebnou vybavenost právě ze základních škol (dále ZŠ).

Provedeným šetřením zjistil, že 27 z 29 středních škol a gymnázií (93 % škol) nemá **preventivní program zaměřené přímo na majetkovou kriminalitu na internetu**. Na 30 ZŠ pak zjistil, že preventivní programy přímo na tuto problematiku **nemá** rovněž 27 škol (**90 % ZŠ škol**). Doplňujícími otázkami zjistil, že na vybraných středních školách a gymnáziích se vyskytl pouze jeden případ této kriminality (žák byl oběť nebo pachatel) a na vybraných ZŠ se vyskytly dva případy. Respondenti šetření neexistenci preventivních programů této problematiky na školách zdůvodňovali nevyskytováním se tohoto jevu na škole, příp. o něm nebyl pedagogický sbor informován (Vyhlídal, 2014, s. 53–54).

Zjištění, že není ve školách tento jev zaznamenáván nebo nebyl zjištěn, však jako argument kategoricky neobstojí, jelikož primární prevence je určená k předcházení jevu, než se vůbec vyskytne. Navíc se kyberkriminalita vyznačuje vysokou mírou latence a pokud se děti a mladiství s tímto jevem ve svém prostředí setkají, ať už v roli oběti nebo jako nezúčastněné osoby, skutečně by v první řadě nebo vůbec informovali pedagogický sbor?

Při realizaci programu primární prevence se zaměřením na děti staršího školního věku, respektive od 12 let, musíme počítat s aktuálním stavem, že tyto děti:

„a) pravděpodobně mají účet na sociální síti (ačkoli porušují pravidla o minimální věkové hranici pro vstup do tohoto prostředí),

b) přicházejí do období puberty a aktivně se zajímají o informace, které jsou spojené např. s tématy lidské sexuality,

c) aktivně se na internetu seznamují, hledají kamarády, ale také možné partnery,

d) většina z nich má k dispozici mobilní telefon či tablet,

e) aktivně využívají komunikační služby typu WhatsApp, Viber, Skype,

f) jsou sebevědomé a v prostředí internetu si věří, mají celou řadu znalostí a dovedností o tom, jak ICT funguje a jaké služby se dají na internetu využívat.“ (Kopecký et al., 2015, s. 127–128).

8 Charakteristika výzkumného šetření

Praktická část diplomové práce je zaměřena na kvantitativně orientované pedagogické výzkumné šetření zaměřené do školního prostředí. Chráska (2016, s. 9) uvádí, že „*výzkumy kvantitativně orientované*[48]“ jsou označovány jako klasické pedagogické výzkumy, přičemž v posledních desetiletích se nejen u nás, ale i ve světě však stále více uplatňují „*výzkumy kvalitativně orientované.“* Oba přístupy je možné a vhodné kombinovat.

V pedagogice existují tedy dva základní typy pedagogického výzkumu. Kvantitativně orientované výzkumy vycházející z pozitivizmu, respektive novopozitivizmu a připouští jednu objektivní realitu. Kvalitativně orientované výzkumy vycházejí z fenomenologie, zdůrazňují subjektivní aspekty a připouští více realit (Chráska, 2016, s. 29).

Konkrétně pedagogický kvantitativní výzkum je řazen do empirického výzkumu (Švec et al., 1998, s. 65) a definujeme jej jako *„záměrnou a systematickou činnost, při které se empirickými metodami zkoumají (ověřují, verifikují, testují) hypotézy o vztazích mezi pedagogickými jevy.*“ (Chráska, 2016, s. 11).

Pro kvantitativní výzkum je charakteristické, že pracuje s číselnými údaji, zjišťuje množství, rozsah nebo frekvenci výskytu jevu a jde matematicky a přehledně zpracovat. Drží si odstup ke zkoumanému jevu. Jeho cílem je třídění údajů a vysvětlení příčin existence jevu a při výběru zkoumaných osob usiluje o co nejlepší reprezentaci populace za účelem zobecnění. Ověřuje rovněž existující pedagogické teorie a zkoumá tradiční výzkumné problémy (Gavora, 2008, s. 34–36). To jsou rovněž důvody volby tohoto typu výzkumu.

Kvantitativní výzkumné šetření prováděné v této práci je závislé na souhlasu ředitelů škol, spolupráci žáků a spolupráci školních metodiků prevence, což není samozřejmostí a může představovat jistá úskalí. Na rozdíl od kvalitativního výzkumu, ale můžeme získat větší množství objektivních dat za poměrně krátkou dobu.

[48] Kvantitativní výzkum lze definovat jako *„Vědecký výzkum je systematické, kontrolované, empirické a kritické zkoumání hypotetických výroků o předpokládaných vztazích mezi přirozenými jevy.“* (Chráska, 2016, s. 11).

9 Deskripce výzkumného šetření

V této kapitole jsou popsány veškeré kroky uskutečněného výzkumného šetření. Veškeré části šetření jsou jeden po druhém logicky uspořádány tak, aby na sebe navazovaly.

9.1 Výzkumné cíle

Empirická část práce musí začít stanovením výzkumných cílů, následně by měly být stanoveny výzkumné problémy a z nich vycházet hypotézy (Švec et al., 1998, s. 67).

Z důvodu přehlednosti jsou cíle rozčleněny na cíl hlavní a cíle dílčí. V tázací formě jsou pak vyjádřeny jednotlivé problémy, v oznamovací formě jsou vyjádřeny hypotézy. Konkrétní výzkumné cíle byly stanoveny na základě vypracované teoretické části práce, zjištění aktuálního stavu dané problematiky a oblastí, které dosud zkoumány nebyly, nebo jim nebyla věnována dostatečná pozornost.

9.1.1 Hlavní a dílčí cíle výzkumného šetření

Hlavním cílem diplomové práce je u vybraných žáků 6. a 9. tříd základních škol 2. stupně v Prostějově zjistit, zda znají rizika podvodného jednání v prostředí informačních a komunikačních technologií (dále IT), zda se s takovým jednáním setkali a zda mají v tomto prostředí zkušenosti s obchodováním.

Dílčí cíle diplomové práce vycházejí z hlavního cíle a z kapitol a podkapitol teoretické části. Tyto dílčí cíle byly nápomocny ke tvorbě obsahu dotazníku:

- ověřit, zda existují na základních školách v Prostějově preventivní programy zaměřené proti podvodnému jednání v prostředí IT, se zaměřením na žáky 2. stupně,
- zjistit od školních metodiků prevence základních škol v Prostějově, zda se u jejich žáků ve škole vyskytl případ podvodného jednání v prostředí IT, kde figuroval žák v roli oběti nebo pachatele,
- zjistit, jak by školní metodici prevence v Prostějově řešili, pokud by za ním přišel žák, že byl podveden v IT prostředí,
- zjistit u vybraných žáků 6. a 9. tříd základních škol v Prostějově, zda mají možnost zaslat platbu prostřednictvím internetu na bankovní účet,
- zjistit u vybraných žáků 6. a 9. tříd základních škol v Prostějově, zda vlastní platební kartu a využívali někdy internetové bankovnictví,

- zjistit u vybraných žáků 6. a 9. tříd základních škol v Prostějově, zda někdy platili platební kartou v IT prostředí,
- zjistit, zda vybraní žáci 9. tříd základních škol v Prostějově nakupují v IT prostředí častěji, než vybraní žáci 6. tříd základních škol v Prostějově,
- zjistit, u vybraných žáků 6. a 9. tříd základních škol v Prostějově, zda někdy prodávali prostřednictvím internetu,
- zjistit zda vybraní žáci 6. a 9. tříd základních škol v Prostějově ověřují prodávající subjekt před internetovým nakupováním jako ochranu před podvodným jednáním,
- zjistit u vybraných žáků 6. a 9. tříd základních škol v Prostějově, zda byli někým poučeni o vybraném podvodném jednání v IT prostředí,
- zjistit, zda se vybraní žáci 9. tříd základních škol v Prostějově stali cílem útoku pachatele vybraného podvodného jednání v IT prostředí častěji, než vybraní žáci 6. tříd základních škol v Prostějově,
- zjistit u vybraných žáků 6. a 9. tříd základních škol v Prostějově, podle čeho by poznali, že jde na internetu o podvodnou nabídku zboží.

9.1.2 Deskriptivní a relační problémy

Hlavní cíl práce včetně dílčích dílů jsou stanoveny, proto můžeme přistoupit ke stanovení výzkumných problémů, které jsou podle Chrásky (2016, s. 11) počáteční fází pedagogického výzkumu. Problémy by měly vyjadřovat vztah mezi dvěma nebo více proměnnými[49] (Chráska, 2016, s. 13–14), čímž jsou myšleny relační problémy.

Kromě relačních výzkumných problémů existují však ještě výzkumné problémy deskriptivní a kauzální (Gavora, 2008, s. 54–55). V této práci se kauzálními problémy zabývat nebudeme, protože se uplatňují v experimentech, mezi nejméně dvěma skupinami, které se liší jedním z jevů, např. výchovným stylem (Gavora, 2008, s. 56), což výzkumné šetřené této práce nezahrnuje.

Deskriptivní problémy jsou problémy popisné, které popisují a zjišťují situaci, stav nebo výskyt určitého jevu (Gavora, 2008, s. 54). Tyto problémy byly stanoveny:

- Jak je to s existencí preventivních programů proti podvodnému jednání v IT prostředí pro žáky 2. stupně na základních školách v Prostějově?

[49] Proměnné jsou „*jevy nebo vlastnosti, které ve výzkumu vystupují a mezi nimiž hledáme (ověřujeme) existenci vztahů.*“ Proměnné lze dělit na tzv. „*nezávisle proměnné a závisle proměnné*.“ (Chráska, 2016, s. 13).

- Jaký je na základních školách v Prostějově výskyt případů podvodného jednání v prostředí IT, kde figuroval žák v roli oběti nebo pachatele?
- Jak by školní metodici prevence řešili, pokud by za ním přišel žák, že byl podveden v IT prostředí?
- Jaké mají vybraní žáci 6. a 9. tříd základních škol v Prostějově možnosti zaslání platby prostřednictvím internetu na bankovní účet?
- Jak je to u vybraných žáků 6. tříd a 9. tříd základních škol v Prostějově s vlastnictvím vlastní platební karty a využíváním internetového bankovnictví?
- Jaké mají vybraní žáci 6. a 9. tříd základních škol v Prostějově zkušenosti s placením platební kartou v IT prostředí?
- Jaké mají vybraní žáci 6. a 9. tříd základních škol v Prostějově zkušenosti s prodejem prostřednictvím internetu?
- Jak si ověřují vybraní žáci 6. a 9. tříd základních škol v Prostějově prodávající subjekt před internetovým nakupováním jako ochranu před podvodným jednáním?
- Byli někým vybraní žáci 6. a 9. tříd základních škol v Prostějově poučeni o vybraném podvodném jednání v IT prostředí?
- Jak by vybraní žáci 6. a 9. tříd základních škol v Prostějově poznali podvodnou nabídku zboží na internetu?

Relační problémy jsou problémy, které zjišťují, zda existuje vztah mezi zkoumanými jevy a jak těsný je tento vztah. Stanovuje, který jev zapříčiňuje který (Gavora, 2008, s. 55), respektive pracuje s nezávisle a závisle proměnnou. Tyto problémy byly stanoveny:

- Jaký je rozdíl v četnosti nakupování v IT prostředí u vybraných žáků 6. a 9. tříd na základních školách v Prostějově?
- Jaký je rozdíl v četnosti cílených útoků pachatele vybraného podvodného jednání v IT prostředí na žáky 6. a 9. tříd na základních školách v Prostějově?

9.1.3 Věcné hypotézy

Hypotézy tvoří jádro kvantitativně orientovaného výzkumu a vyjadřují vztah mezi dvěma proměnnými, proto musí být formulovány jako tvrzení o rozdílech, vztazích nebo následcích. Hypotézy musí být empiricky ověřitelné a lze říci, že se jedná o vědecké predikce (předpovědi), které nám říkají, že *„nastane-li jev A, nastane jev B.“* (Chráska, 2016, s. 14–15).

Nejprve budou stanoveny věcné hypotézy, které budou v následující části práce převedeny do tzv. statistických hypotéz ověřovaných pomocí alternativních a nulových hypotéz.

Věcné hypotézy

- HYPOTÉZA 1: Žáci 9. tříd základních škol v Prostějově častěji nakupují v IT prostředí, než žáci 6. tříd základních škol v Prostějově.

- HYPOTÉZA 2: Žáci 9. tříd základních škol v Prostějově jsou častěji cílem útoku pachatele vybraného podvodného jednání v IT prostředí, než žáci 6. tříd základních škol v Prostějově.

9.2 Výběr prvků do výzkumného souboru

Výběr prvků do výzkumného souboru nám přináší dva důležité pojmy. Základní soubor tvoří všechny prvky patřící do skupiny. Výběrový soubor tvoří určitou část prvků vybraných ze základního souboru a zastupuje, reprezentuje jej (Chráska, 2016, s. 17).

V Prostějově je celkem 11 základních škol, včetně jedné školy, která je určena pouze pro žáky se zdravotním postižením. Celkové množství základních škol bylo ověřeno v Rejstříku škol na webové adrese https://profa.uiv.cz/rejskol/ (Rejstřík škol a školských zařízení, 2018).

Základní soubor tedy tvoří všichni školní metodici prevence a všichni žáci 6. a 9. tříd těchto škol. Jak výzkumné šetření, tak výběr prvků do výzkumného souboru byl rozdělen na dvě úrovně.

V rámci první úrovně byl pro výzkumné šetření zvolen celý základní soubor, všichni školní metodici prevence základních škol v Prostějově, kteří byli následně telefonicky kontaktováni a požádání o umožnění šetření a spolupráci. Výzkumného šetření se zúčastnilo všech 11 školních metodiků prevence.

V rámci druhé úrovně šetření byly ze základního souboru základních škol v Prostějově mechanickým losováním bez vracení vylosovány náhodným výběrem 4 základní školy, jejichž všichni přítomní žáci 6. a 9. tříd tvořili výběrový soubor. Ředitelé těchto škol byli osobně osloveni a požádáni o umožnění provedení výzkumného šetření. Výzkumného šetření se zúčastnilo 115 žáků 9. tříd a 117 žáků 6. tříd. Celkem se šetření tedy zúčastnilo 232 žáků.

Žáci 6. a 9. tříd základních škol byli do výzkumného šetření vybráni z důvodu věkového rozdílu a předpokládaných odlišných zkušeností se zkoumaným jevem.

9.3 Metodologické nástroje

Metoda je způsob, kterým získáme data pro výzkumné šetření. Zatímco v teoretické části práce byla pro získávání informací a dat použita metoda analýzy textových dokumentů, v empirické části jsou využity dva anonymní dotazníky. První dotazník je určen pro školní metodiky prevence a druhý pro žáky 2. stupně základních škol.

Dotazník je výzkumný, respektive průzkumný, vývojový a vyhodnocovací nástroj, který prostřednictvím písemného dotazování nachází uplatnění pro hromadné a poměrně rychlé získávání informací o znalostech, postojích nebo názorech dotazovaných osob k aktuální nebo potencionální skutečnosti. Tato metoda je postavena na dotazování, čímž je příbuzná rozhovoru, respektive ústnímu interview. Oproti rozhovoru má ale dotazník výhody právě v množství a rychlosti získávání informací (Švec et al., 1998, s. 125).

V pedagogických výzkumech je dotazník vyžíván velmi často, dokonce až příliš. Nevýhodou dotazníku je oprávněný fakt, že spíše než pedagogickou realitu zjišťuje, jak tuto realitu vidí ten, komu je dotazník určen (Chráska, 2016, s. 158–159).

Dotazník byl zvolen z důvodu jeho uvedených výhod, dále nižší časové a finanční náročnosti, statistickému a analytickému zpracování, přičemž anonymita odpovídajících v dotazníku nebrání v otevřenosti a pravdivosti odpovědí, přesto nelze nepravdivé vyplnění dotazníku, nebo nepochopení či důsledné nepřečtení určité položky zcela vyloučit.

Struktura dotazníku byla konstruována podle Švece et al., (1998, s. 125–130). Dotazník byl tedy rozdělen na tři části. Úvodní část tvoří informace a instrukce k dotazníku, druhou část tvoří jednotlivé položky dotazníku a třetí část tvoří zjišťování citlivých údajů – pohlaví příslušnost k 6. nebo 9. třídě. Samotná část dotazníku s položkami byla vytvořena s důrazem na srozumitelnost, jasnost, jednoznačnost a pochopení pro respondenty. První dotazník směřující ke školním metodikům prevence obsahuje 5 položek, druhý dotazník směřující k žákům základních škol obsahuje 35 položek. Položky v dotaznících jsou koncipovány tak, aby odpověděly na výzkumné otázky a umožnily verifikaci hypotéz. Jednotlivé položky v dotazníku byly konstruovány tak, aby nebyly zbytečně složité na přemýšlení a časově nenáročné. Přesto jsou některé položky delší, což bylo nutné za účelem vysvětlení a pochopení položky.

Veškerá data a informace, které byly zjištěny dotazníkem, jsou v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů. Jsou tedy zcela anonymní. Ředitelé škol i školní metodici prevence byli seznámeni s tím, že cílem výzkumného šetření je přispět k pedagogickému rozvoji v dané oblasti, nikoliv poškodit např. pověst školy nebo žáků.

Z důvodu anonymity nejsou v této práci uváděny konkrétní školy, ve kterých bylo výzkumné šetření realizováno. S výsledky výzkumného šetření však ředitelé jednotlivých škol byli seznámeni.

9.4 Pilotní studie a předvýzkum

Pro předejití chyb a nesrovnalostí v dotazníku je třeba se věnovat i pilotní studii a předvýzkumu, které tvoří součást kvantitativního výzkumu. Gavora (2008, s. 83–84) uvádí, že výzkumník se při nich setkává poprvé s praxí a díky zjištěným poznatkům si může ověřit fakta a předejít chybám samotného výzkumu. Při pilotní studii se výzkumník zejména seznamuje s prostředím, u předvýzkumu je ověřován výzkumný nástroj na malém souboru respondentů. Cílem předvýzkumu je zjistit, jestli výzkumný nástroj funguje a jak funguje, respektive zda zkoumané osoby rozumí pokynům a otázkám, zda jsou ochotny se do výzkumu zapojit, zda trvá práce naplánovanou dobu, zda se dají získané údaje správně vyhodnotit.

Pilotní studie byla provedena na náhodně vybrané základní škole v Prostějově. Oba dotazníky byly ověřovány na malém výzkumném vzorku respondentů. Položky v dotazníku byly formulovány nejprve pod dohledem vedoucího práce, poté po jejich vyplnění a zpětné vazbě školních metodiků prevence pro první dotazník a žáků 6. a 9. tříd pro dotazník druhý, došlo k jejich vyhodnocení a finální úpravě. Finální podoby dotazníků včetně četností odpovědí uvedených v závorkách za každou odpovědí, jsou založeny v příloze. Finální dotazníky byly následně předloženy všem respondentům výzkumného šetření.

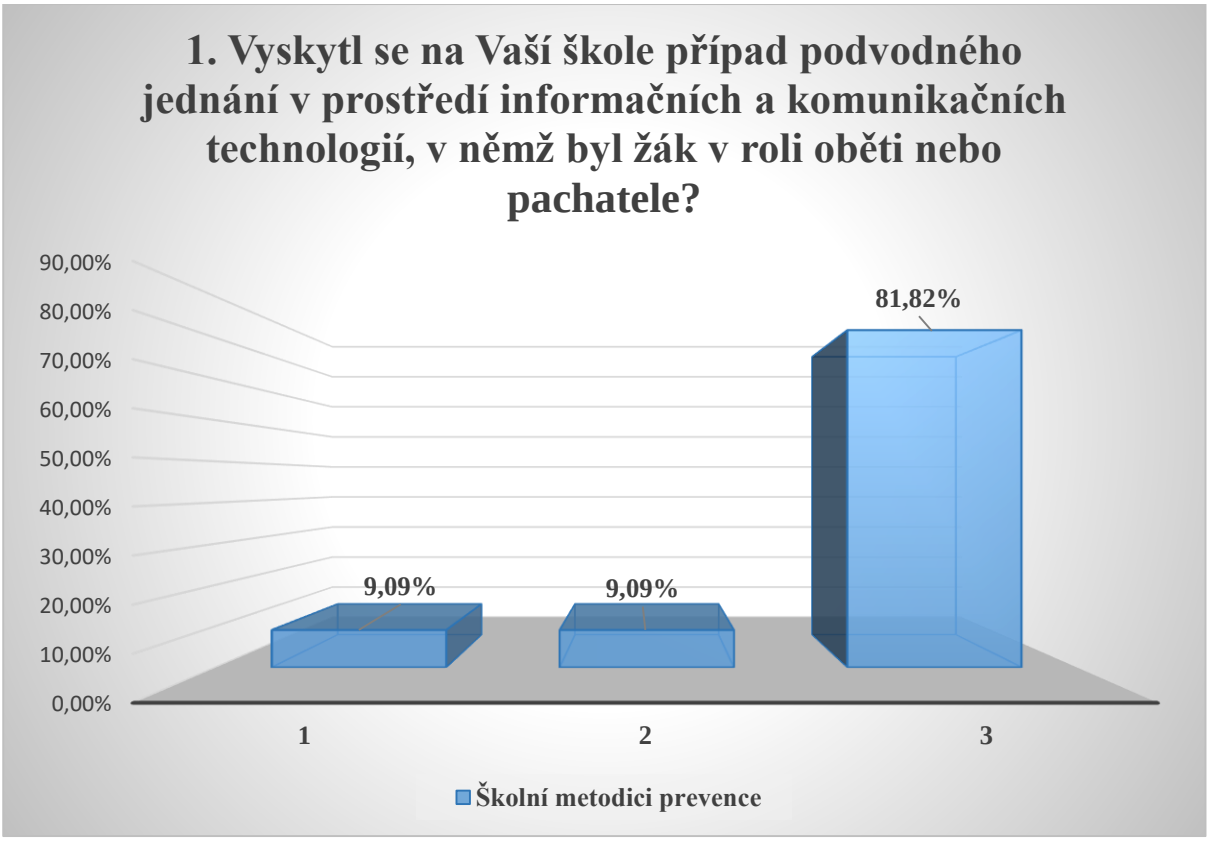
10 Výsledky

V této kapitole jsou zpracovány výsledky výzkumného šetření, které odpovídají na deskriptivní a relační problémy a následně jsou zde ověřeny vědecké predikce. Veškeré výsledky získané dotazníkovou metodou byly zpracovány fyzicky, poté překontrolovány a následně zapsány do programu Microsoft Office 2016, ve kterém byly vygenerovány grafy. Každá jednotlivá odpověď je tedy uvedena v grafické podobě. Veškerá data jsou uváděna v procentuálním zastoupení (relativní četnost) a vztahují se k jednotlivým skupinám respondentů zvlášť (školní metodici prevence, žáci 6. tříd a žáci 9. tříd základních škol).

10.1 Výsledky dotazníkového šetření

Dotazníkového šetření se v Prostějově zúčastnilo celkem 115 žáků 9. tříd, 117 žáků 6. tříd a všech 11 školních metodiků prevence. **V první fázi dotazníkového šetření byli osloveni školní metodici prevence** základních škol. Dotazník obsahoval 5 položek.

Položka č. 1



Graf č. 1 *– relativní četnost odpovědí na položku č. 1 v dotazníku pro školní metodiky.*

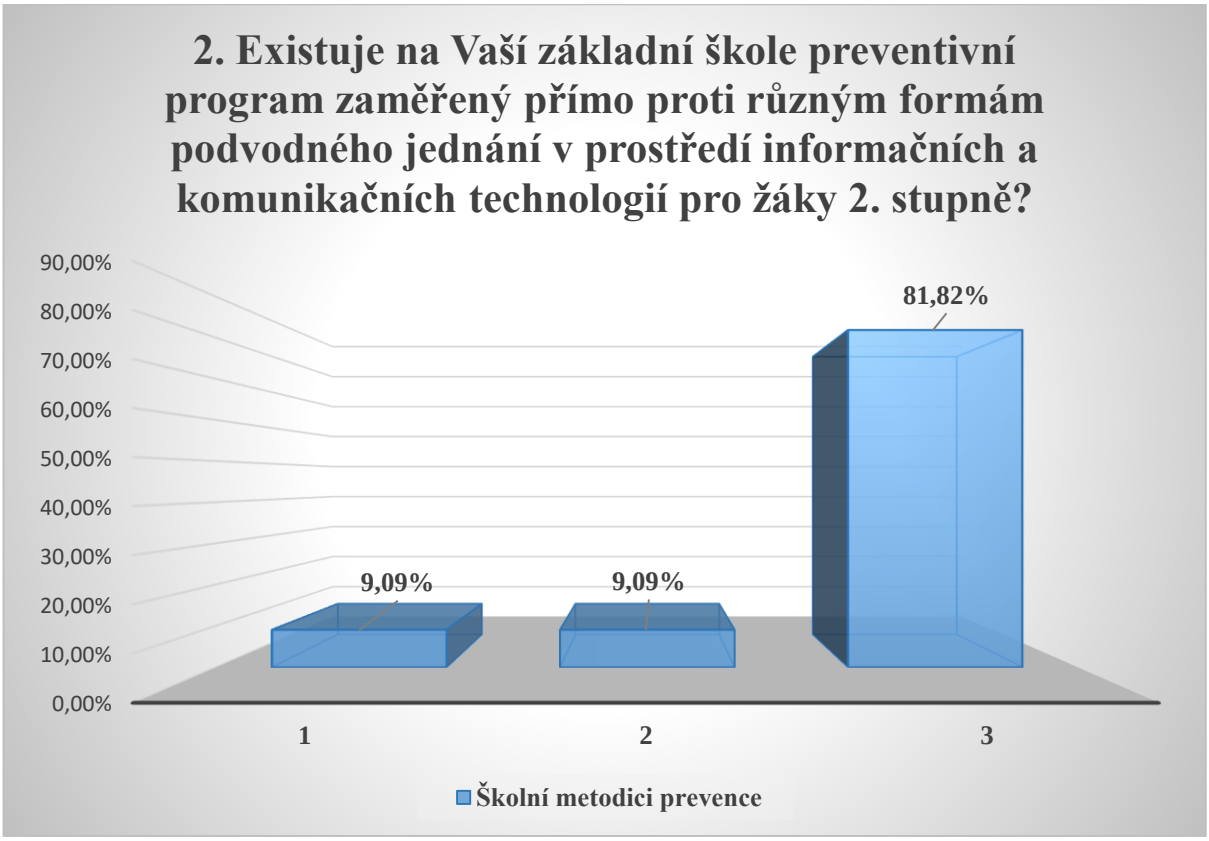
Odpovědi vztahující se k číselným hodnotám 1–3 v grafu č. 1:

1	Ano, žák byl pachatel.	**2**	Ano, žák byl oběť.	**3**	Ne, nemám informace.

Na první položku č. 1 odpovědělo všech 11 školních metodiků prevence. V případě pachatele se jednalo o 12. letého žáka, který se před 2 roky dopustil trestného činu Podvodu podle § 209 trestního zákoníku. Rodič mu zakoupil platebními údaji z platební karty vylepšení herního obsahu (mikrotransakce) do počítačové hry, platební údaje zůstaly v počítači uloženy a chlapec si tajně nakupoval další 2 měsíce bez vědomí rodičů, čímž způsobil škodu kolem 16.000,- Kč. Také byl dotazníkovým šetřením zjištěn jeden žák, který se stal obětí internetového podvodu, přičemž daný školní metodik neuvedl k danému případu žádné další skutečnosti. Pokud metodici odpovídali, že se takový případ nevyskytl, do poznámky mnohdy uvedli, že se o žádném takovém případu spíše nedozvěděli.

Zjištěným výsledkem z této položky byl tak splněn dílčí cíl diplomové práce „*Jaký je na základních školách v Prostějově výskyt případů podvodného jednání v prostředí IT, kde figuroval žák v roli oběti nebo pachatele?*“

Položka č. 2



Graf č. 2 *– relativní četnost odpovědí na položku č. 2 v dotazníku pro školní metodiky.*

Odpovědi vztahující se k číselným hodnotám 1–3 v grafu č. 2:

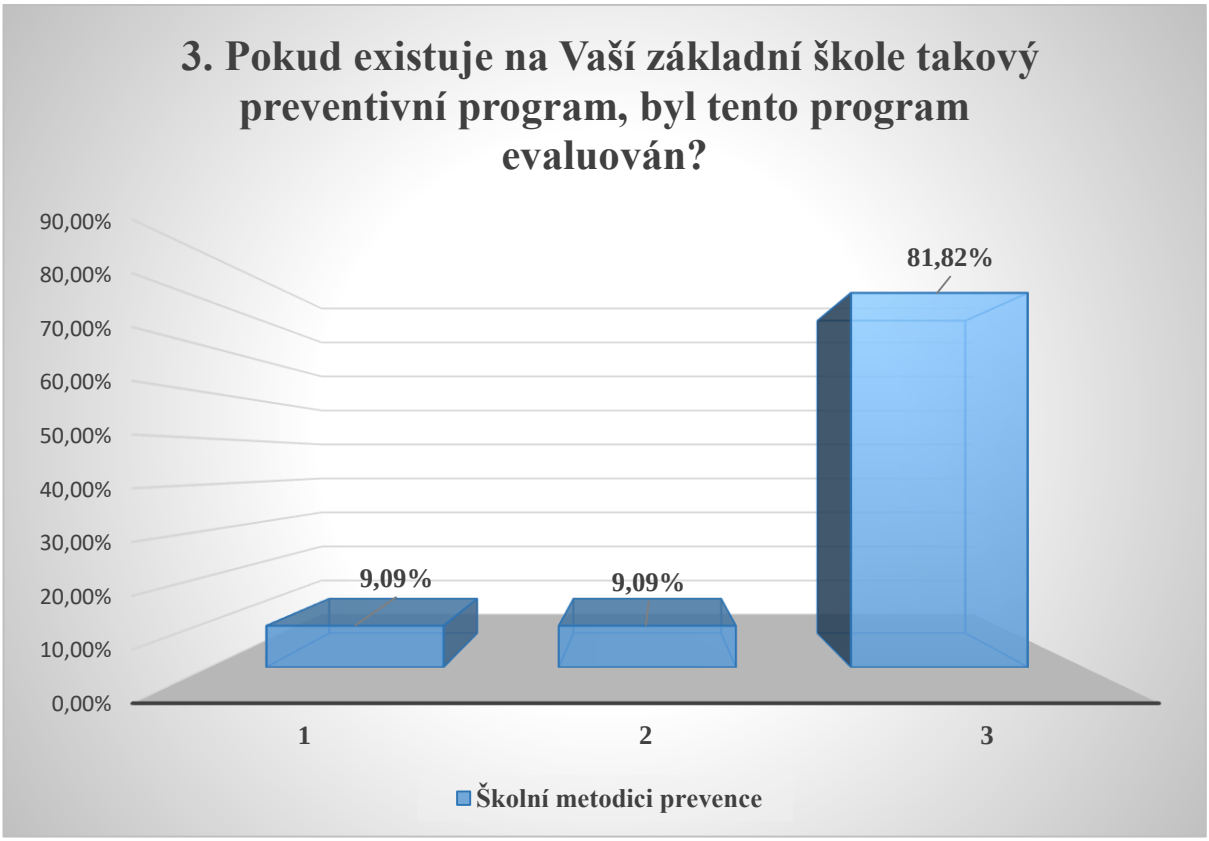
1	Ano, přímo proti různým podvodům.
2	Ano, ale jen částečně s jiným programem

3	Ne, nemáme program proti podvodům.

Na položku č. 2 odpovědělo všech 11 školních metodiků prevence. Na jedné škole v Prostějově se nachází program zaměřený přímo na internetové podvody při nákupu zboží, phishing, spam, scam, hoax. Na jedné škole v Prostějově se takový program nachází částečně s jiným programem, jehož název je „*Nebezpečí internetu*“. Všichni ostatní metodici prevence uvedli, že na jejich škole není žádný takový program primární prevence. Tři metodici prevence, kteří uvedli, že nemají žádný takový program, do poznámky uvedli, že riziko internetového nakupování je probíráno v rámci výuky finanční gramotnost.

Zjištěným výsledkem z této položky byl tak splněn dílčí cíl diplomové práce „*Jak je to s existencí preventivních programů proti podvodnému jednání v IT prostředí pro žáky 2. stupně na základních školách v Prostějově?*“

Položka č. 3



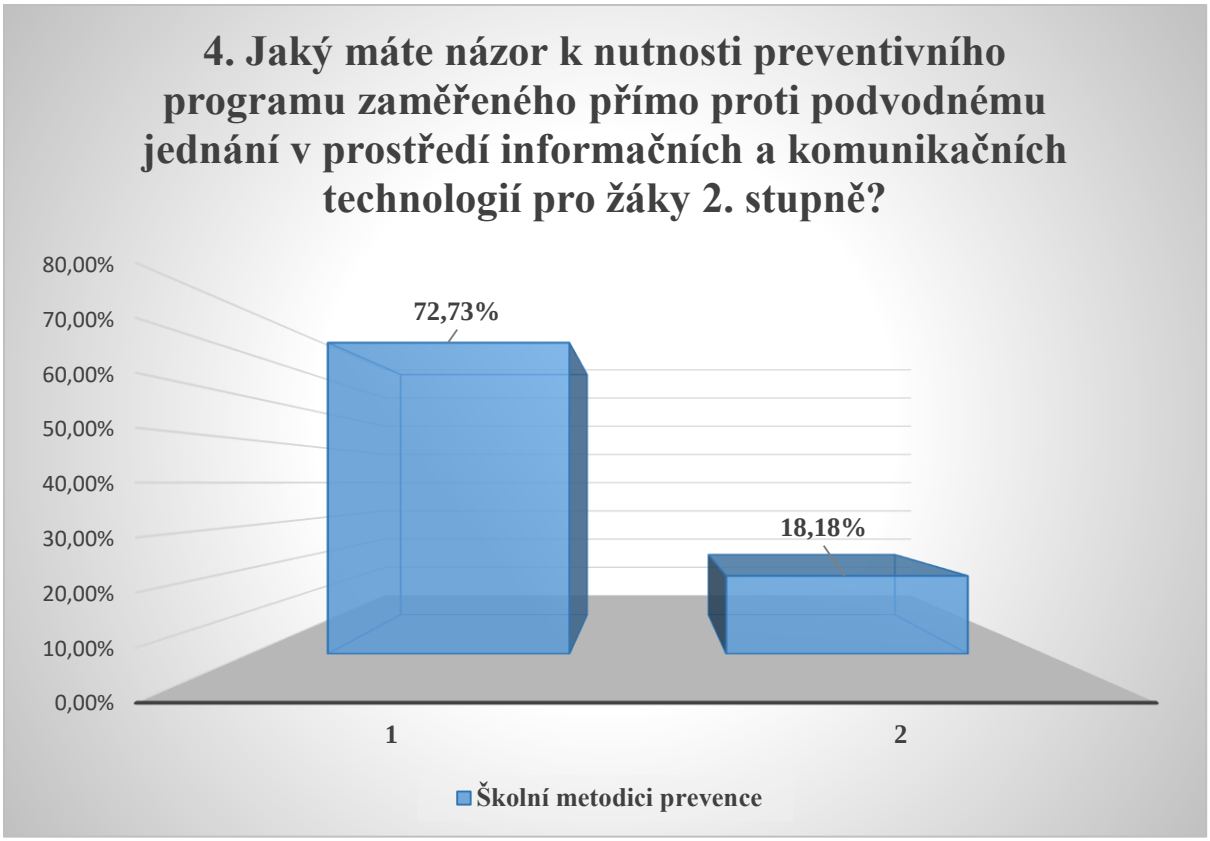
Graf č. 3 *– relativní četnost odpovědí na položku č. 3 v dotazníku pro školní metodiky.*

Odpovědi vztahující se k číselným hodnotám 1–3 v grafu č. 3:

1	Ano, byl evaluován žáky.
2	Ne, nebyl evaluován nikým.
3	Ne, nemáme žádný takový program proti podvodům

Na položku č. 3 odpovědělo všech 11 školních metodiků prevence. Preventivní program, který byl evaluován údajně s pozitivním výsledkem, konkrétně žáky, byl ten, který byl na internetové podvody zaměřen jen částečně. Preventivní program, který byl zaměřen konkrétně na internetové podvody, evaluován nikým nebyl. Všichni ostatní metodici uvedli, že žádný takový preventivní program na škole nemají.

Položka č. 4



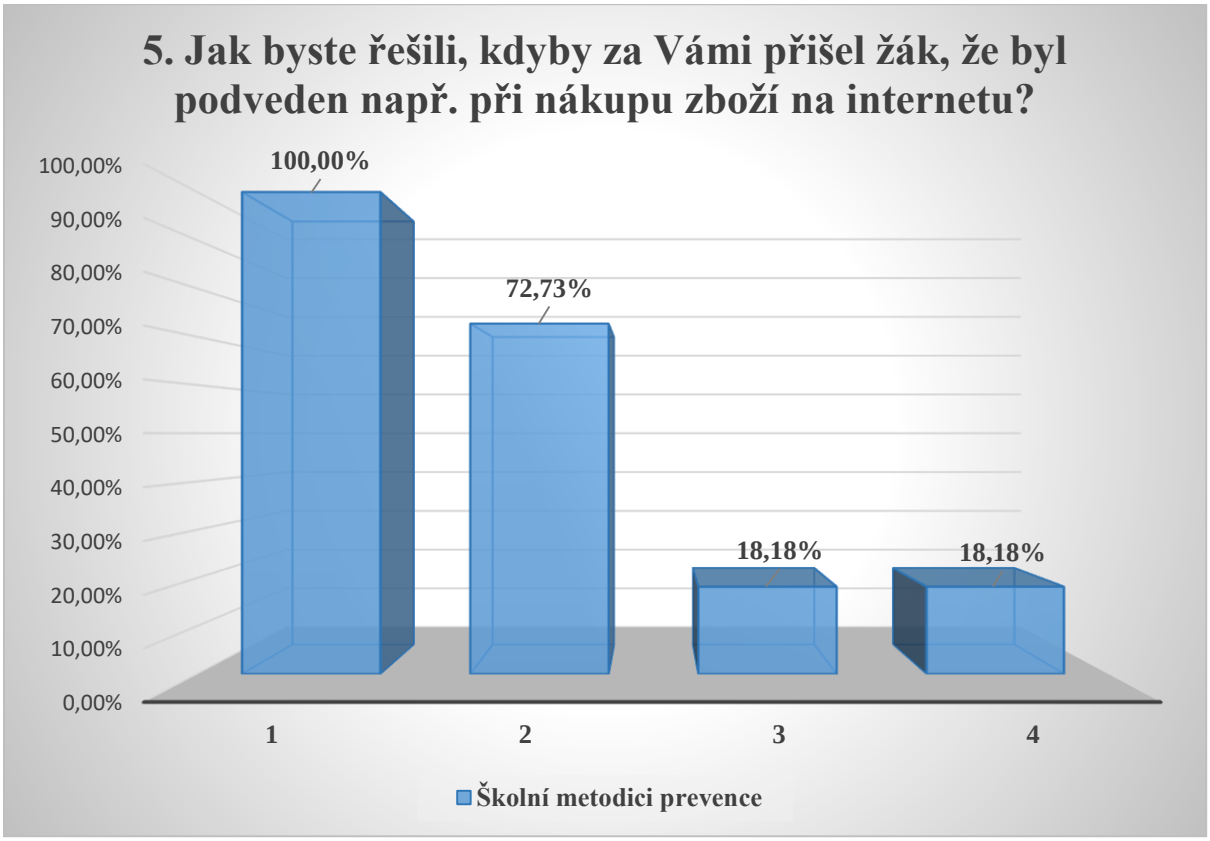
Graf č. 4 *– relativní četnost odpovědí na položku č. 4 v dotazníku pro školní metodiky.*

Odpovědi vztahující se k číselným hodnotám 1–2 v grafu č. 4:

1	Takový program bychom přivítali.
2	Je to záležitost rodičů a tento program není třeba.

Na položku č. 4 odpovědělo všech 11 školních metodiků prevence. Veškeré odpovědi byly zahrnuty pod dva hlavní body. Školní metodici, kteří uváděli, že takový program by přivítali, do poznámky obecně uváděli, že dnešní doba si to žádá; že někteří žáci vlastní platební karty; že na internetu nakupují. Ti metodici prevence, kteří takový preventivní program považují za nepotřebný, do poznámky shodně uvedli, že se podle jejich názoru nejedná o téma v kompetenci školy, ale rodičů.

Položka č. 5



Graf č. 5 *– relativní četnost odpovědí na položku č. 5 v dotazníku pro školní metodiky.*

Odpovědi vztahující se k číselným hodnotám 1–4 v grafu č. 5:

1	Nahlásili bychom to na Policii ČR.
2	Vyrozuměli bychom rodiče.

3	Obrátili bychom se na IT specialistu za účelem zajištění důkazů.
4	Oznámili bychom to vedení školy.

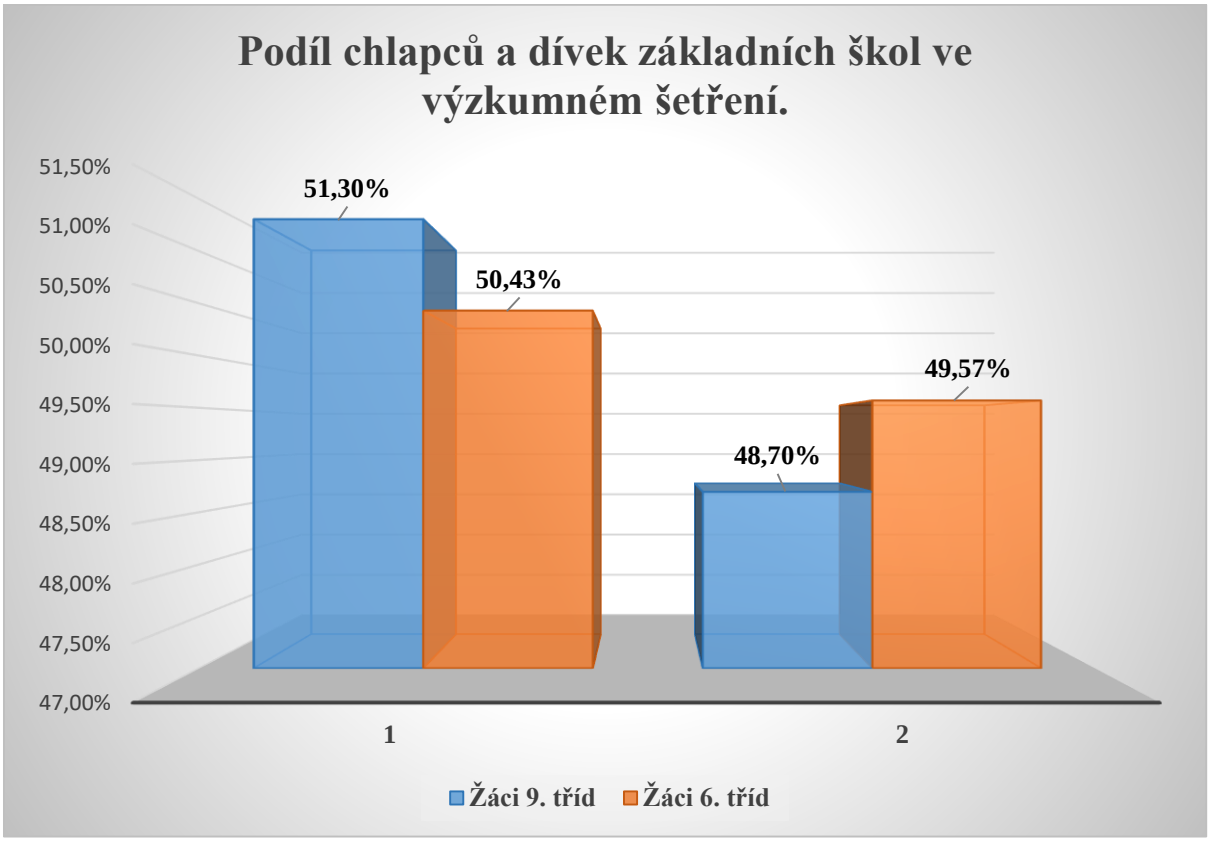
Na položku č. 5 odpovědělo všech 11 školních metodiků prevence. Veškeré varianty odpovědí byly zahrnuty pod čtyři hlavní celky odpovědí. Pouze dva metodici prevence, respektive ti, kteří by se obrátili na IT specialistu, do poznámky uvedli, že by se snažili danému žákovi co nejvíce pomoci v rámci možností školy.

Zjištěným výsledkem z této položky byl tak splněn dílčí cíl diplomové práce „*Jak by školní metodici prevence řešili, pokud by za ním přišel žák, že byl podveden v IT prostředí?*“

Pro vyhodnocení první části dotazníkového šetření je třeba konstatovat, že pouze 11 metodiků prevence představuje velmi malé množství respondentů, proto mohou být výsledné grafy určitým způsobem zavádějící vůči dalším školám v České republice. Dané výsledky se ovšem vztahují pouze na konkrétní město Prostějov ke všem 11 základním školám.

Ve druhé fázi dotazníkového šetření byli osloveni žáci základních škol v Prostějově, prostřednictvím ředitelů škol. Výběr škol byl vybrán na základě mechanického losování bez vracení, byly vybrány 4 školy, v jejichž třídách byly dotazníky rozdány pedagogy, což byla podmínka ředitelů. Dotazník měl 35 položek výzkumných, 1 položku zjišťující pohlaví a 1 položku zjišťující příslušnost k 6. nebo 9. třídě základní školy. Podrobné výsledky dotazníkového šetření s uváděnou jednotlivou četností u každé odpovědi zvlášť u žáků 6. tříd a 9. tříd ZŠ jsou založeny v příloze této diplomové práce. Na položky, které měly více než dvě varianty odpovědí (ano/ne), mohli žáci zvolit i více odpovědí, čímž de facto na každou odpověď v dotazníku odpovídali ano/ne. ANO, pokud odpověď zakřížkovali, NE pokud ji nezakřížkovali.

Podíl chlapců a dívek z výzkumného šetření

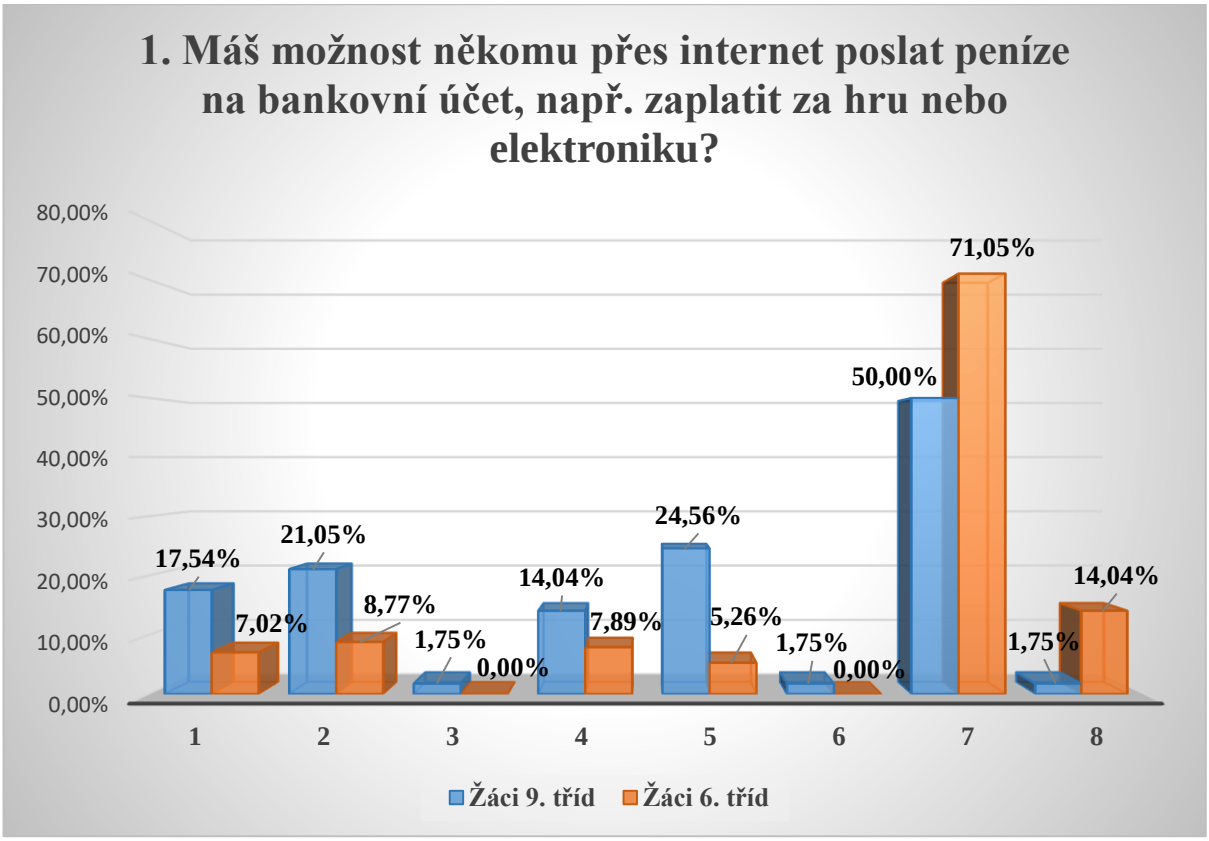


Graf č. 6 *– relativní četnost podílu chlapců a dívek základních škol z výzkumného šetření.*

Odpovědi vztahující se k číselným hodnotám 1–2 v grafu č. 6:

1	Dívka	**2**	Chlapec

Položka č. 1



Graf č. 7 *– relativní četnost odpovědí na položku č. 1 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–8 v grafu č. 7:

1	Ano, internetovým bankovnictvím.
2	Ano, platební kartou rodičů.
3	Ano, platební kartou dědečka/babičky.
4	Ano, přes Paypal, Gopay, PayU apod.

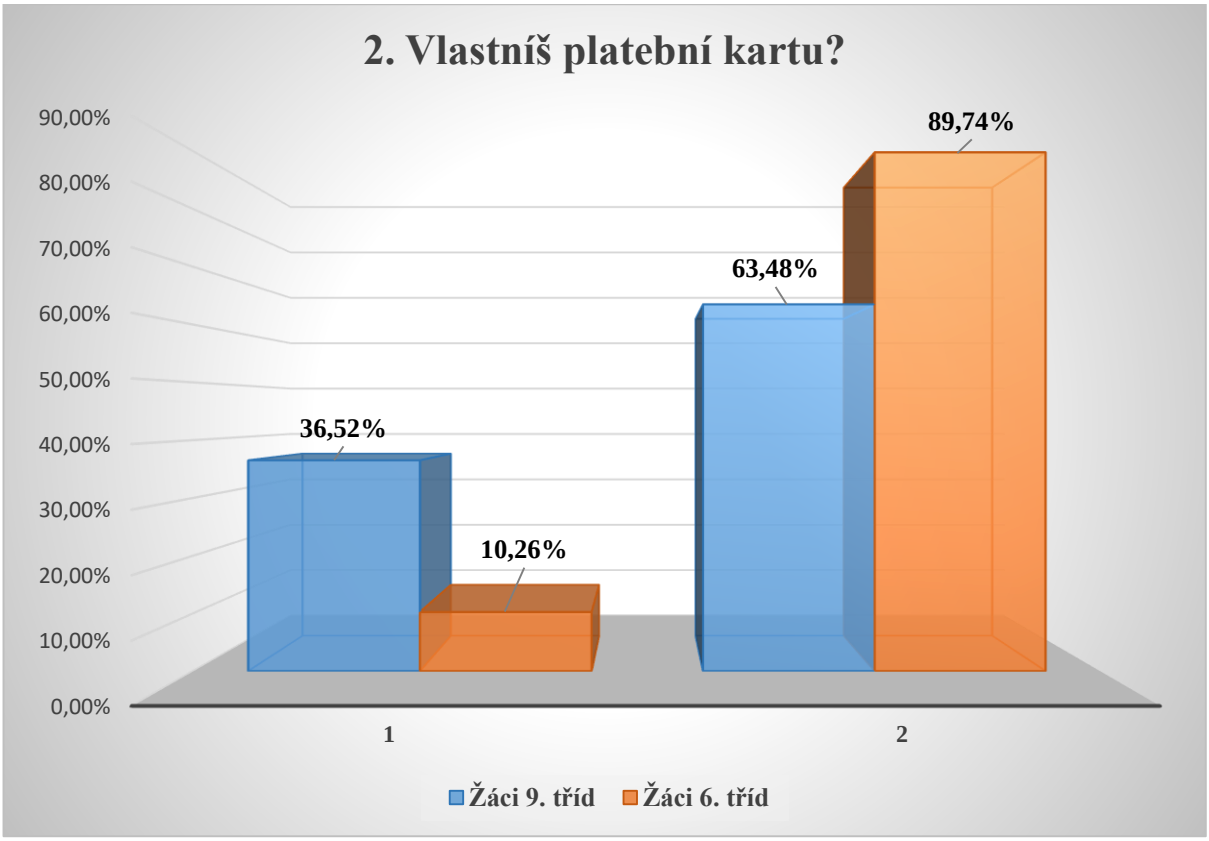
5	Ano, vlastní platební kartou.
6	Ano, platební kartou kamaráda.
7	Já sám/a ne.
8	Nevím.

První položkou bylo od žáků 9. tříd mimo jiné zjištěno, že téměř 18 % z nich má možnost zaslat platbu internetovým bankovnictvím, 21 % platební kartou rodičů, 14 % prostřednictvím elektronické peněženky typu Paypal apod., téměř 25 % vlastní platební kartou a 50 % z nich nemá žádnou možnost platbu přes internet zaslat.

Od žáků 6. tříd bylo pak mimo jiné zjištěno, že 7 % z nich má možnost zaslat platbu internetovým bankovnictvím, téměř 9 % platební kartou rodičů, téměř 8% prostřednictvím systému typu Paypal apod., 5 % vlastní platební kartou a 71 % nemá vůbec žádnou možnost platbu přes internet zaslat. 14 % žáků na tuto položku odpověď nevědělo.

Zjištěným výsledkem z této položky byl tak splněn dílčí cíl diplomové práce „*Jaké mají vybraní žáci 6. a 9. tříd základních škol v Prostějově možnosti zaslání platby prostřednictvím internetu na bankovní účet?*“

Položka č. 2



Graf č. 8 *– relativní četnost odpovědí na položku č. 2 v dotazníku pro žáky základních škol.*

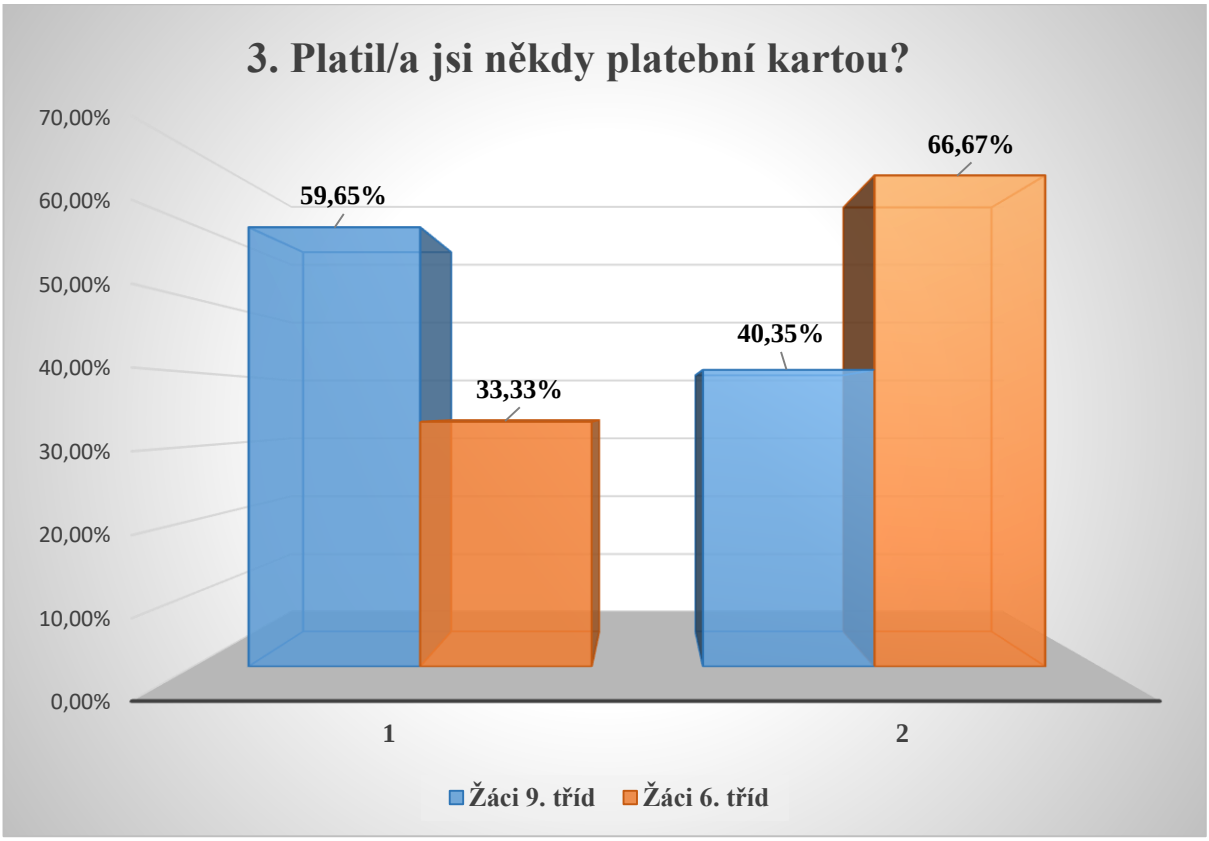
Odpovědi vztahující se k číselným hodnotám 1–2 v grafu č. 8:

1	Ano	**2**	Ne

Touto položkou bylo zjišťováno, jaká je četnost žáků, kteří mají svoji vlastní platební kartu. **Téměř 37 % žáků 9. tříd uvedlo, že platební kartu vlastní, stejně jako 10 % žáků 6. tříd.**

Zjištěným výsledkem z této položky byl tak splněn částečně dílčí cíl diplomové práce *„Jak je to u vybraných žáků 6. tříd a 9. tříd základních škol v Prostějově s vlastnictvím vlastní platební karty a využíváním internetového bankovnictví?“*

Položka č. 3



Graf č. 9 *– relativní četnost odpovědí na položku č. 3 v dotazníku pro žáky základních škol.*

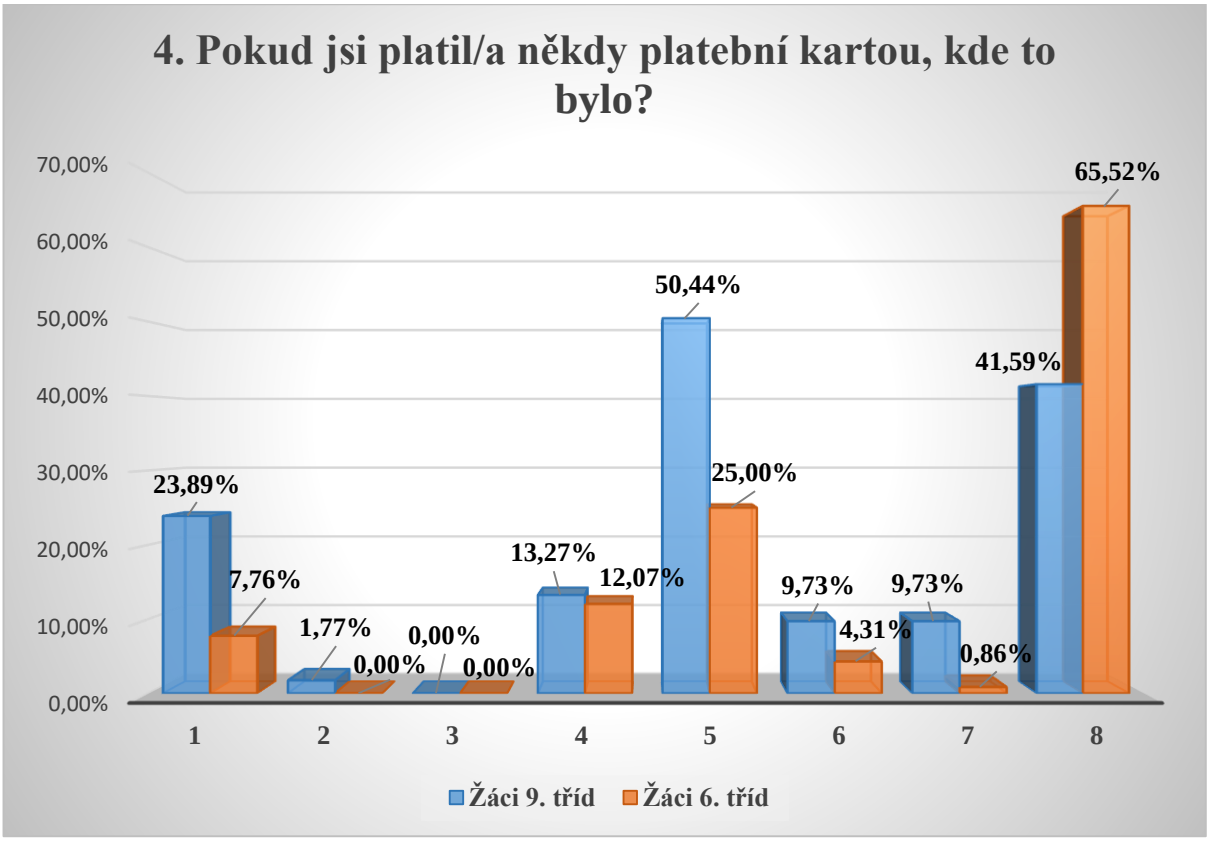
Odpovědi vztahující se k číselným hodnotám 1–2 v grafu č. 9:

1	Ano	**2**	Ne

Samotné vlastnictví platební karty žáky základních škol neznamená to, že žáci platební kartu používají a platí s ní nebo ne. Platební karta a údaje s ní spojené jsou velmi častým předmětem útoku pachatele podvodného jednání v IT prostředí, a proto je důležité zjištění, v jaké míře žáci s platební kartou přišli do styku, respektive platili.

Téměř 60 % žáků 9. uvedlo, že někdy platební kartou platilo, v případě žáků 6. tříd to bylo 33 %.

Položka č. 4



Graf č. 10 *– relativní četnost odpovědí na položku č. 4 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–8 v grafu č. 10:

1	Na internetu, za nákup v obchodě (e-shopu).
2	Na internetu, za nákup přes inzerát v bazaru.
3	Na internetu, za nákup v aukci.
4	Na internetu, za nákup počítačové hry.

5	V obchodě.
6	V restauraci.
7	Na poště nebo někde jinde.
8	Nikdy jsem neplatil/a platební kartou.

Na fyzickou manipulaci s platební kartou je zaměřen skimming, na údaje potřebné k zaplacení platební kartou je zaměřen např. phishing nebo malware. Danou položkou v dotazníku bylo zjišťováno, kde konkrétně platební kartou, pokud vůbec, žáci platili.

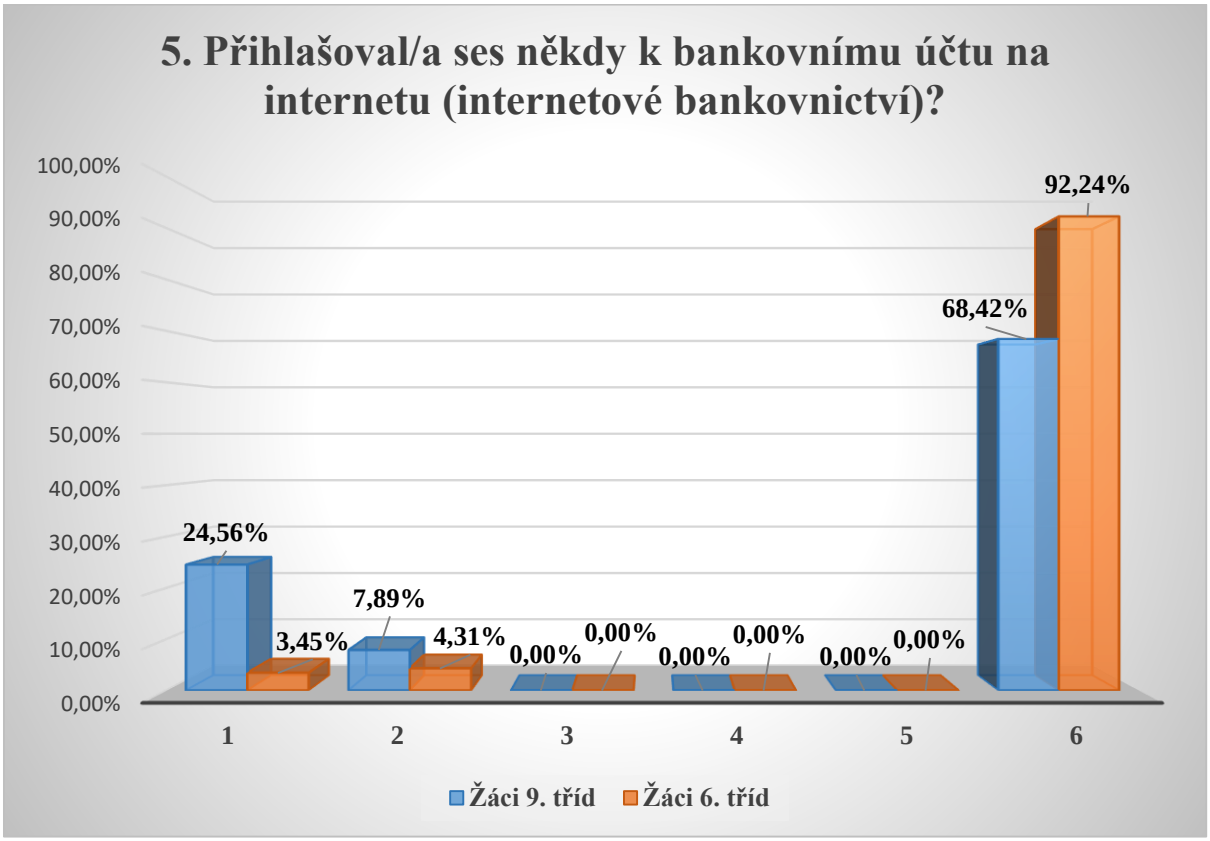
U žáků 9. tříd bylo zjištěno, že téměř 24 % z nich platilo kartou za nákup v e-shopu, téměř 2 % za nákup přes inzerát v bazaru, 13 % za nákup počítačové hry, 50 % v obchodě, téměř 10 % v restauraci, téměř 10 % na poště nebo jinde a téměř 42 % žáků uvedlo, že nikdy platební kartou neplatilo.

U žáků 6. tříd bylo zjištěno, že téměř 8 % z nich platilo kartou za nákup v e-shopu, 12 % za nákup počítačové hry, 25 % v obchodě, 4 % v restauraci a téměř 66 % uvedlo, že nikdy

platební kartou neplatilo. Touto položkou byly zároveň ověřeny negativní odpovědi z položky č. 3.

Zjištěným výsledkem z této položky byl tak splněn dílčí cíl diplomové práce „*Jaké mají vybraní žáci 6. a 9. tříd základních škol v Prostějově zkušenosti s placením platební kartou v IT prostředí?*“ Jak často v daných případech platí platební kartou žáci, bohužel zjišťováno nebylo.

Položka č. 5



Graf č. 11 *– relativní četnost odpovědí na položku č. 5 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–6 v grafu č. 11:

1	Ano, k vlastnímu bankovnímu účtu.
2	Ano, k bankovnímu účtu rodičů.
3	Ano, k bankovnímu účtu kamaráda.

4	Ano, k bankovnímu účtu dědečka/babičky.
5	Ano, k bankovnímu účtu někoho jiného.
6	Ne.

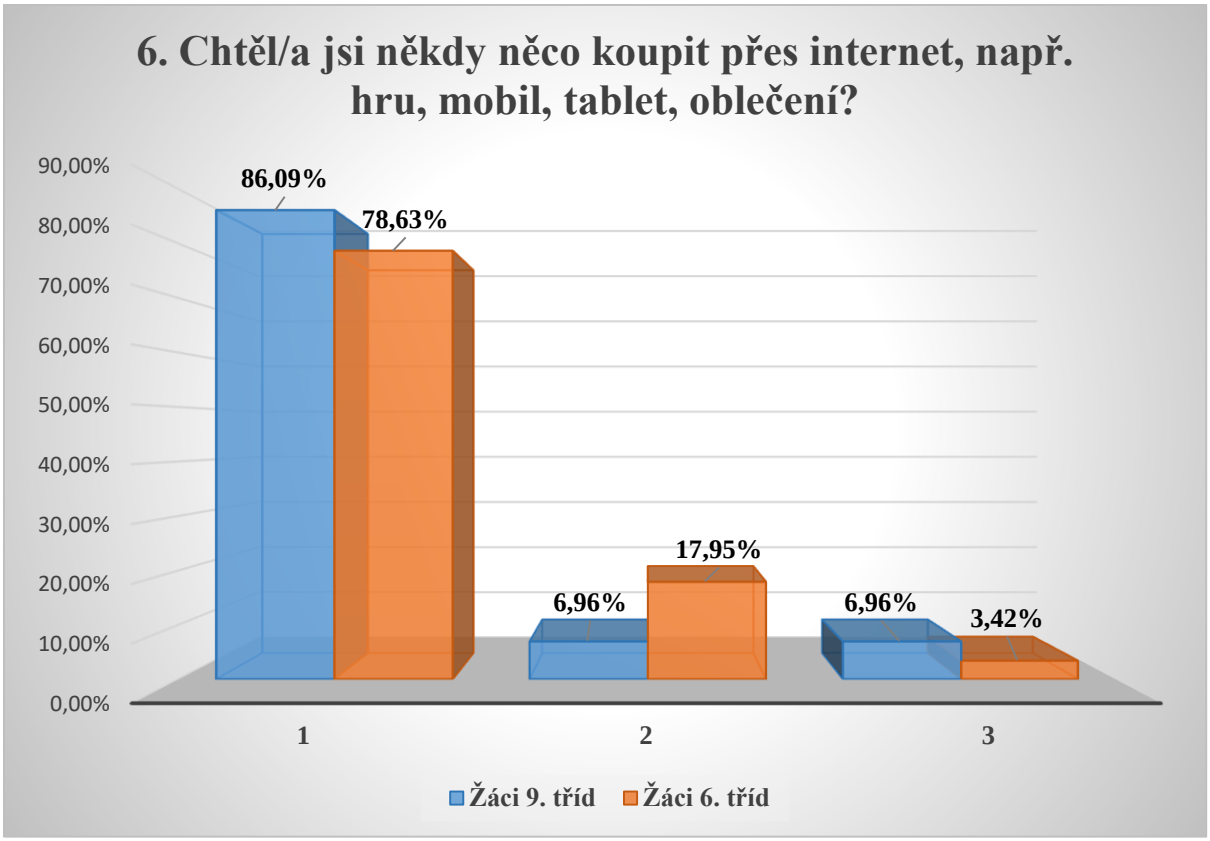
Při zkoumání daného jevu bylo podstatné rovněž zjistit, jakou zkušenost mají žáci základních škol s přihlašováním do internetového bankovnictví.

Téměř 25% žáků 9. třídu uvedlo, že se přihlásilo k internetovému bankovnictví k vlastnímu bankovnímu účtu a téměř 8 % se přihlásilo někdy k bankovnímu účtu rodičů.

Téměř 4 % žáků 6. tříd se přihlásilo k vlastnímu bankovnímu účtu a 4 % se přihlásilo někdy k bankovnímu účtu rodičů.

Zjištěným výsledkem z této položky byla tak splněna druhá část dílčího cíle diplomové práce *„Jak je to u vybraných žáků 6. tříd a 9. tříd základních škol v Prostějově s vlastnictvím vlastní platební karty a využíváním internetového bankovnictví?“* Jak často se k danému internetovému bankovnictví žáci přihlašují, zjišťováno nebylo.

Položka č. 6



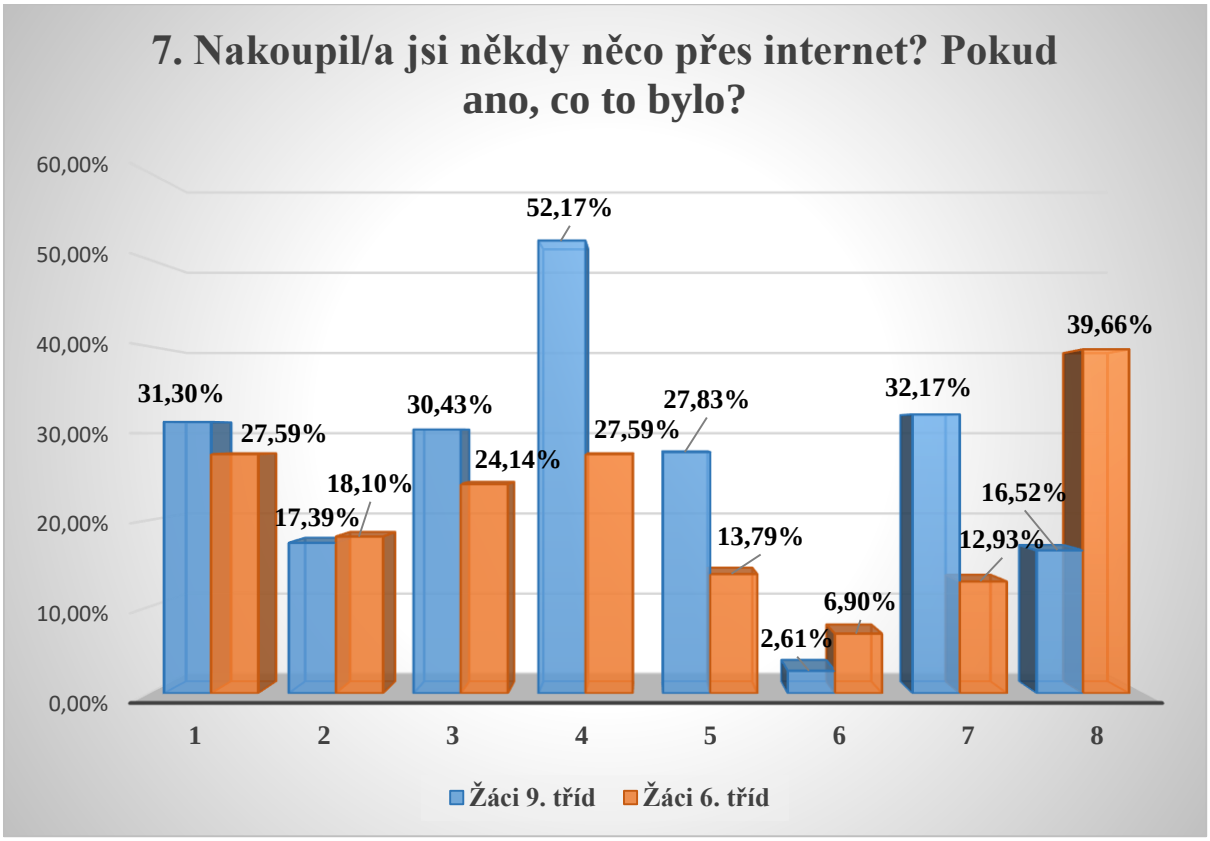
Graf č. 12 *– relativní četnost odpovědí na položku č. 6 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–3 v grafu č. 12:

1	Ano	**2**	Ne	**3**	Nevím

Tato položka, ačkoliv přímo nenaplňuje žádný dílčí cíl práce, přináší zjištění, zda mají žáci vůbec zájem o nakupování v IT prostředí, což může být předpokladem vyhledávání zboží na internetu. 86 % žáků 9. tříd uvedlo pozitivní odpověď, téměř 7 % uvedlo negativní odpověď a téměř 7 % nevědělo. Téměř 79 % žáků 6. tříd uvedlo pozitivní odpověď, 18 % negativní a 3 % nevědělo.

Položka č. 7



Graf č. 13 *– relativní četnost odpovědí na položku č. 7 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–8 v grafu č. 13:

1	Ano, hry.
2	Ano, vylepšení do her.
3	Ano, elektroniku.
4	Ano, oblečení.

5	Ano, sportovní věci.
6	Ano, hračky.
7	Ano, jiné věci.
8	Nenakupoval/a jsem nic přes internet.

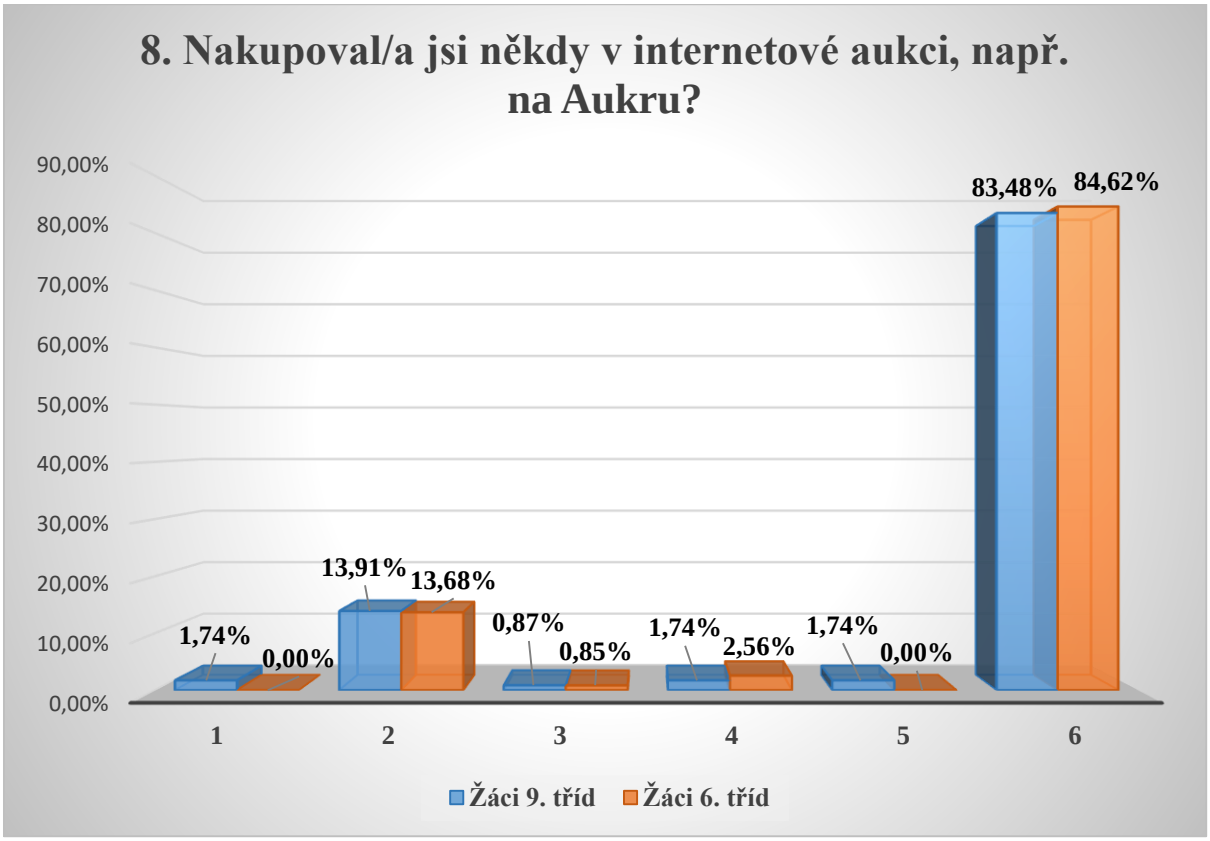
Tato položka se zabývala otázkou, zda žáci nakoupili v prostředí internetu někdy nějaké zboží a pokud ano, tak jaké. Přesto, že položka nespadá přímo pod některý dílčí cíl, pod hlavní cíl práce ji lze zahrnout (zda mají žáci zkušenosti s nakupováním).

83 % žáků 9. tříd uvedlo, že někdy něco přes internet nakoupilo, stejně jako 60 % žáků 6. tříd.

Žáci 9. tříd nejčastěji nakoupili oblečení (52 %), hry (31 %), elektroniku (30 %), sportovní věci (28 %), vylepšení do her (17 %), hračky (3 %) a jiné než nabízené věci (32 %).

Žáci 6. tříd nejčastěji nakoupili oblečení (téměř 28 %) stejně jako hry (téměř 28 %), elektroniku (24 %), vylepšení do her (18 %), sportovní věci (téměř 14 %), hračky (7 %) a jiné než nabízené věci (13 %).

Položka č. 8



Graf č. 14 *– relativní četnost odpovědí na položku č. 8 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–6 v grafu č. 14:

1	Ano, sám/a jsem nakupoval/a.
2	Ano, s rodičem jsem nakupoval/a.
3	Ano, s dědečkem/babičkou jsem nakupoval/a.

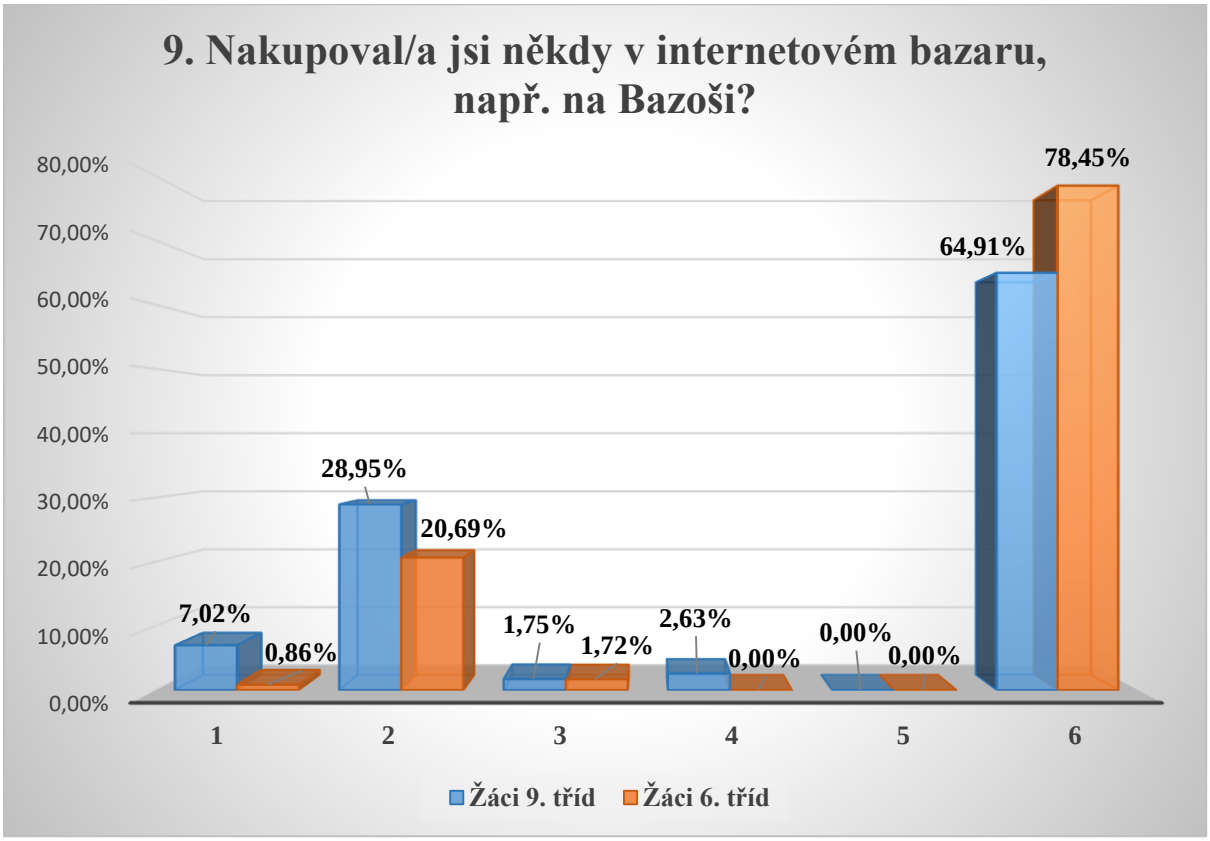
4	Ano, s kamarádem jsem nakupoval/a.
5	Ano, s někým jiným jsem nakupoval/a.
6	Nenakupoval/a jsem.

Tato položka je již specifiky zaměřena na zjištění, zda mají žáci zkušenost s nákupem prostřednictvím internetové aukce.

Téměř 16 % žáků 9. tříd má s nákupem v aukci nějakou zkušenost, stejně jako 15 % žáků 6. tříd. V naprosté většině obou skupin žáci nakupovali s rodiči (totožně téměř 14 %), přičemž pouze 2 % žáků 9. tříd uvedlo, že nakupovali sami.

Zjištěným výsledkem z této položky byla tak splněna část dílčího cíle diplomové práce *„Jaký je rozdíl v četnosti nakupování v IT prostředí u vybraných žáků 6. a 9. tříd na základních školách v Prostějově?“*

Položka č. 9



Graf č. 15 *– relativní četnost odpovědí na položku č. 9 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–6 v grafu č. 15:

1	Ano, sám/a jsem nakupoval/a.
2	Ano, s rodičem jsem nakupoval/a.
3	Ano, s dědečkem/babičkou jsem nakupoval/a.

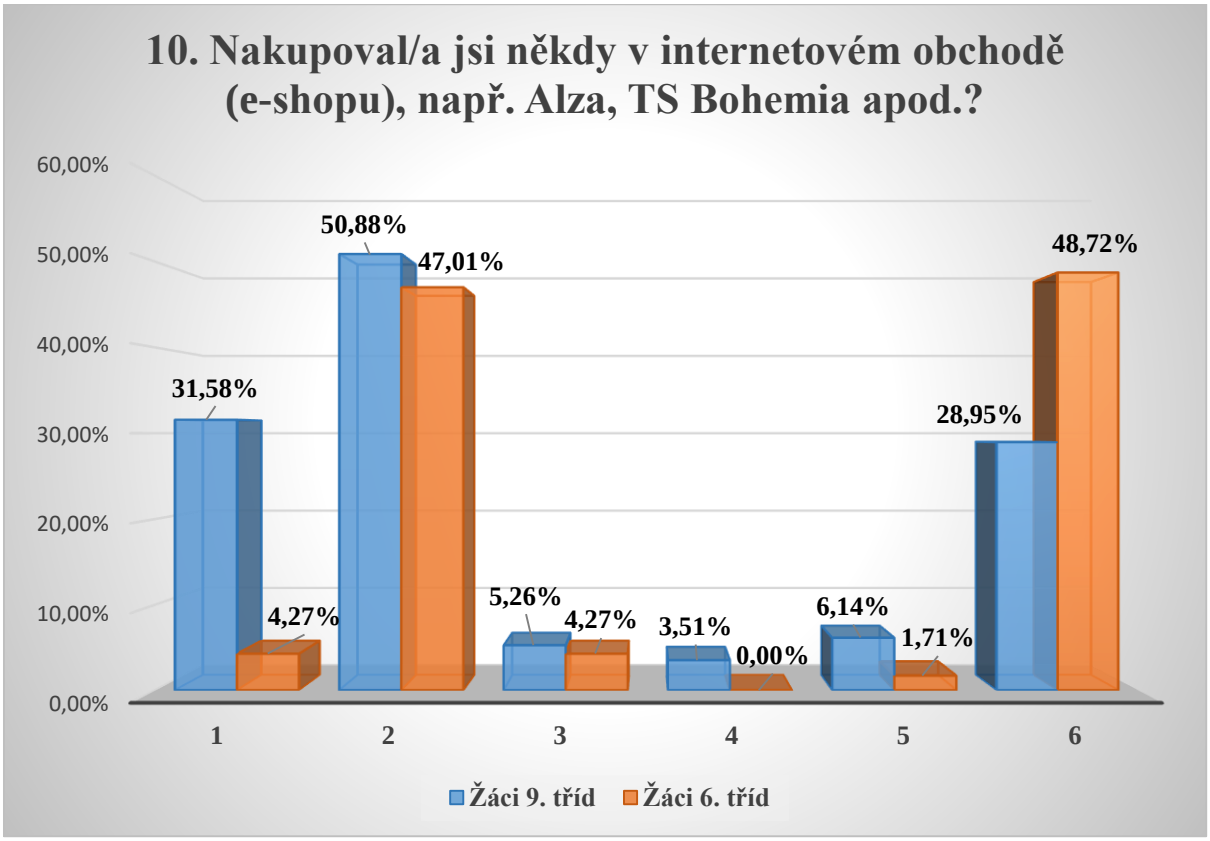
4	Ano, s kamarádem jsem nakupoval/a.
5	Ano, s někým jiným jsem nakupoval/a.
6	Nenakupoval/a jsem.

Tato položka je specifiky zaměřena na zjištění, zda mají žáci zkušenost s nákupem prostřednictvím internetového bazaru.

35 % žáků 9. tříd někdy v bazaru nakupovalo, stejně jako téměř 22 % žáků 6. tříd. Ve většině obou skupin žáci nakupovali s rodiči (29 % v případě žáků 9. tříd, téměř 21 % v případě žáků 6. tříd), přičemž 7 % žáků 9. tříd v internetovém bazaru nakupovalo samo, stejně jako necelé 1 % žáků 6. tříd. Žáci 9. tříd také nakupovali s dědečkem nebo babičkou (téměř 2 %) nebo s kamarádem (téměř 3 %). Žáci 6. tříd nakupovali s dědečkem nebo babičkou také minimálně (téměř 2 %)

Zjištěným výsledkem z této položky byla tak splněna část dílčího cíle diplomové práce *„Jaký je rozdíl v četnosti nakupování v IT prostředí u vybraných žáků 6. a 9. tříd na základních školách v Prostějově?“*

Položka č. 10



Graf č. 16 *– relativní četnost odpovědí na položku č. 10 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–6 v grafu č. 16:

1	Ano, sám/a jsem nakupoval/a.
2	Ano, s rodičem jsem nakupoval/a.
3	Ano, s dědečkem/babičkou jsem nakupoval/a.

4	Ano, s kamarádem jsem nakupoval/a.
5	Ano, s někým jiným jsem nakupoval/a.
6	Nenakupoval/a jsem.

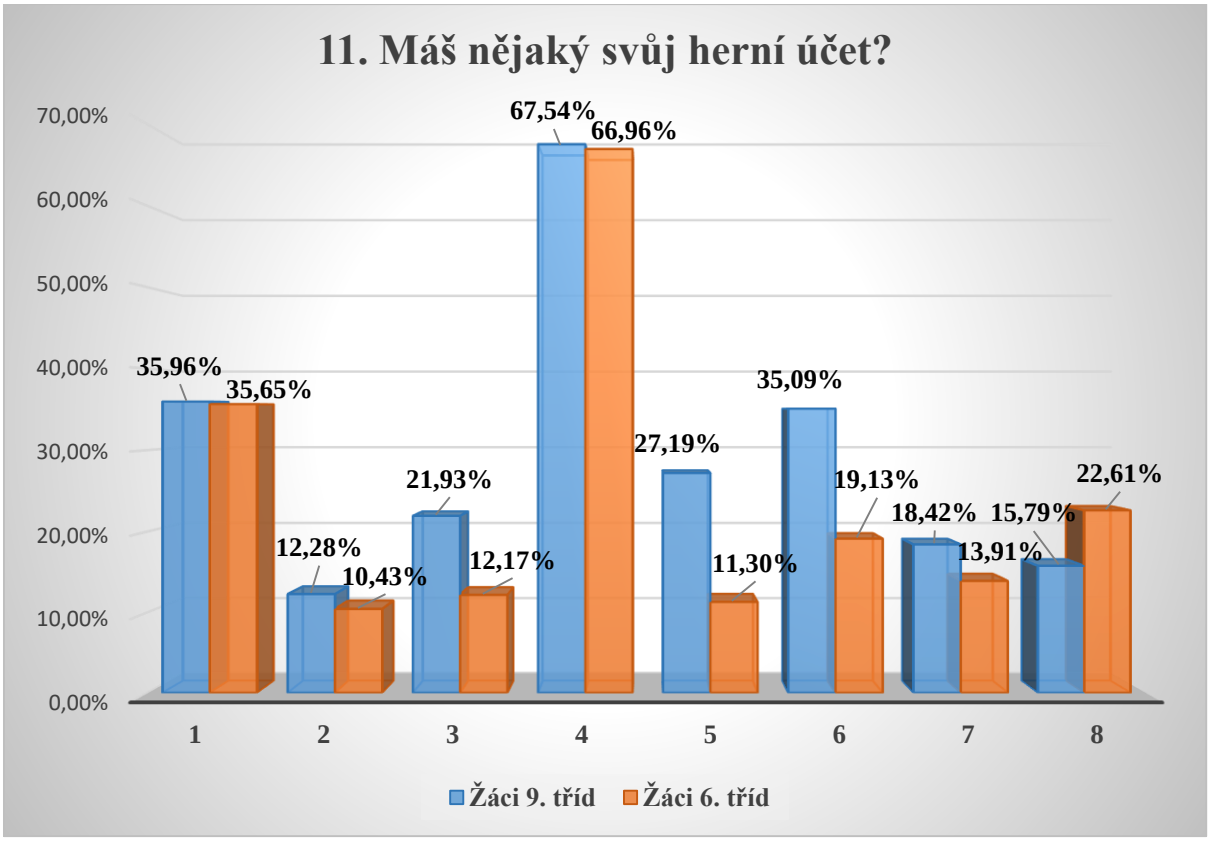
Tato položka je specifiky zaměřena na zjištění, zda mají žáci zkušenost s nákupem prostřednictvím internetového obchodu (e-shopu).

71 % žáků 9. tříd někdy v internetovém obchodě nakupovalo, stejně jako téměř 51 % žáků 6. tříd. Ve většině obou skupin žáci nakupovali s rodiči (téměř 51 % v případě žáků 9. tříd, 47 % v případě žáků 6. tříd), přičemž téměř 32 % žáků 9. tříd v internetovém obchodě nakupovalo samo, stejně jako 4 % žáků 6. tříd.

Žáci 9. tříd nakupovali také někdy s dědečkem nebo babičkou (5 %), s kamarádem (téměř 4 %) nebo s někým jiným (6 %). Žáci 6. tříd nakupovali někdy s dědečkem nebo babičkou (4 %) nebo s někým jiným (téměř 2 %).

Zjištěným výsledkem z této položky byla tak splněna část dílčího cíle diplomové práce *„Jaký je rozdíl v četnosti nakupování v IT prostředí u vybraných žáků 6. a 9. tříd na základních školách v Prostějově?“*

Položka č. 11



Graf č. 17 *– relativní četnost odpovědí na položku č. 11 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–8 v grafu č. 17:

1	Ano, Steam
2	Ano, Playstation Network.
3	Ano, Xbox Live.
4	Ano, Google Play.

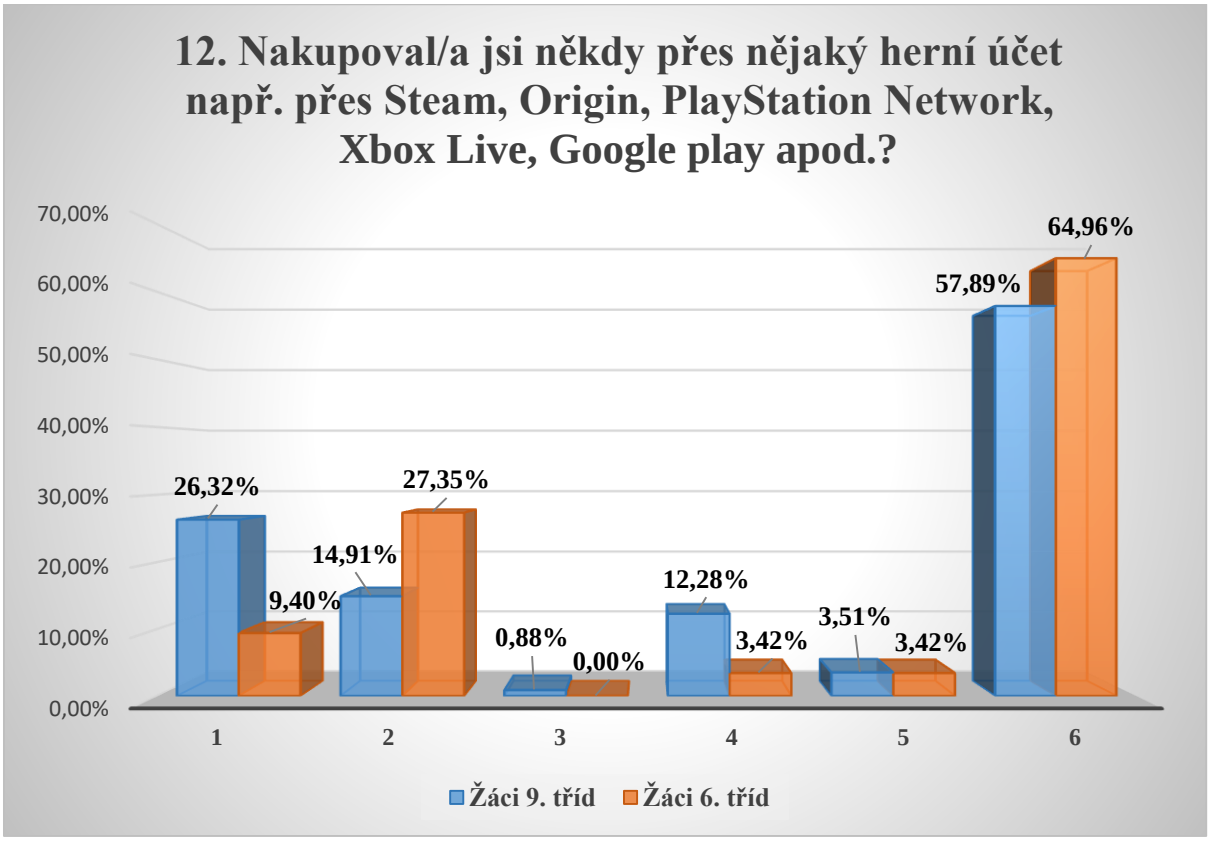
5	Ano, App Store.
6	Ano, Microsoft Store.
7	Ano, mám ale jiný účet.
8	Ne, nemám žádný podobný herní účet.

Herní účty mnohdy s herním obsahem, přihlašovací údaje, osobní a další citlivé údaje s těmito účty související jsou rovněž cílem útoku pachatele podvodného jednání v IT prostředí, a přesto, že není tato položka v dotazníku vázána přímo na dílčí cíl práce, může být podstatná pro případné další zkoumání.

84 % žáků 9. tříd uvedlo, že má nějaký herní účet, stejně jako 77 % žáků 6. tříd. Nejčastějším herním účtem mezi žáky 9. tříd a žáky 6. tříd (v obou případech kolem 67 %) je Google play (pro operační systém Android). Následně žáci 9. tříd a žáci 6. tříd využívají Steam

(v obou případech 36 %). Dále mají žáci 9. tříd účty Microsoft Store (35 %), App Store (27 %), Xbox live (22 %), jiný účet (18 %) a Playstation Network (12 %). Žáci 6. tříd mají účty dále u Microsoft Store (19 %), jiný účet (14 %), Xbox Live (12 %), App Store (11 %), Playstation Network (10 %).

Položka č. 12



Graf č. 18 *– relativní četnost odpovědí na položku č. 12 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–6 v grafu č. 18:

1	Ano, sám/a jsem si tam nakoupil/a.
2	Ano, s rodičem jsem tam nakupoval/a.
3	Ano, s dědečkem/babičkou jsem nakupoval/a.

4	Ano, s kamarádem jsem tam nakupoval/a.
5	Ano, s někým jiným jsem tam nakupoval/a.
6	Nenakupoval/a jsem.

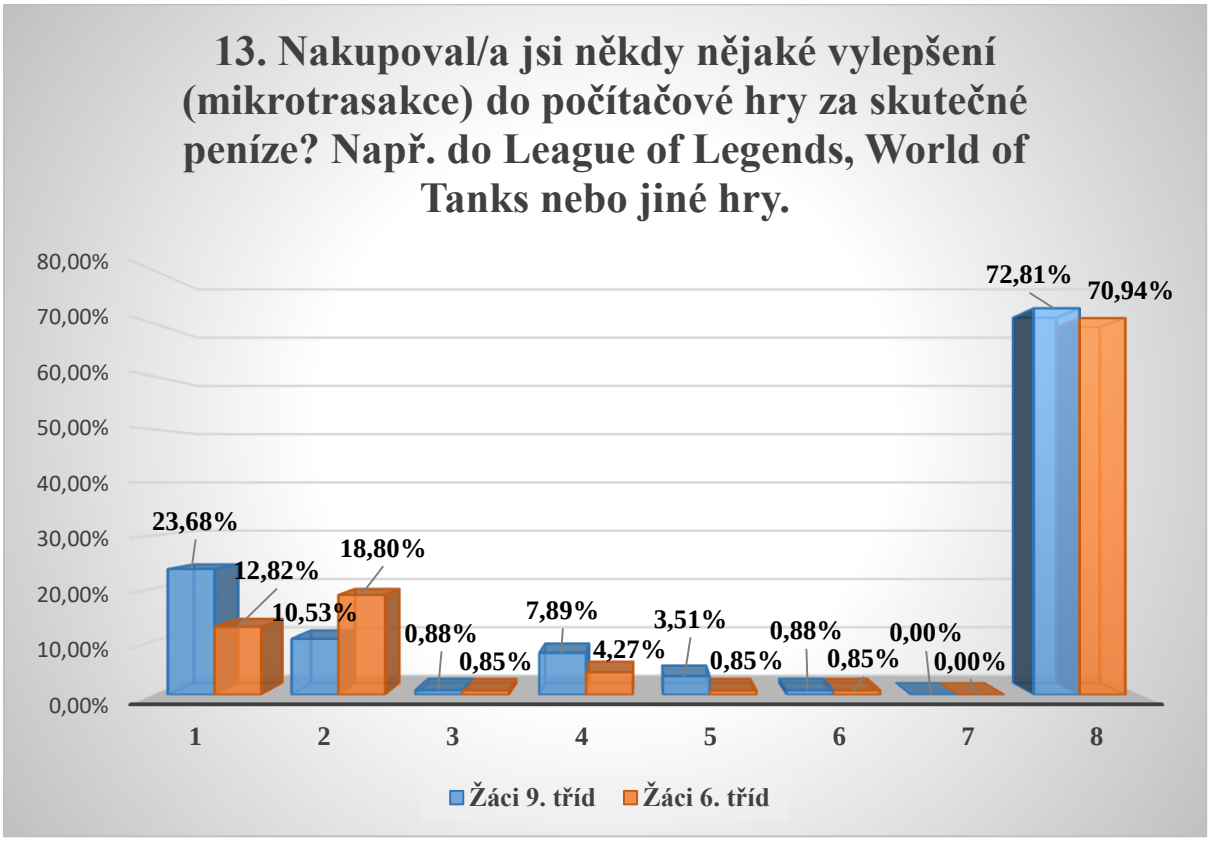
Herní účty slouží rovněž k nakupování her, a proto bylo podstatné zjistit, zda žáci přes tyto herní účty nakupují a pokud ano, tak s kým.

42 % žáků 9. tříd uvedlo, že někdy nakoupilo přes herní účet, stejně jako 35 % žáků 6. tříd. 26 % žáků 9. tříd nakupovalo samo, stejně jako 9 % žáků 6. tříd. S rodiči nakupovalo 15 % žáků 9. tříd a 27 % žáků 6. tříd. Dále žáci 9. tříd nakupovali někdy

s kamarádem (12 %), s někým jiným (téměř 4 %) nebo s dědečkem nebo babičkou (téměř 1 %). Žáci 6. tříd nakupovali někdy také s kamarádem (3 %) nebo s někým jiným (3 %).

Zjištěným výsledkem z této položky byla tak splněna část dílčího cíle diplomové práce *„Jaký je rozdíl v četnosti nakupování v IT prostředí u vybraných žáků 6. a 9. tříd na základních školách v Prostějově?“*

Položka č. 13



Graf č. 19 *– relativní četnost odpovědí na položku č. 13 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–8 v grafu č. 19:

1	Ano, sám/a jsem tam nakupoval/a.
2	Ano, s rodičem jsem tam nakupoval/a.
3	Ano, s dědečkem/babičkou jsem nakupoval/a.
4	Ano, s kamarádem jsem tam nakupoval/a.

5	Ano, s někým jiným jsem tam nakupoval/a.
6	Ano, sám/a jsem si to koupil/a, bez vědomí rodičů, z jejich platební karty.
7	Ano, sám/a jsem si to koupil/a, bez vědomí dědečka/babičky, z jejich platební karty.
8	Nenakupoval/a jsem nic takového.

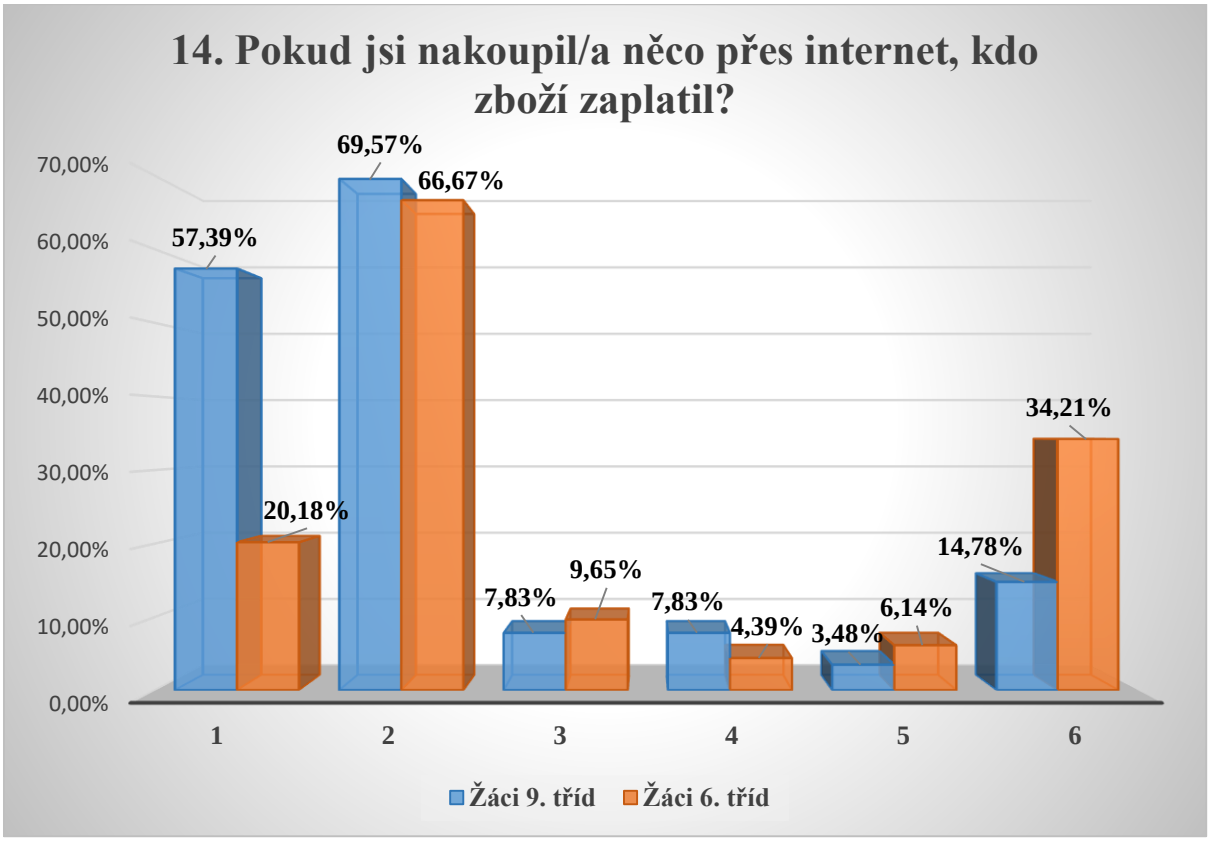
Herní vývojáři mnohdy poskytují počítačové hry zdarma ke stažení a jejich prostředkem k výdělku jsou nákupy herního vylepšení za menší částky v podobě mikrotransakcí. Proto bylo

předmětem zjištění ve výzkumném šetření i to, zda takový obsah žáci nakupují a pokud ano, tak s kým.

27 % žáků 9. tříd uvedlo, že někdy nakoupilo herní vylepšení, stejně jako 29 % žáků 6. tříd. Téměř 24 % žáků 9. tříd nakupovalo samo, stejně jako téměř 13 % žáků 6. tříd. S rodiči nakupovalo téměř 11 % žáků 9. tříd a téměř 19 % žáků 6. tříd. Dále žáci 9. tříd nakupovali někdy s kamarádem (téměř 8 %), s někým jiným (téměř 4 %) nebo s dědečkem nebo babičkou (téměř 1%). Žáci 6. tříd nakupovali někdy také s kamarádem (4 %) nebo s někým jiným (téměř 1 %) nebo s dědečkem nebo babičkou (téměř 1 %). Velmi zajímavým zjištěním bylo, že **téměř 1 % žáků 9. tříd stejně jako téměř 1% žáků 6. tříd provedlo nákup z platební karty rodičů, bez jejich vědomí. Dané jednání je de facto protiprávní jednání!** (Respondent zamlčel podstatné skutečnosti, čímž způsobil škodu majiteli bankovního účtu – rodičům).

Zjištěným výsledkem z této položky byla tak splněna část dílčího cíle diplomové práce *„Jaký je rozdíl v četnosti nakupování v IT prostředí u vybraných žáků 6. a 9. tříd na základních školách v Prostějově?“*

Položka č. 14



Graf č. 20 *– relativní četnost odpovědí na položku č. 14 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–6 v grafu č. 20:

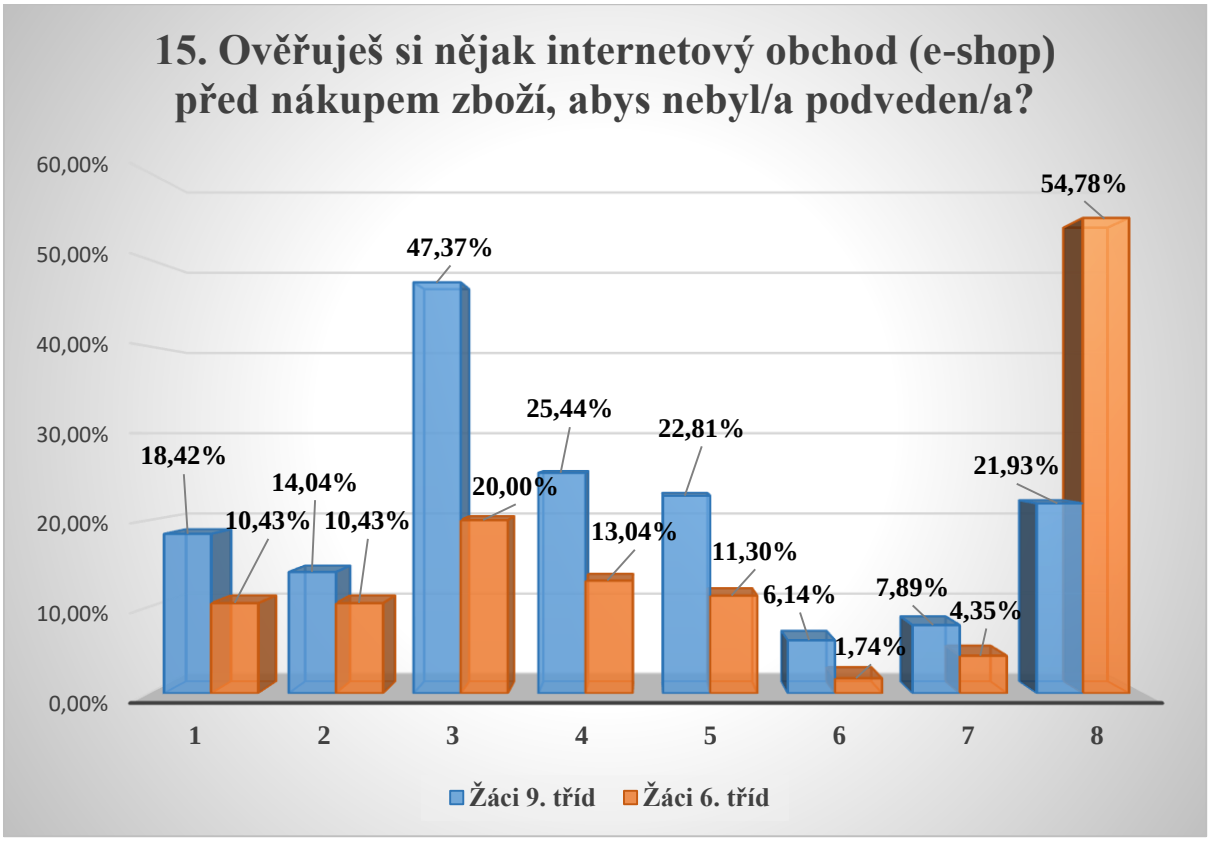
1	Já sám/a.
2	Rodiče.
3	Dědeček/babička.

4	Kamarád.
5	Někdo jiný.
6	Nenakupoval/a jsem nic přes internet.

85 % žáků 9. tříd uvedlo na tuto položku č. 14, že někdy nakupovalo přes internet, stejně jako 66 % žáků 6. tříd. Obdobně dopadlo dotazování v položce č. 7, kde 83 % žáků 9. tříd uvedlo, že někdy něco přes internet nakoupilo (rozdíl 2 %), stejně jako 60 % žáků 6. tříd (což je ale rozdíl 6 % ve stejné odpovědi?).

57 % žáků 9. tříd samo zaplatilo zboží, které přes internet zakoupili, stejně jako 20 % žáků 6. tříd. Za téměř 70 % žáků 9. tříd zaplatili za zboží nakoupené přes internet někdy rodiče, stejně jako za téměř 67 % žáků 6. tříd. Za žáky 9. tříd rovněž zaplatili někdy dědeček nebo babička (téměř 8 %), kamarád (téměř 8 %) a někdo jiný (téměř 4 %). Za žáky 6. tříd zaplatili také dědeček a babička (téměř 10 %), kamarád (4 %) a někdo jiný (6 %).

Položka č. 15



Graf č. 21 *– relativní četnost odpovědí na položku č. 15 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–8 v grafu č. 21:

1	Neověřuji.
2	Nevím jak a kde bych měl/a.
3	Ano, hledám a čtu si jeho hodnocení.
4	Ano, hledám o něm informace na internetu.

5	Ano, čtu si obchodní podmínky.
6	Ano, předem telefonuji na kontakt.
7	Ano, hledám jak dlouho e-shop existuje.
8	Nenakupuji v e-shopech.

78 % žáků 9. tříd v této položce uvedlo, že nakoupilo v e-shopu, stejně jako 45 % žáků 6. tříd. Zajímavé srovnání se nabízí s položkou č. 10, kde 71 % žáků 9. tříd uvedlo, že někdy v internetovém obchodě nakupovalo (rozdíl 7 %), stejně jako téměř 51 % žáků 6. tříd (rozdíl 6 %). Rozdíl odpovědí mezi položkou č. 10 a č. 15 může být způsoben tím, že někteří žáci, kteří v předchozí položce uvedli, že nenakupovali v e-shopu, dále v položce č. 15 uváděli, že si e-shop neověřují, místo aby odpověděli, že nenakupovali. Tato položka tedy žáky mohla být pojata i tak, že si e-shop neověřují, protože nenakupují. Přesto odpovědi žáků poskytují určitá zjištění a námět k případnému dalšímu zkoumání.

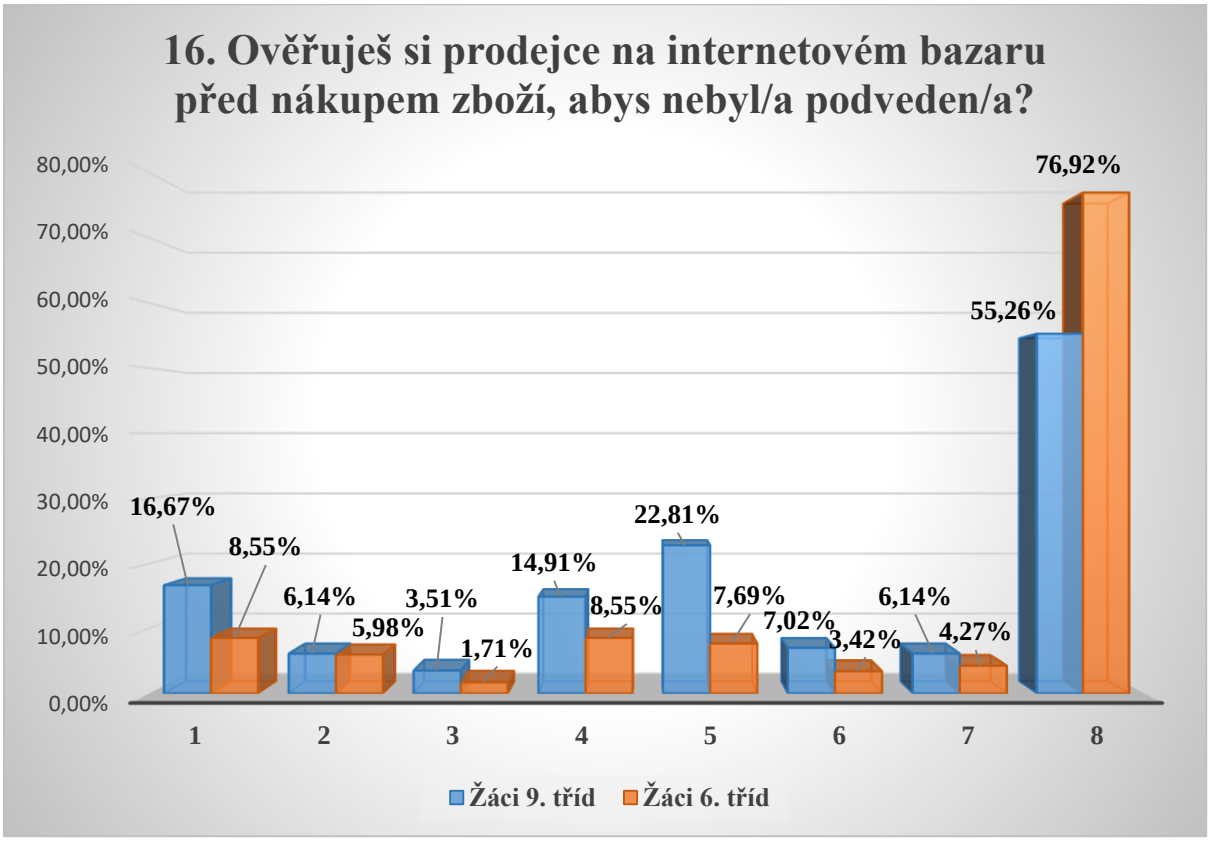
Při dotazování, zda si žáci ověřují e-shop před nákupem, aby nebyli podvedeni, žáci 9. tříd uváděli, že si o něm hledají hodnocení (47 %), informace (25 %), pročítají si obchodní

podmínky (téměř 23 %), **hledají dobu existence e-shopu (téměř 8 %),** předem telefonují na kontakt (6 %). 18 % žáků 9. tříd si e-shopy nijak neověřuje a 14 % ani neví jak a kde.

Při dotazování, zda si žáci ověřují e-shop před nákupem, aby nebyli podvedeni, žáci 6. tříd uváděli, že si o něm hledají hodnocení (20 %), informace (13 %), pročítají si obchodní podmínky (téměř 11 %), hledají dobu existence e-shopu (téměř 4 %), předem telefonují na kontakt (téměř 2 %). 10% žáků 6. tříd si e-shopy nijak neověřuje a 10 % ani neví jak a kde.

Zjištěným výsledkem z této položky byla splněna část dílčího cíle diplomové práce „*Jak si ověřují vybraní žáci 6. a 9. tříd základních škol v Prostějově prodávající subjekt před internetovým nakupováním jako ochranu před podvodným jednáním?“*

Položka č. 16



Graf č. 22 *– relativní četnost odpovědí na položku č. 16 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–8 v grafu č. 22:

1	Neověřuji.
2	Nevím jak a kde bych měl/a.
3	Neověřuji, komunikuji jen přes email.
4	Ano, prohlížím si i další nabídky prodejce.

5	Ano, hledám a čtu si hodnocení prodejce.
6	Ano, dotazuji se na možnost osobního převzetí.
7	Ano, telefonuji na kontakt, vyptávám se na zboží.
8	Nenakupuji v internetových bazarech.

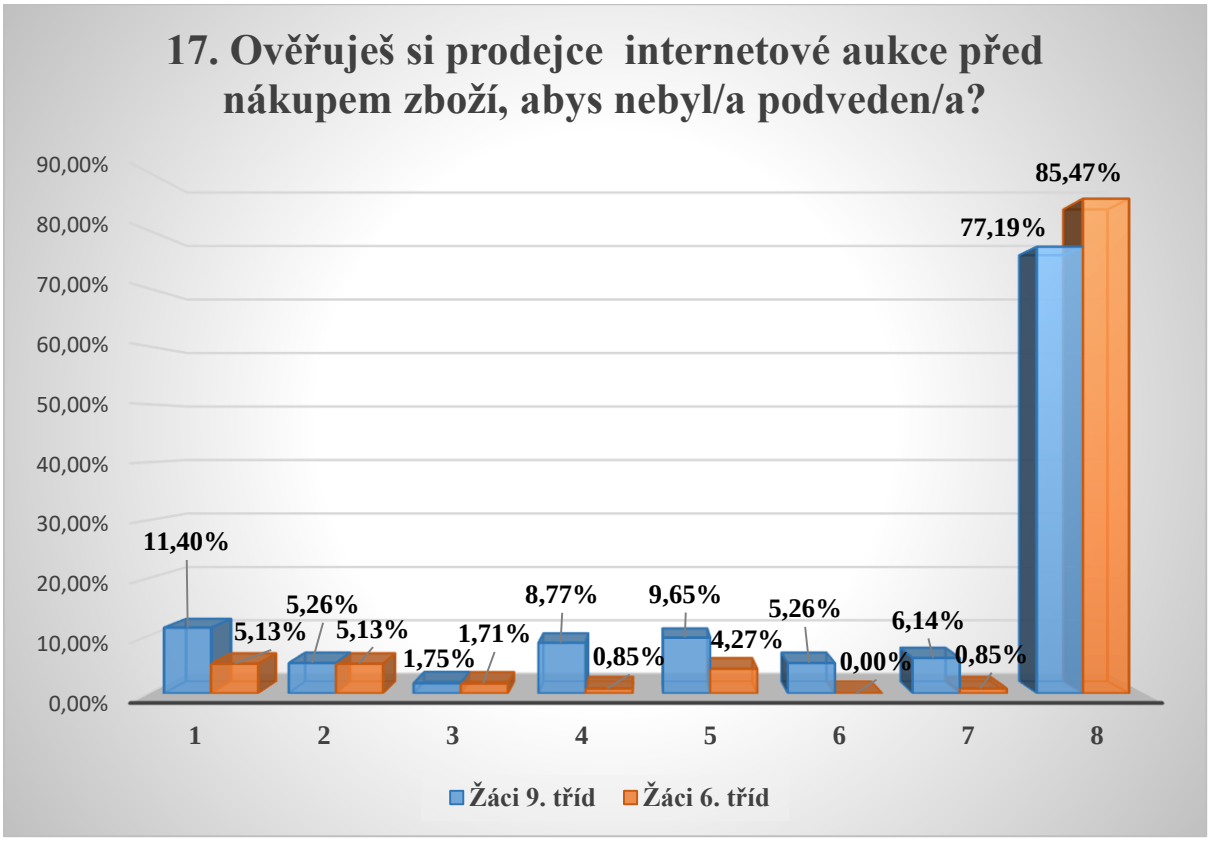
Téměř 45 % žáků 9. tříd v této položce uvedlo, že nakupovalo někdy v bazaru, stejně jako 23 % žáků 6. tříd. Zajímavé srovnání se nabízí s položkou č. 9, kde 35 % žáků 9. tříd uvedlo, že někdy v internetovém bazaru nakupovalo (rozdíl 10 %), stejně jako téměř 22 % žáků 6. tříd (rozdíl 1 %). Rozdíl odpovědí mezi položkou č. 9 a č. 16 může být způsoben opět tím, že někteří žáci, kteří v předchozí položce uvedli, že nenakupovali v bazaru, dále v položce č. 16 uváděli, že si prodejce bazarového inzerátu neověřují, místo aby odpověděli, že nenakupovali. Je ovšem zajímavé, že žáci 6. tříd odpověděli na stejnou položku totožně, na rozdíl od žáků 9. tříd. Přesto nám odpovědi žáků poskytují určitá zjištění.

Při dotazování, zda si žáci ověřují prodejce internetového bazaru před nákupem, aby nebyli podvedeni, žáci 9. tříd uváděli, že si o něm hledají hodnocení (téměř 23 %), prohlíží si další nabídky prodejce (15 %), dotazují se na možnost osobního převzetí (7 %), telefonují na kontakt (6 %). Téměř 17 % žáků 9. tříd si prodejce v bazaru neověřuje, 6 % neví jak a kde a téměř 4 % z nich jen komunikují přes email.

Při dotazování, zda si žáci ověřují prodejce internetového bazaru před nákupem, aby nebyli podvedeni, žáci 6. tříd uváděli, že si o něm hledají hodnocení (téměř 8 %), prohlíží si další nabídky prodejce (téměř 9 %), dotazují se na možnost osobního převzetí (téměř 4 %), telefonují na kontakt (4 %). Téměř 9 % žáků 6. tříd si prodejce bazaru neověřuje, 6 % neví jak a kde a téměř 2 % z nich jen komunikují přes email.

Zjištěným výsledkem z této položky byla splněna část dílčího cíle diplomové práce „*Jak si ověřují vybraní žáci 6. a 9. tříd základních škol v Prostějově prodávající subjekt před internetovým nakupováním jako ochranu před podvodným jednáním?*“

Položka č. 17



Graf č. 23 *– relativní četnost odpovědí na položku č. 17 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–8 v grafu č. 23:

1	Neověřuji.
2	Nevím jak a kde bych měl/a.
3	Neověřuji, komunikuji jen přes email.
4	Ano, prohlížím si další nabídky prodejce.

5	Ano, hledám a čtu si hodnocení prodejce.
6	Ano, dotazuji se na možnost osobního převzetí.
7	Ano, telefonuji na kontakt, vyptávám se na zboží.
8	Nenakupuji v internetových aukcích.

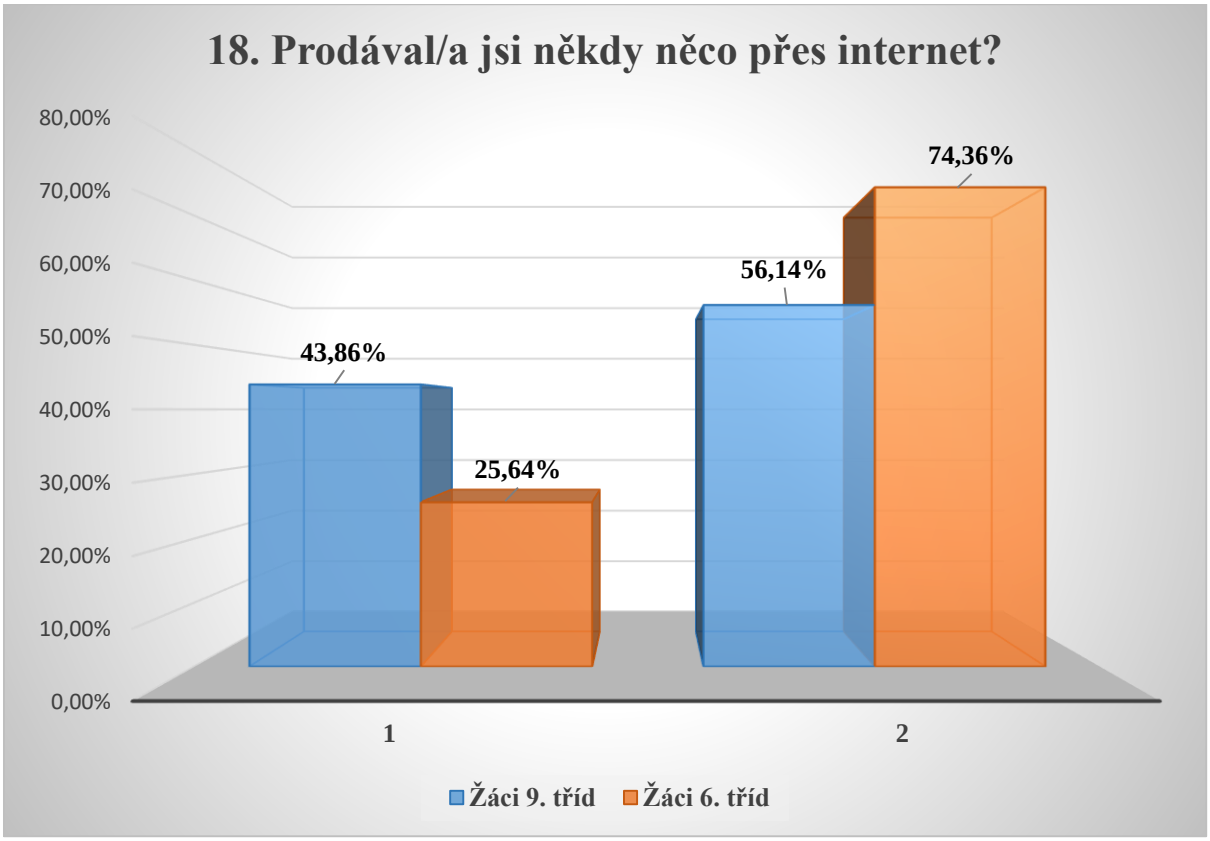
Téměř 23 % žáků 9. tříd v této položce uvedlo, že nakoupilo v aukci, stejně jako téměř 15 % žáků 6. tříd. Zajímavé srovnání se nabízí s položkou č. 8, kde téměř 17 % žáků 9. tříd uvedlo, že někdy v internetové aukci nakupovalo (rozdíl 5%), stejně jako 15% žáků 6. tříd (rozdíl 2%). Rozdíl odpovědí mezi položkou č. 8 a č. 17 může být způsoben opět tím, že někteří žáci, kteří v položce č. 8 uvedli, že nenakupovali nikdy v aukci, dále v položce č. 17 uváděli, že si prodejce aukce neověřují, namísto aby odpověděli, že nenakupovali. Tato položka tedy některými žáky mohla být opět pojata tak, že když nenakupují, ani si prodejce neověřují. Přesto nám odpovědi žáků poskytují určitá zjištění.

Při dotazování, zda si žáci ověřují prodejce internetové aukce před nákupem, aby nebyli podvedeni, žáci 9. tříd uváděli, že si čtou hodnocení prodejce (téměř 10 %), prohlíží si další nabídky prodejce (téměř 9 %), dotazují se na možnost osobního převzetí (5 %), telefonují na kontakt (6 %). 11% žáků 9. tříd uvedlo, že si prodejce aukce neověřuje, 5 % neví jak a kde a téměř 2 % z nich jen komunikují přes email.

Při dotazování, zda si žáci ověřují prodejce internetové aukce před nákupem, aby nebyli podvedeni, žáci 6. tříd uváděli, že si čtou hodnocení prodejce (4 %), prohlíží si další nabídky prodejce (téměř 1 %), telefonují na kontakt (téměř 1 %). 5 % žáků 6. tříd uvedlo, že si prodejce aukce neověřuje, 5 % neví jak a kde a téměř 2 % z nich jen komunikují přes email.

Zjištěným výsledkem z této položky byla splněna část dílčího cíle diplomové práce „*Jak si ověřují vybraní žáci 6. a 9. tříd základních škol v Prostějově prodávající subjekt před internetovým nakupováním jako ochranu před podvodným jednáním?“*

Položka č. 18



Graf č. 24 *– relativní četnost odpovědí na položku č. 18 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–2 v grafu č. 24:

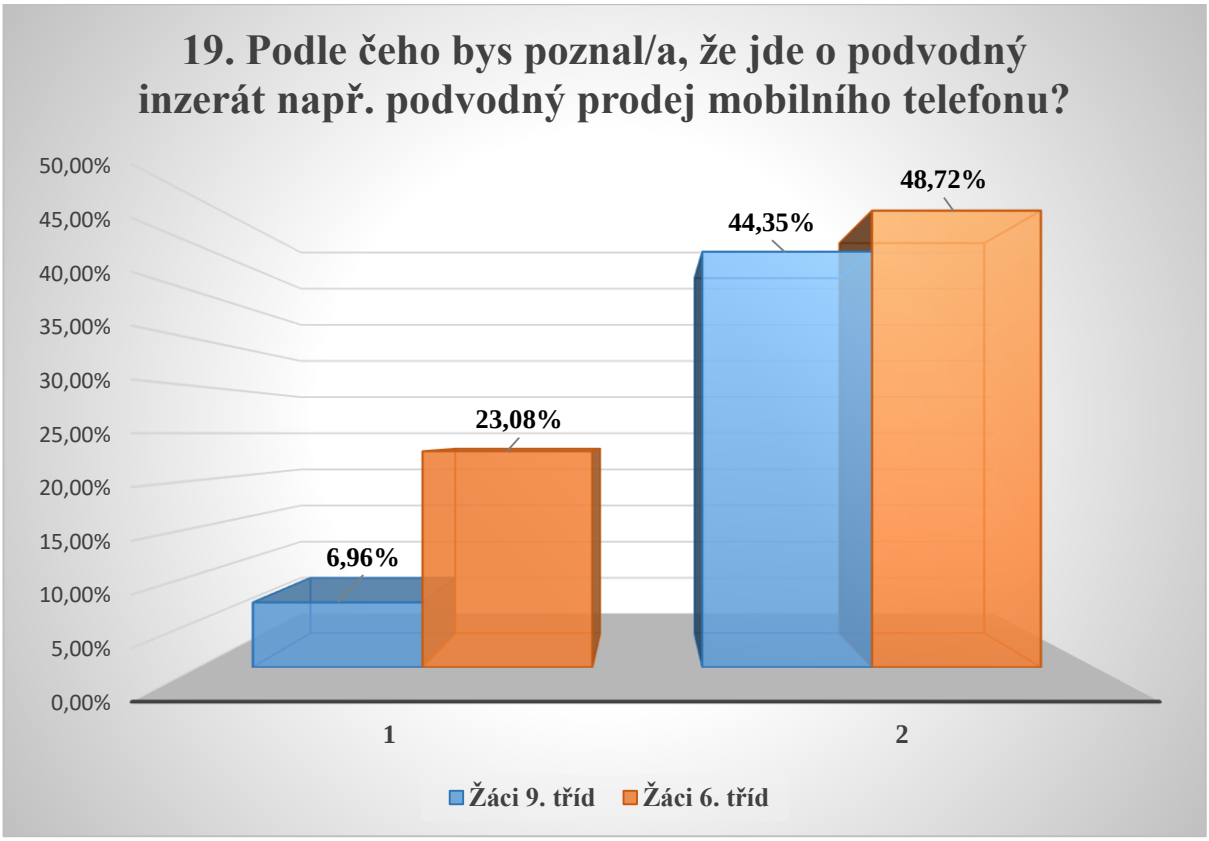
1	Ano	**2**	Ne

Tato položka zjišťovala, jakou zkušenost mají žáci s prodejem zboží na internetu. Pokud žáci něco přes internet prodávají, lze vyvodit, že se v prostředí internetové inzerce pohybují.

Téměř 44 % žáků 9. tříd uvedlo, že někdy přes internet něco prodávalo, stejně jako téměř 26 % žáků 6. tříd.

Zjištěným výsledkem z této položky byl tak splněn dílčí cíl diplomové práce „*Jaké mají vybraní žáci 6. a 9. tříd základních škol v Prostějově zkušenosti s prodejem prostřednictvím internetu*?“

Položka č. 19



***Graf č. 25**– relativní četnost odpovědí na položku č. 19a v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–2 v grafu č. 25:

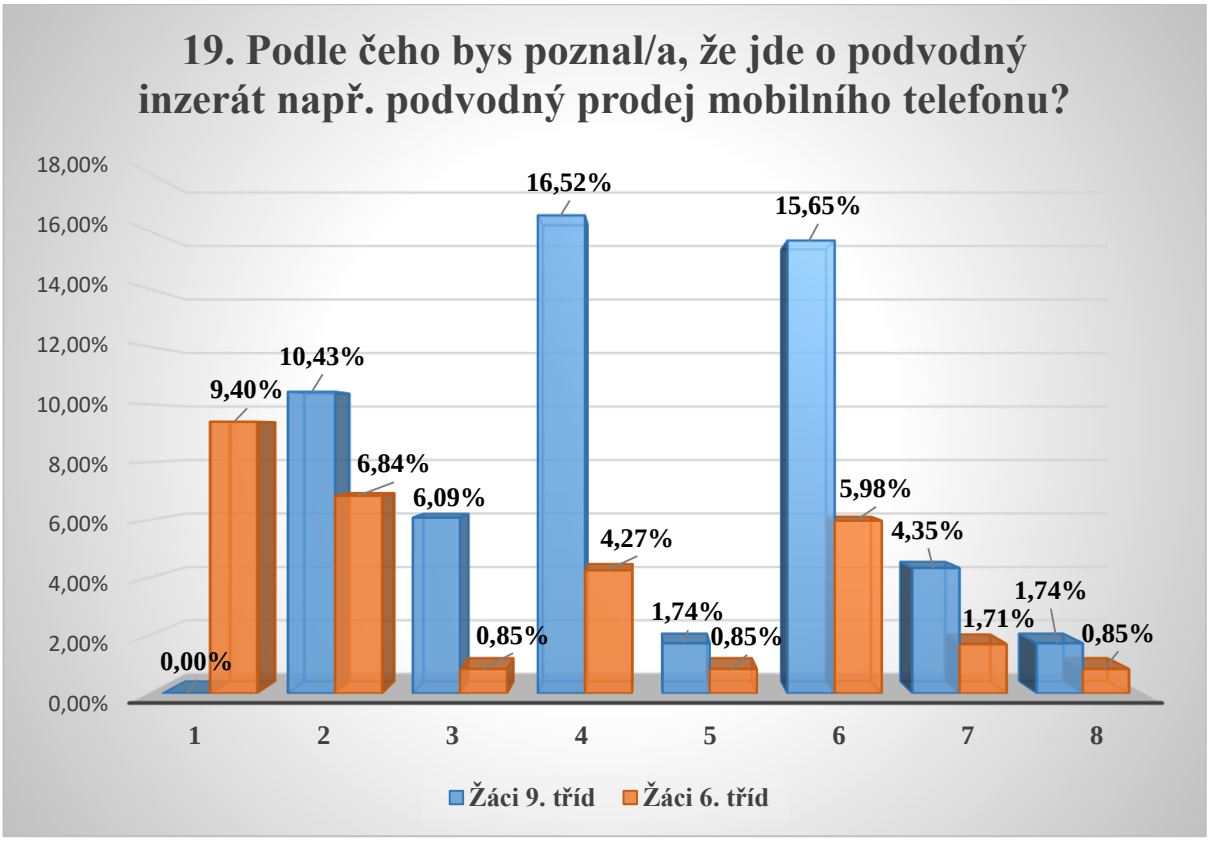
1	Žáci, kteří uvedli přímo, že neví.

2	Žáci, kteří neodpověděli.

Touto položkou bylo mezi žáky zjišťováno, podle čeho by poznali, že jde o podvodný inzerát na internetu. U zadání této položky byla poznámka, že pokud žáci vědí odpověď, nechť ji uvedou. Pokud bychom považovali, že odpověď přímo „*nevím*“ je totožná se žádnou odpovědí, za tohoto předpokladu lze připustit, že **51 % žáků 9. tříd neví, podle čeho by poznalo podvodný inzerát, stejně jako téměř 72 % žáků 6. tříd**. Od 49 % žáků 9. tříd byla tedy získána kladná odpověď, stejně jako od 28 % žáků 6. tříd.

Jaké odpovědi žáci odpovídali, jsou uvedeny v následujícím grafu.

Položka č. 19



***Graf č. 26**– relativní četnost odpovědí na položku č. 19b v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–8 v grafu č. 26:

1	Žáci odpověděli chybnou odpověď (např. velmi vysoká cena, starý inzerát, zboží nabízeno zdarma).
2	V inzerátu by bylo málo údajů k prodejci, chybějící kontakt, nebo k nabízenému zboží.
3	Podaný inzerát by měl gramatické chyby v textu, strojová čeština.
4	Nízká cena, velmi výhodná koupě

5	Popis nabízeného zboží v inzerátu by neodpovídal popisu existujícího zboží.
6	Fotografie by byla stažená z internetu, inzerát by měl málo fotografií nebo by byl bez fotografie zboží.
7	Prodejce by vyžadoval zaplatit platbu pouze předem na účet.
8	Nefunkční tel. kontakt prodejce.

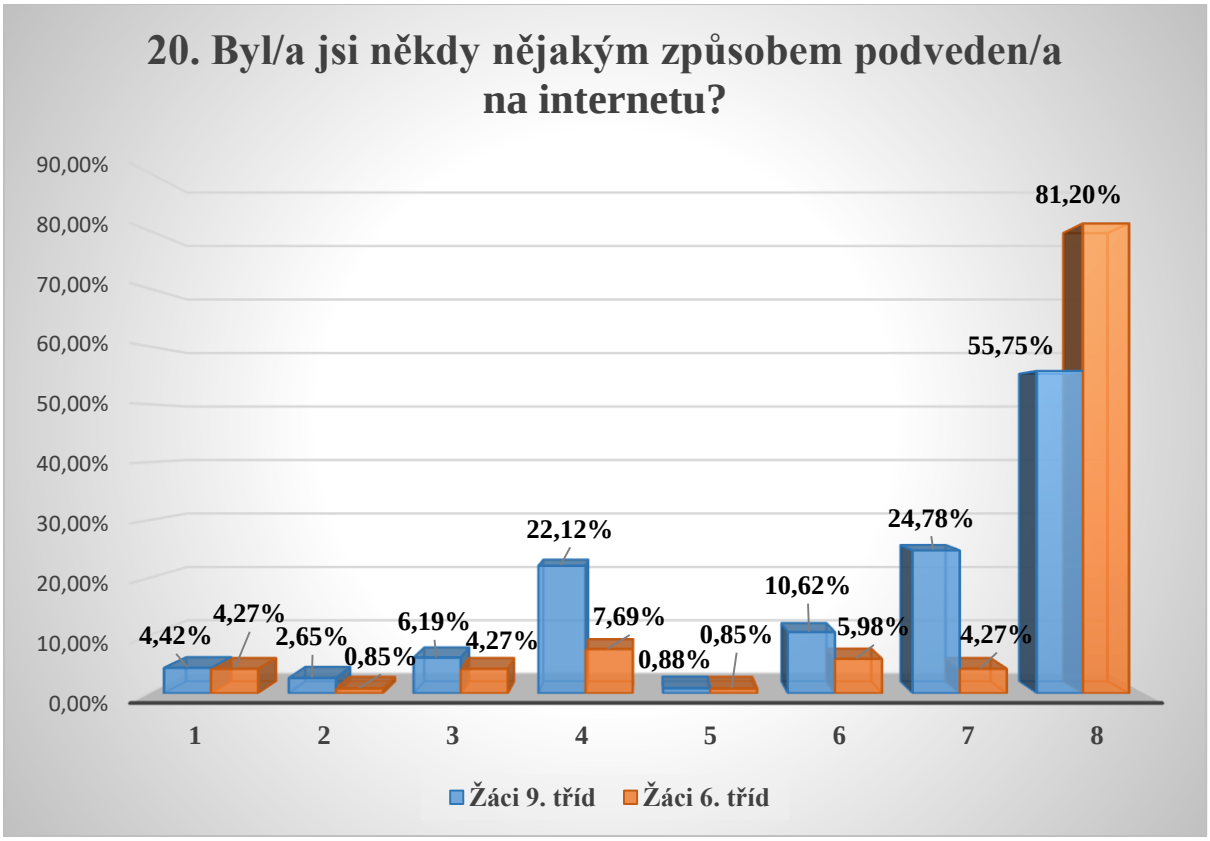
Žáci 9. tříd uváděli, že podvodný inzerát by poznali podle velmi nízké ceny (téměř 17 %), podle fotografií stažených z internetu nebo málo fotografií (téměř 16 %), podle chybějících údajů ke zboží či prodejci, např. kontakt (10 %), podle gramatických chyb nebo strojové češtiny (6 %), podle požadavku pouze platby předem na účet (4 %), podle chybného popisu zboží v inzerátu (téměř 2 %) a podle nefunkčního tel. kontaktu (téměř 2 %).

Žáci 6. tříd uváděli, že podvodný inzerát by poznali podle velmi nízké ceny (4 %), podle fotografií stažených z internetu nebo málo fotografií (6 %), podle chybějících údajů ke zboží či prodejci, např. kontakt, (téměř 7 %), podle gramatických chyb nebo strojové češtiny (téměř

1 %), podle požadavku pouze platby předem na účet (téměř 2 %), podle chybného popisu zboží v inzerátu (téměř 1 %) a podle nefunkčního tel. kontaktu (téměř 1 %). 9 % žáků 6. tříd navíc odpovědělo chybnou odpověď, např. že zboží by bylo nabízeno za velmi vysokou cenu, inzerát by byl hodně starý, zboží by bylo nabízeno zdarma.

Zjištěným výsledkem z této položky byl tak splněn dílčí cíl diplomové práce „*Jak by vybraní žáci 6. a 9. tříd základních škol v Prostějově poznali podvodnou nabídku zboží na internetu?*“

Položka č. 20



Graf č. 27 *– relativní četnost odpovědí na položku č. 20 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–8 v grafu č. 27:

1	Ano, přišel/a jsem o peníze nebo jiný majetek (vznikla mi majetková škoda).
2	Ano, ale někdo jiný díky mě přišel o peníze (např. rodiče, dědeček, babička, kamarád).
3	Ano, někdo mě podvedl a klikl/a jsem na zavirovaný odkaz, obrázek, stránku, apod.
4	Přišla mi podvodná zpráva nebo email.

5	Ano, přišel/přišla jsem o své osobní údaje, heslo, fotky, videa, apod.
6	Ano, někdo se mi naboural do facebookového, herního, bankovního či jiného účtu nebo emailu.
7	Ano, psal mi někdo z falešného profilu na Facebooku.
8	Ne.

Položka č. 20 zjišťovala, zda byli žáci některým vybraným způsobem podvedeni v IT prostředí a pokud ano, jakým vybraným způsobem konkrétně.

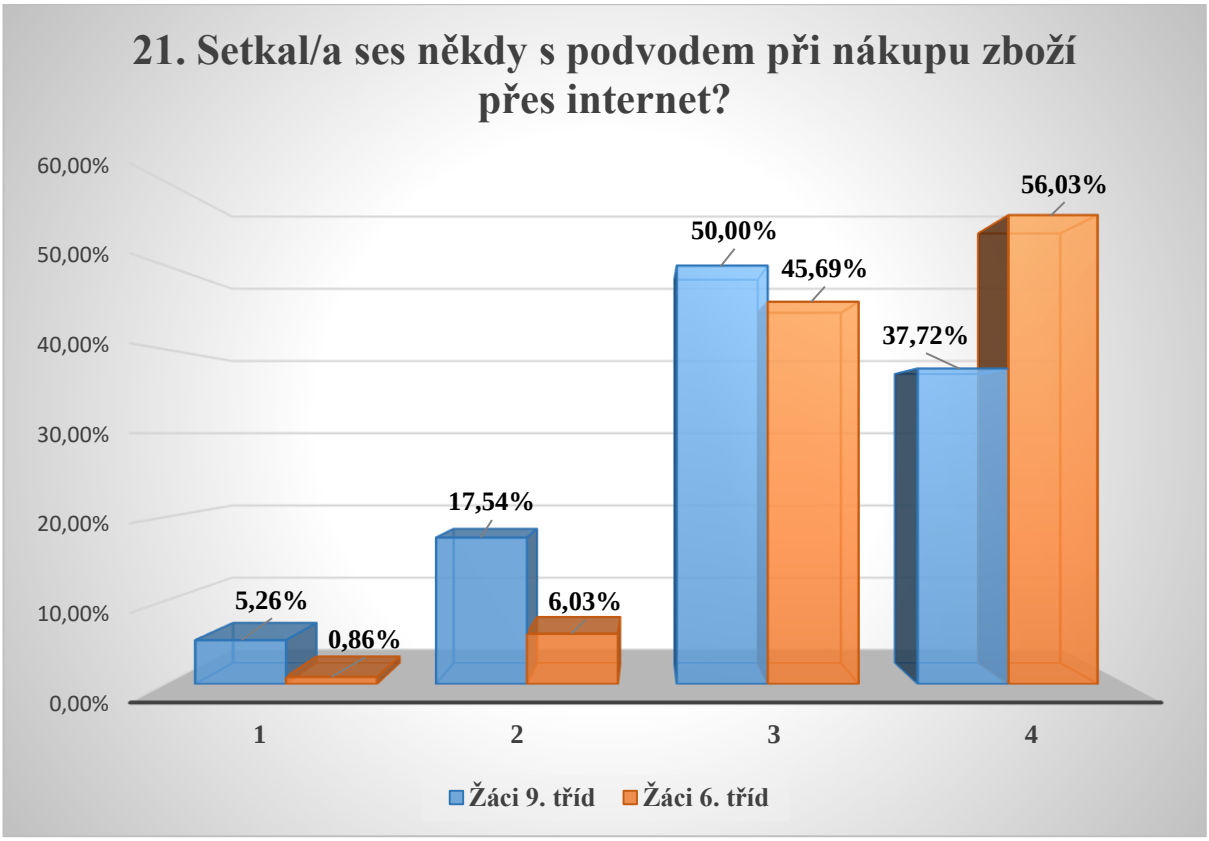
44 % žáků 9. tříd uvedlo, že bylo někdy nějakým způsobem na internetu podvedeno, stejně jako téměř 19 % žáků 6. tříd.

Žáci 9. tříd uváděli, že jim někdo psal z falešného facebookového účtu (téměř 25 %), přišla jim podvodná zpráva (22 %), někdo se jim „*naboural*“ do nějakého účtu (téměř 11 %), někdo je podvedl a klikli na zavirovaný odkaz (6 %), vlivem podvodu jim vznikla majetková škoda (4 %), někomu jinému jejich vlivem vznikla majetková škoda (téměř 3 %), přišli o osobní údaje či fotografie (téměř 1 %).

Žáci 6. tříd uváděli, že jim přišla podvodná zpráva (téměř 8 %), někdo se jim „*naboural*“ do nějakého účtu (6 %), někdo je podvedl a klikli na zavirovaný odkaz (4 %), vlivem podvodu jim vznikla majetková škoda (4 %), někdo jim psal z falešného facebookového účtu (4 %), někomu jinému jejich vlivem vznikla majetková škoda (téměř 1 %), přišli o osobní údaje či fotografie (téměř 1 %).

Zjištěným výsledkem z této položky byla splněna část dílčího cíle diplomové práce „*Jaký je rozdíl v četnosti cílených útoků pachatele vybraného podvodného jednání v IT prostředí na žáky 6. a 9. tříd na základních školách v Prostějově?*“

Položka č. 21



Graf č. 28 *– relativní četnost odpovědí na položku č. 21 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–4 v grafu č. 28:

1	Ano, byl/a jsem podveden/a přímo já.
2	Ano, podvedli někoho z mého okolí (rodina, kamarád, známý, apod.).

3	Vím, že takové podvody existují.
4	Ne, nesetkal/a jsem se s takovým podvodem.

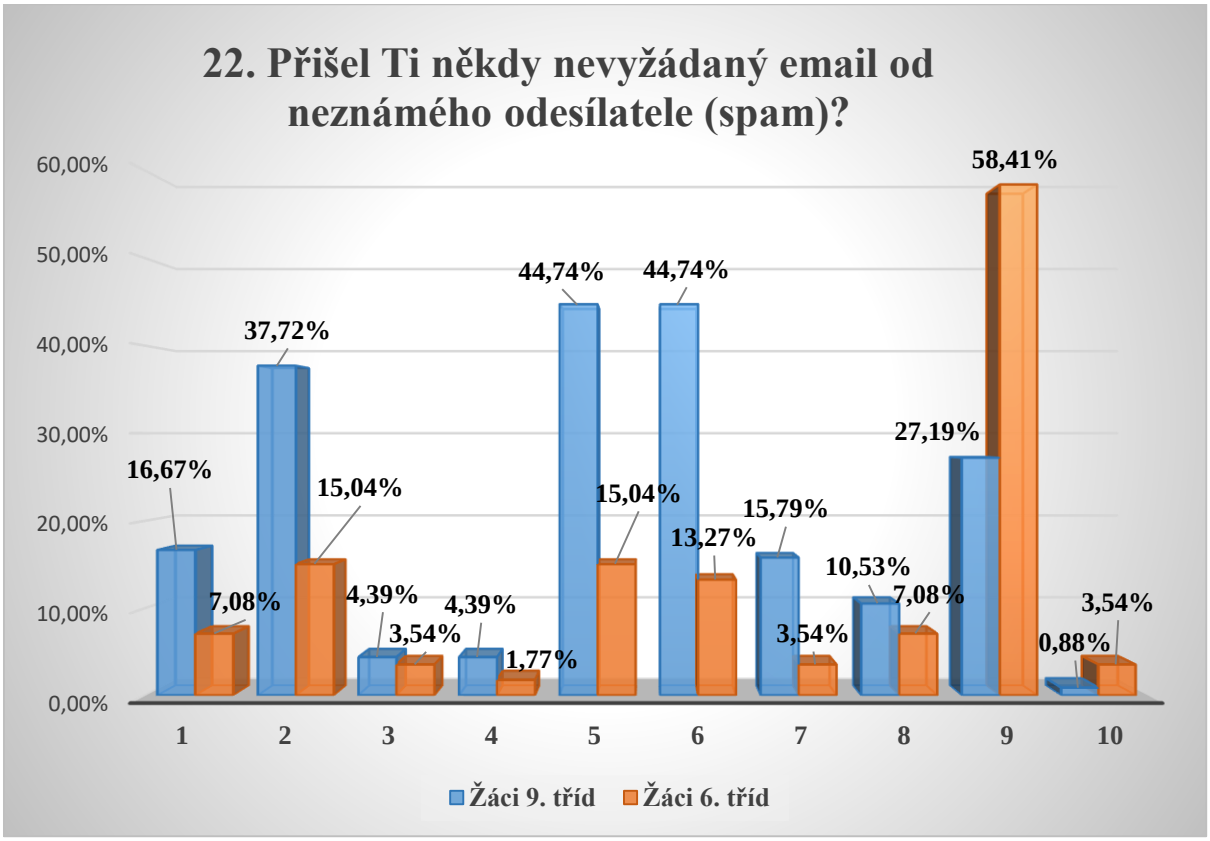
Položka č. 21 se zaměřovala přímo na to, zda se žáci setkali s internetovým podvodem při nákupu zboží.

Žáci 9. tříd uvedli, že byli podvedeni přímo oni (5 %), dále že znají někoho, kdo byl podveden z jejich okolí tímto způsobem (téměř 18 %), mají povědomí, že takové podvody existují (50 %) a nikdy se s takovým podvodem nesetkalo téměř 38 % žáků 9. tříd.

Žáci 6. tříd uvedli, že byli podvedeni přímo oni (téměř 1 %), dále že znají někoho, kdo byl podveden z jejich okolí takovým způsobem (6 %), mají povědomí, že takové podvody existují (téměř 46 %) a nikdy se s takovým podvodem nesetkalo 56 % žáků 6. tříd.

Zjištěným výsledkem z této položky byla splněna část dílčího cíle diplomové práce *„Jaký je rozdíl v četnosti cílených útoků pachatele vybraného podvodného jednání v IT prostředí na žáky 6. a 9. tříd na základních školách v Prostějově?“*

Položka č. 22



Graf č. 29 *– relativní četnost odpovědí na položku č. 22 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–10 v grafu č. 29:

1	Ano, někdo se chtěl semnou seznámit.
2	Ano, přišla zpráva, že jsem něco vyhrál/a.
3	Ano, přišla podvodná výzva, že dlužím peníze.
4	Ano, přišla mi podvodná faktura k zaplacení.
5	Ano, přišla mi nabídka zboží nebo reklama.

6	Ano, přišel/a, ale neotvíral/a jsem ho.
7	Ano, někdo mi nabízel, že si můžu vydělat peníze.
8	Ano, přišel, ale týkal se něčeho jiného.
9	Ne, nepřišel.
10	Nemám email.

Položka č. 22 od žáků přímo zjišťovala, zda jim byla někdy doručena nevyžádaná zpráva (spam nebo scam) a pokud ano, tak jaká.

Téměř 72 % žáků 9. tříd uvedlo, že jim byla doručena nevyžádaná zpráva (spam nebo scam), stejně jako 38 % žákům 6. tříd. Téměř 45 % žáků 9. třídy takovou zprávu vůbec neotvíralo, stejně jako 13 % žáků 6. tříd.

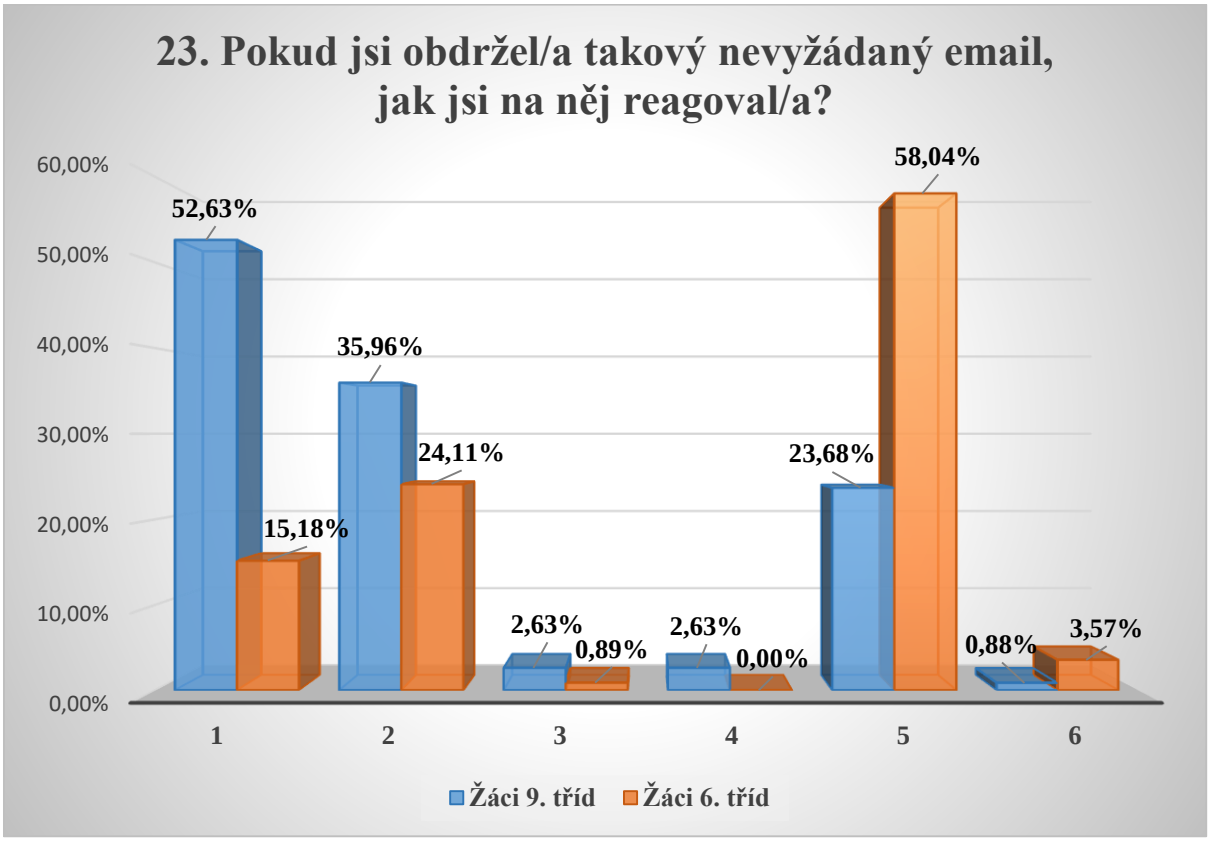
Nejčastěji byla žákům 9. tříd doručena nevyžádaná zpráva týkající se reklamy nebo nabídky zboží (téměř 45 %), podvodná zpráva že něco vyhráli (téměř 38 %), někdo se s nimi chtěl seznámit (téměř 17 %), někdo jim nabízel výdělek peněz (téměř 16 %), týkala se něčeho

jiného (téměř 11 %), přišla jim podvodná výzva k úhradě dluhu (4 %), podvodná faktura k zaplacení (4 %).

Nejčastěji byla žákům 6. tříd doručena nevyžádaná zpráva týkající se reklamy nebo nabídky zboží (15 %), podvodná zpráva že něco vyhráli (téměř 15 %), někdo se s nimi chtěl seznámit (7 %), někdo jim nabízel výdělek peněz (téměř 4 %), týkala se něčeho jiného (7 %), přišla jim podvodná výzva k úhradě dluhu (téměř 4 %), podvodná faktura k zaplacení (téměř 2 %).

Zjištěným výsledkem z této položky byla splněna část dílčího cíle diplomové práce *„Jaký je rozdíl v četnosti cílených útoků pachatele vybraného podvodného jednání v IT prostředí na žáky 6. a 9. tříd na základních školách v Prostějově?“*

Položka č. 23



Graf č. 30 *– relativní četnost odpovědí na položku č. 23 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–6 v grafu č. 30:

1	Nečetl/a jsem ho a vymazal/a.
2	Přečetl/a jsem ho a vymazal/a.
3	Přečetl/a jsem ho a odepsal/a.

4	Přečetl/a jsem ho a klikl/a na přílohu nebo odkaz v této zprávě.
5	Nepřišel mi žádný takový email.
6	Nemám email.

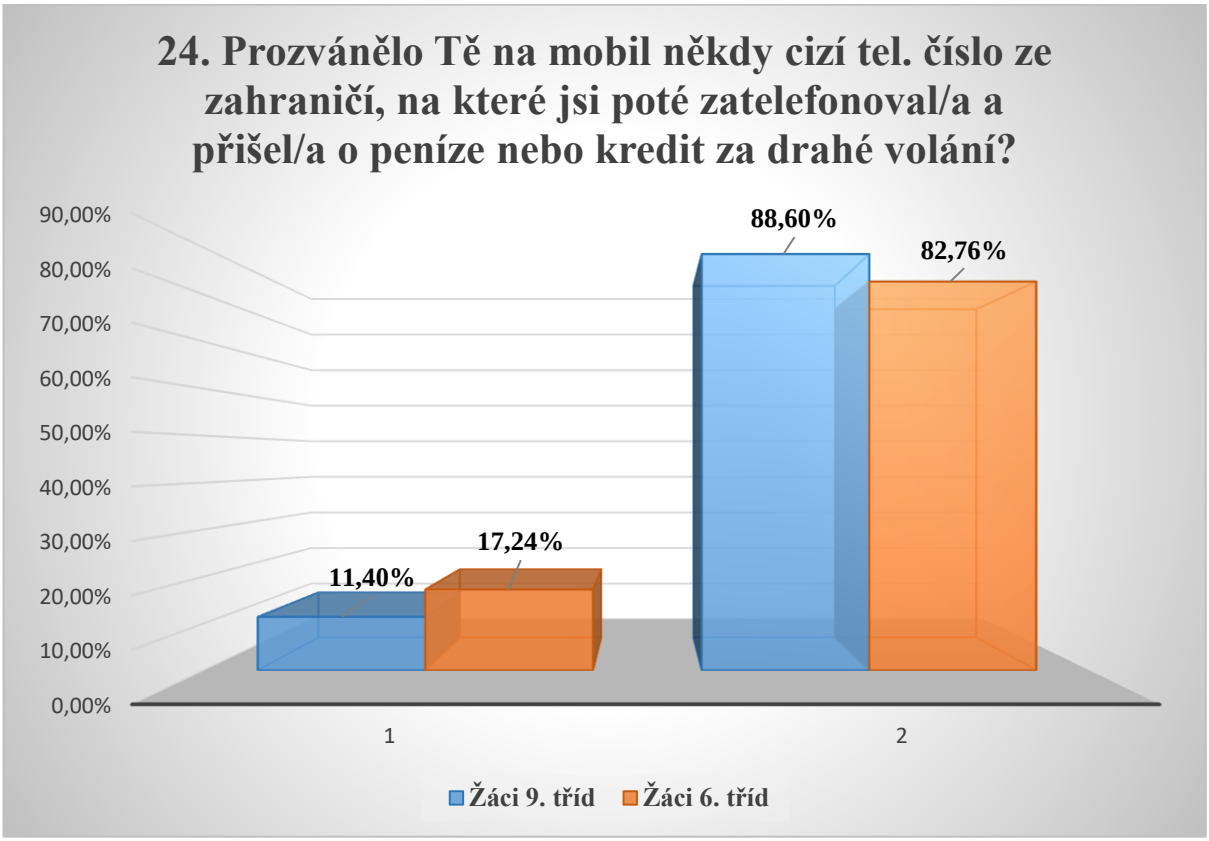
Položka č. 23 zjišťovala, jak žáci na nevyžádanou zprávu reagovali.

Téměř 76 % žáků 9. tříd v této položce uvedlo, že jim byla doručena nevyžádaná zpráva (spam nebo scam), stejně jako 38 % žákům 6. tříd. Po srovnání s předcházející položkou (č. 22) byl zaznamenán rozdíl na stejnou odpověď, a to u žáků 9. tříd, kteří původně uváděli doručení takové zprávy v 72 %, což činí rozdíl 4 %.

Žáci 9. tříd uvedli, že takový email vůbec nečetli a rovnou jej vymazali (téměř 53 %), přečetli a vymazali (36 %), přečetli a odepsali (téměř 3 %) nebo přečetli a klikli na přiložený odkaz (téměř 3 %).

Žáci 6. tříd uvedli, že takový email vůbec nečetli a rovnou jej vymazali (15 %), přečetli a vymazali (24 %), přečetli a odepsali (téměř 1 %), přičemž uváděli, že nikdy na přiložený odkaz v takové zprávě neklikali.

Položka č. 24



Graf č. 31 *– relativní četnost odpovědí na položku č. 24 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–2 v grafu č. 31:

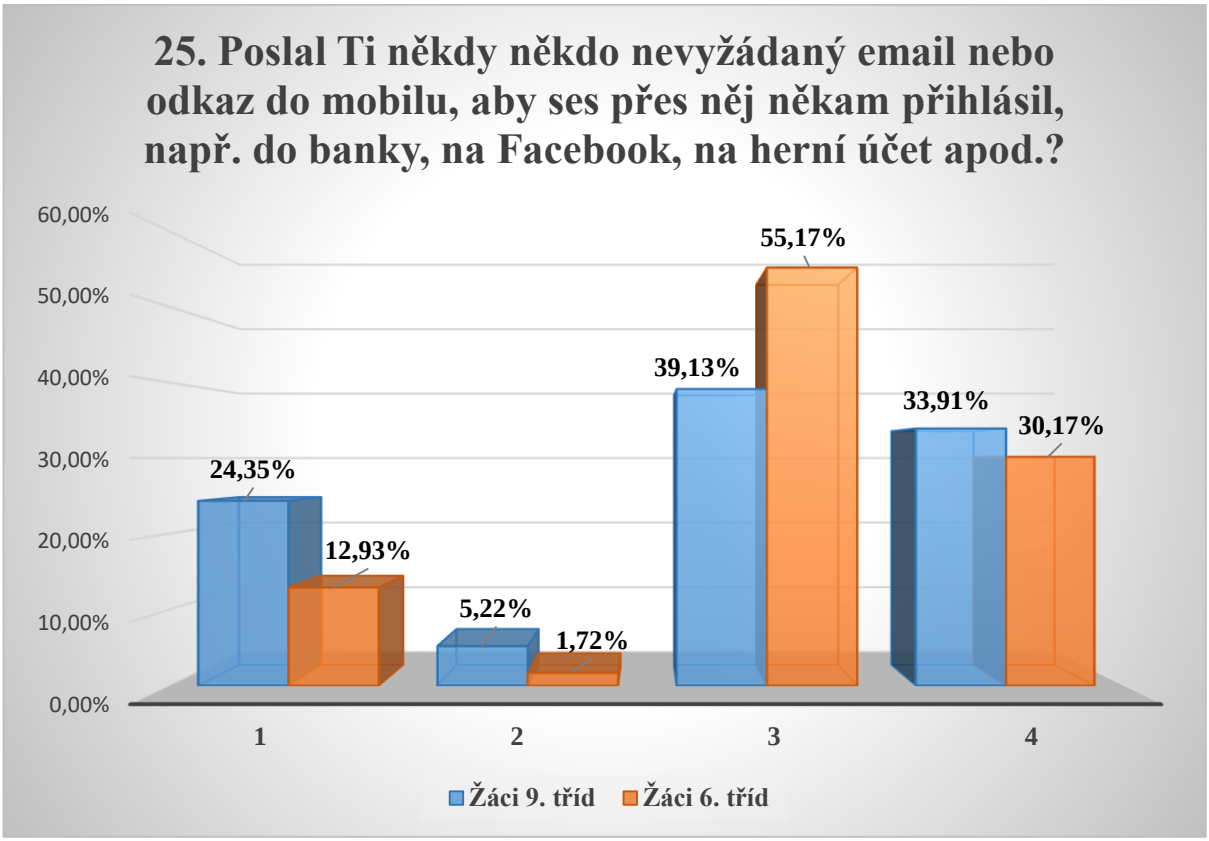
1	Ano	**2**	Ne

Položka č. 24 se pokoušela zjistit, zda se žáci někdy setkali s podvodnou formou. wangiri.

11 % žáků 9. tříd uvedlo, že se setkalo s prozváněním ze zahraničí, přičemž přišli o peníze nebo kredit, stejně jako 17 % žáků 6. tříd.

Zjištěným výsledkem z této položky byla splněna část dílčího cíle diplomové práce *„Jaký je rozdíl v četnosti cílených útoků pachatele vybraného podvodného jednání v IT prostředí na žáky 6. a 9. tříd na základních školách v Prostějově?“*

Položka č. 25



Graf č. 32 *– relativní četnost odpovědí na položku č. 25 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–4 v grafu č. 32:

1	Ano, ale nepřihlásil/a jsem se přes odkaz.
2	Ano, přihlásil/a jsem se přes odkaz.

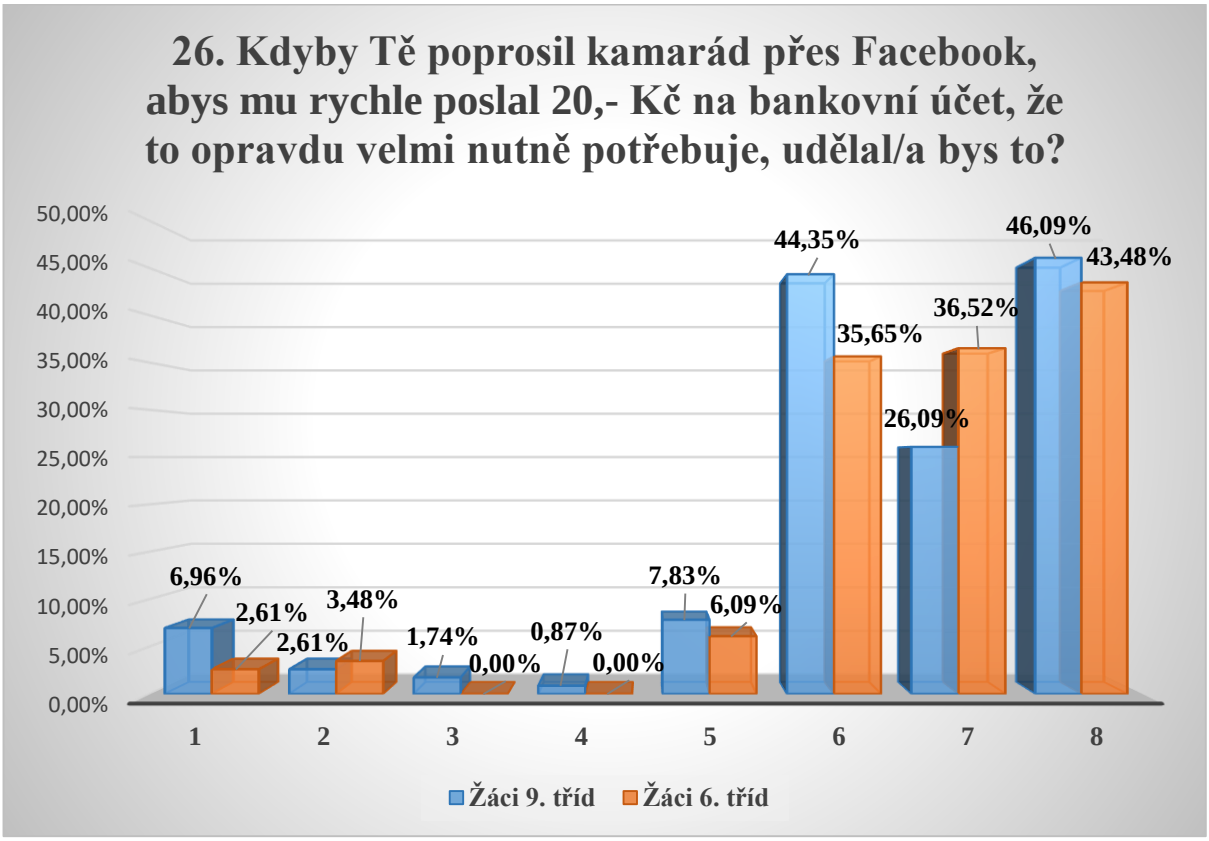
3	Ne, nic takového mi nepřišlo.
4	Nevím. Nejsem si vědom/a.

Nevyžádaná zpráva spolu s odkazem k přihlášení do bankovního účtu, herního účtu nebo účtu na sociální síti bývá mnohdy prostředkem k podvodu v IT prostředí (phishing).

27 % žáků 9. tříd stejně jako 15 % žáků 6. tříd uvedlo, že jim byla doručena taková nevyžádaná zpráva s odkazem na přihlášení.

24 % žáků 9. tříd, stejně jako 13 % žáků 6. tříd uvedlo, že jim taková nevyžádaná zpráva s odkazem k přihlášení byla někdy zaslána, přičemž přes odkaz se nepřihlásili. 5 % žáků 9. tříd, stejně jako téměř 2 % žáků 6. tříd uvedlo, že jim taková zpráva přišla a přes nabízený odkaz se přihlásili.

Položka č. 26



Graf č. 33 *– relativní četnost odpovědí na položku č. 26 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–8 v grafu č. 33:

1	Poslal/a bych mu to já sám/a ze svého bankovního účtu nebo platební karty.
2	Poprosil/a bych rodiče o platební kartu a poslal/a bych mu to já sám/a.
3	Poprosil/a bych dědečka/babičku o platební kartu a poslal/a bych mu to já sám/a.
4	Poprosil/a bych kamaráda nebo někoho jiného o platební kartu a poslal/a bych mu to já sám/a.

5	Poprosil/a bych rodiče nebo někoho jiného, aby mu to oni sami poslali.
6	Nejdřív bych si ověřil/a, jestli mi napsal skutečně můj kamarád.
7	Nereagoval/a bych vůbec na to.
8	Odmítl/a bych mu to poslat.

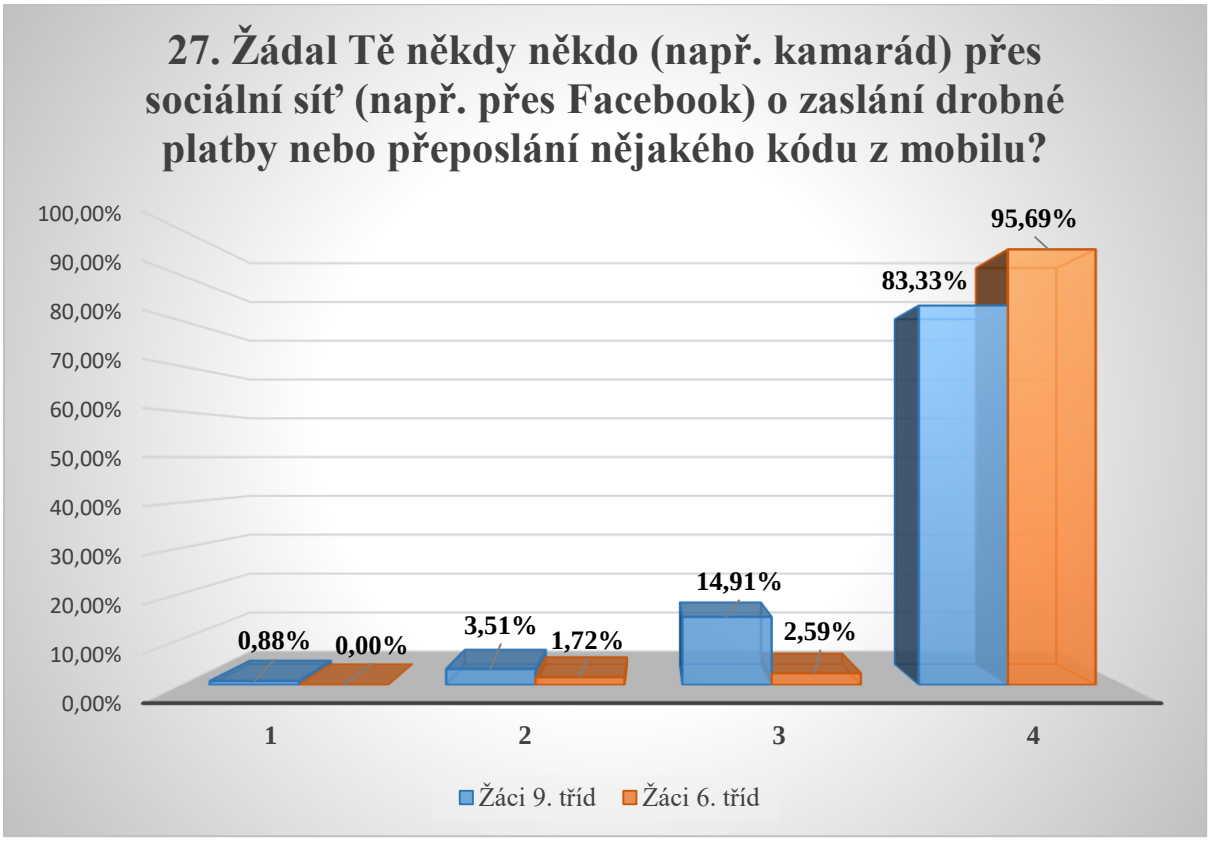
Položka č. 26 se pokoušela mimo stanovené konkrétní dílčí cíle zjistit, zda znají žáci riziko podvodu, respektive jak by žáci reagovali, pokud by je kamarád v IT prostředí oslovil o zaslání drobné platby. Položka byla imitací podvodné formy phishing.

44 % žáků 9. tříd uvedlo, že by si nejdřív ověřilo, zda je oslovil skutečně kamarád s požadavkem o zaslání platby, stejně jako téměř 36 % žáků 6. tříd.

Žáci 9. tříd dále uváděli, že by na takovou zprávu vůbec nereagovali (26 %), odmítli by to poslat (46 %), poprosili by rodiče, nebo někoho jiného, aby to poslali (téměř 8 %), poslali by to sami ze svého bankovního účtu (téměř 7 %), poprosili by rodiče o platební kartu a poslali by mu to sami (téměř 3 %), poprosili by dědečka nebo babičku o platební kartu a poslali by mu to sami (téměř 2 %), poprosili by kamaráda nebo někoho jiného o platební kartu a poslali by mu to sami (téměř 1 %).

Žáci 6. tříd uváděli, že by na takovou zprávu vůbec nereagovali (téměř 37 %), odmítli by to poslat (43 %), poprosili by rodiče nebo někoho jiného, aby to poslali (6 %), poslali by to sami ze svého bankovního účtu (téměř 3 %), poprosili by rodiče o platební kartu a poslali by mu to sami (téměř 4 %).

Položka č. 27



Graf č. 34 *– relativní četnost odpovědí na položku č. 27 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–4 v grafu č. 34:

1	Ano, byl to podvod, přišel/přišla jsem o peníze.
2	Ano, byl to podvod, ale nereagoval/a jsem na to.

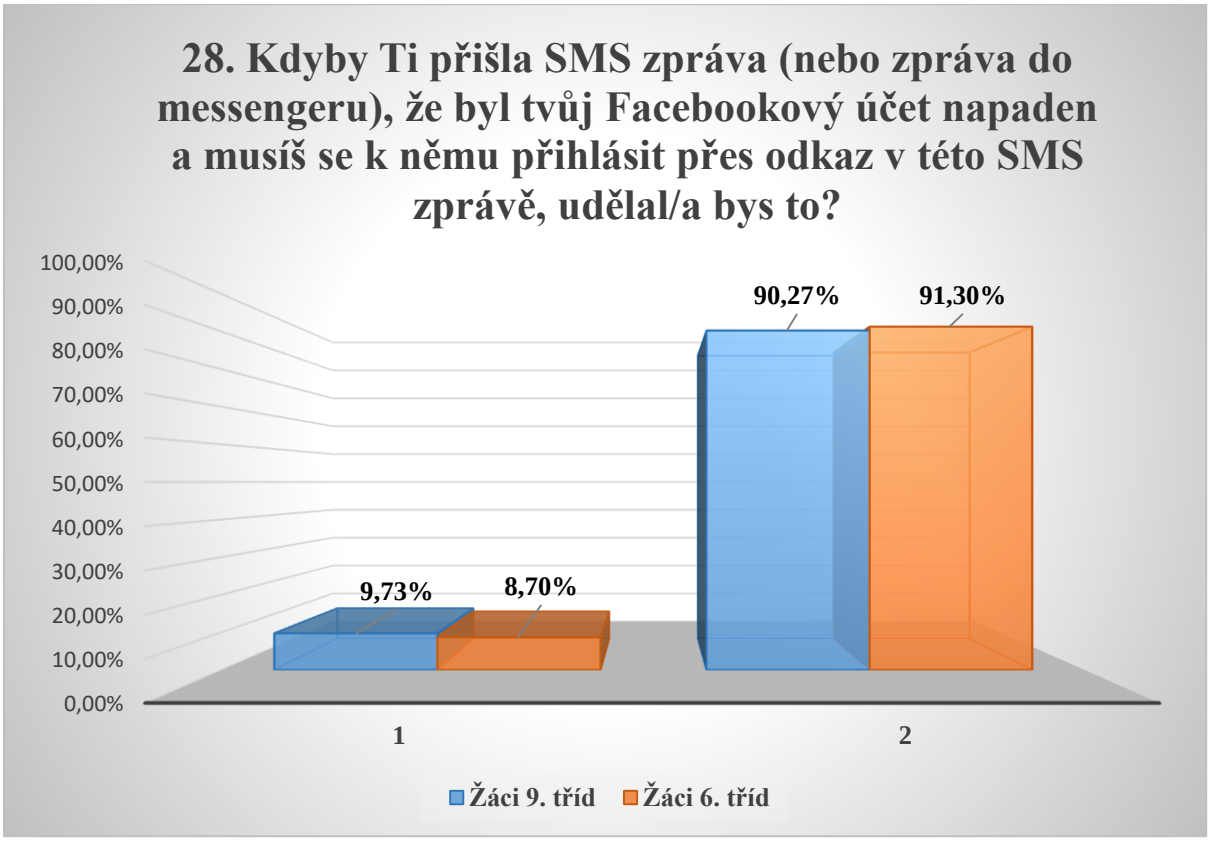
3	Ano, ale podvod to nebyl.
4	Nikdo to po mně nikdy nechtěl.

Položka č. 27 se pokoušela mimo stanovené dílčí cíle zjistit, jakou mají zkušenost žáci se žádostí o zaslání drobné platby (možný phishing) nebo přeposlání platebního kódu (možná podvodná mobilní platba) na sociální síti.

Téměř 17 % žáků 9. tříd se s takovým požadavkem setkalo, přičemž žáci 9. tříd dále odpověděli, že se s takovým jednáním setkali, ale o podvod se nejednalo (15 %), dále se s takovým jednáním setkali, byl to podvod a nereagovali na to (téměř 4 %) a dokonce se s takovým jednáním setkali a přišli o peníze (téměř 1 %).

4 % žáků 6. tříd rovněž uvedlo, že se s takovým požadavkem setkalo, přičemž žáci 6. tříd dále odpověděli, že se s takovým jednáním setkali, ale o podvod se nejednalo (téměř 3 %) a dále se s takovým jednáním setkali, byl to podvod, ale nereagovali na to (téměř 2 %). Tímto způsobem podvedeni přímo nebyli.

Položka č. 28



Graf č. 35 *– relativní četnost odpovědí na položku č. 28 v dotazníku pro žáky základních škol.*

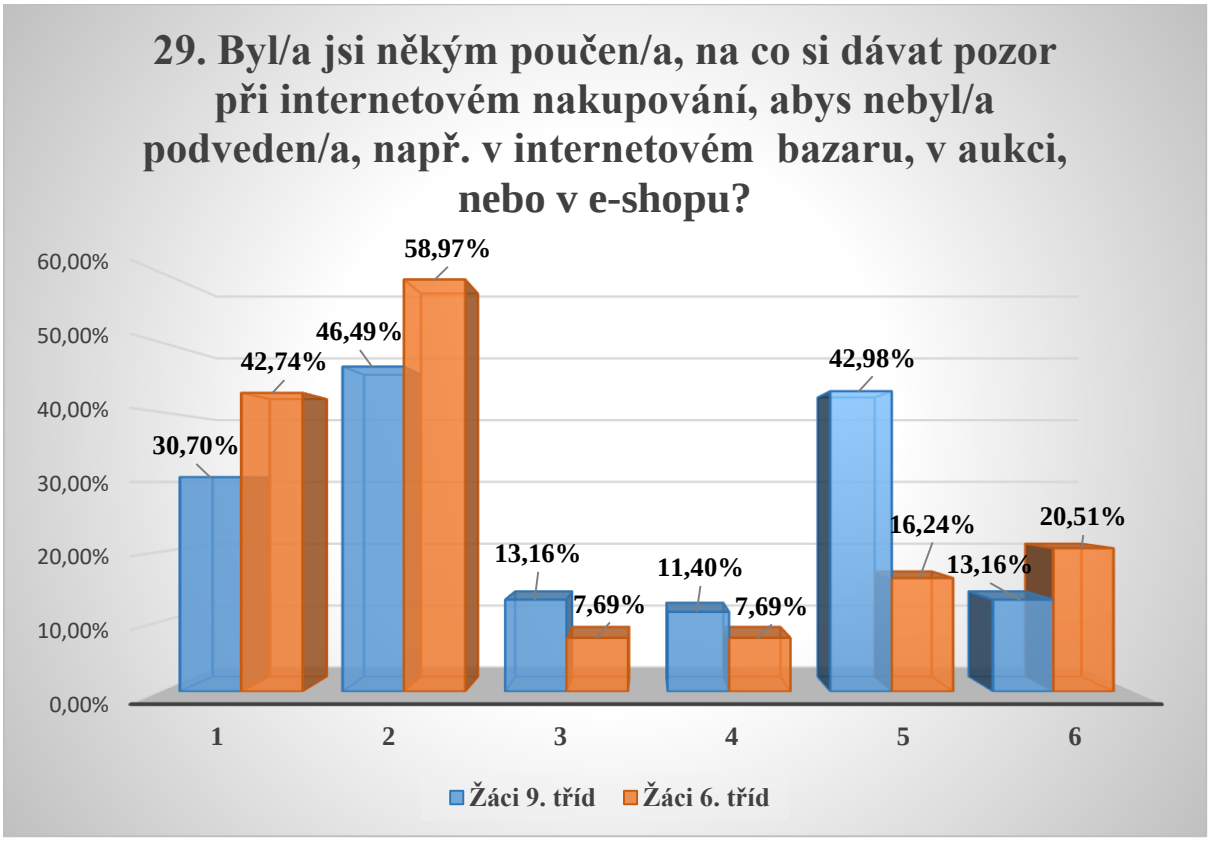
Odpovědi vztahující se k číselným hodnotám 1–2 v grafu č. 35:

1	Ano	**2**	Ne

Facebook v případě napadení účtu žádnou zprávu nezasílá. Tato položka č. 28 je tak jednoduchou imitací phishingu pomocí SMS zprávy (smishing).

Téměř 10 % žáků 9. tříd uvedlo, že přes takovou SMS zprávu by se ke svému účtu přihlásilo, stejně jako téměř 9 % žáků 6. tříd.

Položka č. 29



Graf č. 36 *– relativní četnost odpovědí na položku č. 29 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–6 v grafu č. 36:

1	Ano, ve škole.
2	Ano, rodiči.
3	Ano, kamarádem.

4	Ano, někým jiným.
5	Sám/a jsem si o tom četl/a, slyšel/a.
6	Ne, nikým.

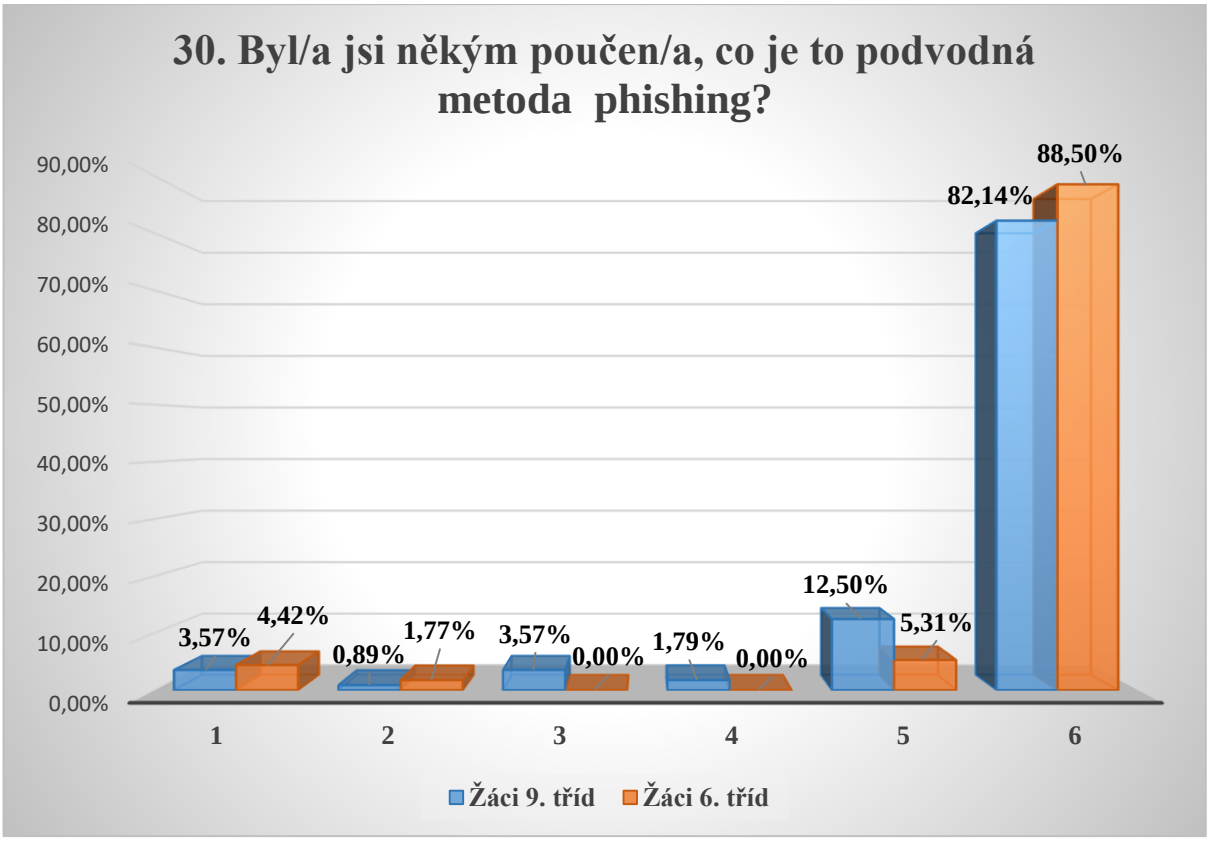
Zda byli žáci seznámeni s vybranými riziky podvodného jednání v IT prostředí, se zabývaly v dotazníku položky č. 29–33 a pokud ano, tak kým.

Na položku č. 29 **žáci 9. tříd uvedli, že před internetovými podvody souvisejícími s nakupováním byli poučeni ve škole (téměř 31 %),** rodiči (téměř 47 %), kamarádem (13 %) nebo někým jiným (11 %). Také se o tento druh internetových podvodů někteří sami zajímali (téměř 43 %) a nikým poučeni nebyli (13 %).

Žáci 6. tříd uvedli, že před internetovými podvody souvisejícími s nakupováním byli poučeni ve škole (téměř 43 %), rodiči (59 %), kamarádem (téměř 8 %) nebo někým jiným (téměř 8 %). Také se o tento druh internetových podvodů někteří sami zajímali (16 %) a nikým poučeni nebyli (téměř 21 %).

Zjištěným výsledkem z této položky byla splněna část dílčího cíle diplomové práce *„Byli někým vybraní žáci 6. a 9. tříd základních škol v Prostějově poučeni o vybraném podvodném jednání v IT prostředí?“*

Položka č. 30



Graf č. 37 *– relativní četnost odpovědí na položku č. 30 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–6 v grafu č. 37:

1	Ano, ve škole.
2	Ano, rodiči.
3	Ano, kamarádem.

4	Ano, někým jiným.
5	Sám/a jsem si o tom četl/a, slyšel/a.
6	Nevím co je to phishing.

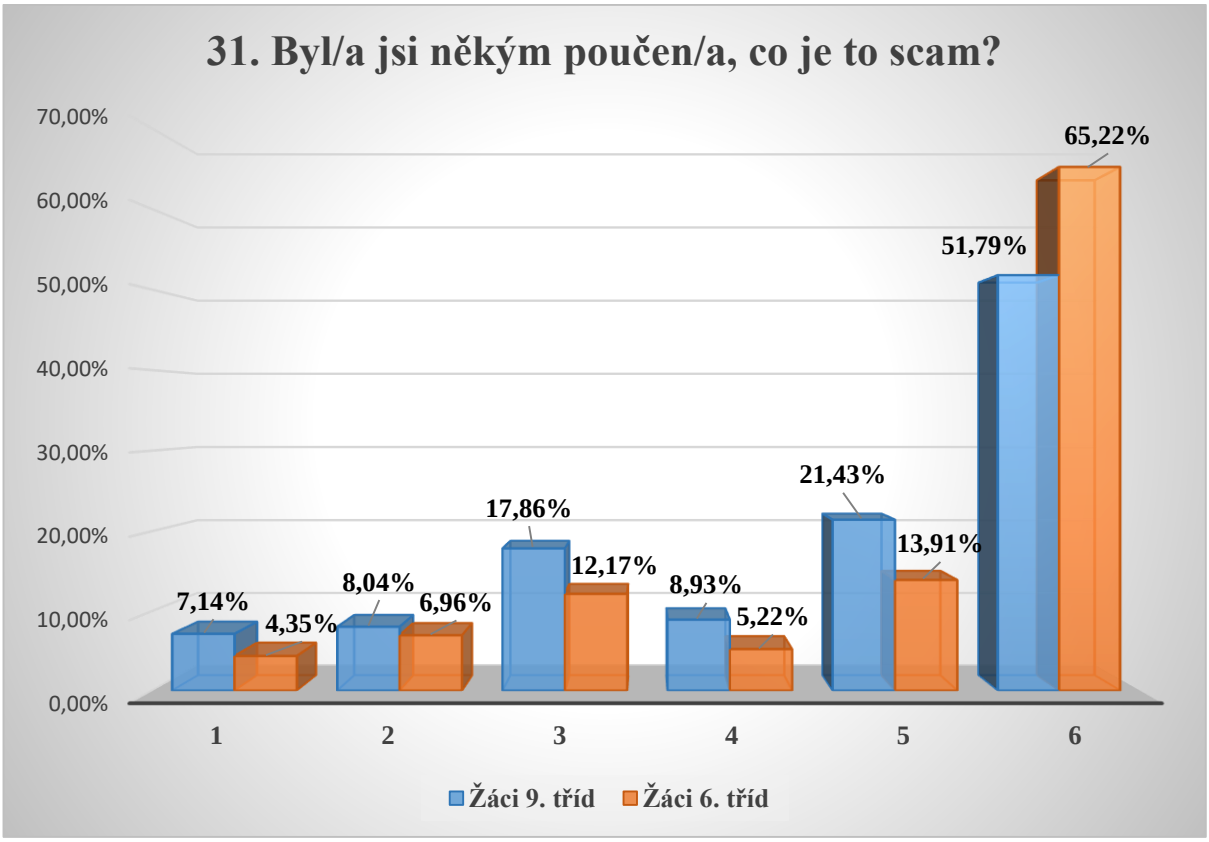
82 % žáků 9. tříd uvedlo, že neví, co je to phishing, stejně jako téměř 89 % žáků 6. tříd.

Žáci 9. tříd dále uvedli, že o tom, co je phishing, byli poučeni ve škole (téměř 4 %), rodiči (téměř 1 %), kamarádem (téměř 4 %) nebo někým jiným (téměř 2 %), ale také se někteří o phishing sami zajímali (téměř 13 %).

Žáci 6. tříd dále uvedli, že o phishingu byli poučeni ve škole (4 %) nebo rodiči (téměř 2 %), ale také se někteří o tento druh podvodu sami zajímali (5 %).

Zjištěným výsledkem z této položky byla splněna část dílčího cíle diplomové práce *„Byli někým vybraní žáci 6. a 9. tříd základních škol v Prostějově poučeni o vybraném podvodném jednání v IT prostředí?“*

Položka č. 31



Graf č. 38 *– relativní četnost odpovědí na položku č. 31 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–6 v grafu č. 38:

1	Ano, ve škole.
2	Ano, rodiči.
3	Ano, kamarádem.
4	Ano, někým jiným.
5	Sám/a jsem si o tom četl/a, slyšel/a.
6	Nevím co je to scam.

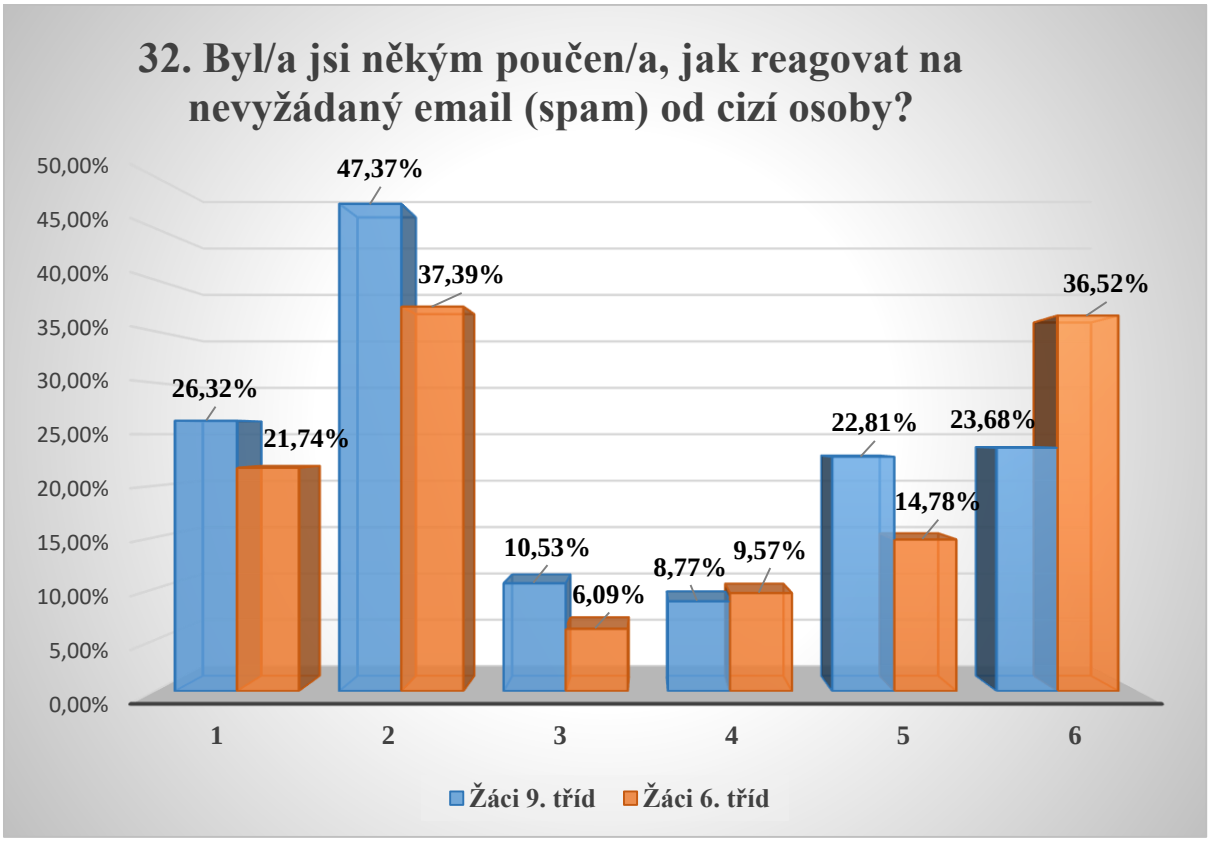
Téměř 52 % žáků 9. tříd uvedlo, že neví, co je to scam, stejně jako 65 % žáků 6. tříd.

Žáci 9. tříd dále uvedli, že o tom, co je to scam byli poučeni ve škole (7 %), rodiči (8 %), kamarádem (téměř 18 %) nebo někým jiným (9 %), ale také se někteří o scam sami zajímali (21 %).

Žáci 6. tříd dále uvedli, že o scamu byli poučeni ve škole (4 %), rodiči (7 %), kamarádem (12 %) nebo někým jiným (5 %), ale také se někteří o scam sami zajímali (14 %).

Zjištěným výsledkem z této položky byla splněna část dílčího cíle diplomové práce *„Byli někým vybraní žáci 6. a 9. tříd základních škol v Prostějově poučeni o vybraném podvodném jednání v IT prostředí?“*

Položka č. 32



Graf č. 39 *– relativní četnost odpovědí na položku č. 32 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–6 v grafu č. 39:

1	Ano, ve škole.
2	Ano, rodiči.
3	Ano, kamarádem.

4	Ano, někým jiným.
5	Sám/a jsem si o tom četl/a, slyšel/a.
6	Ne.

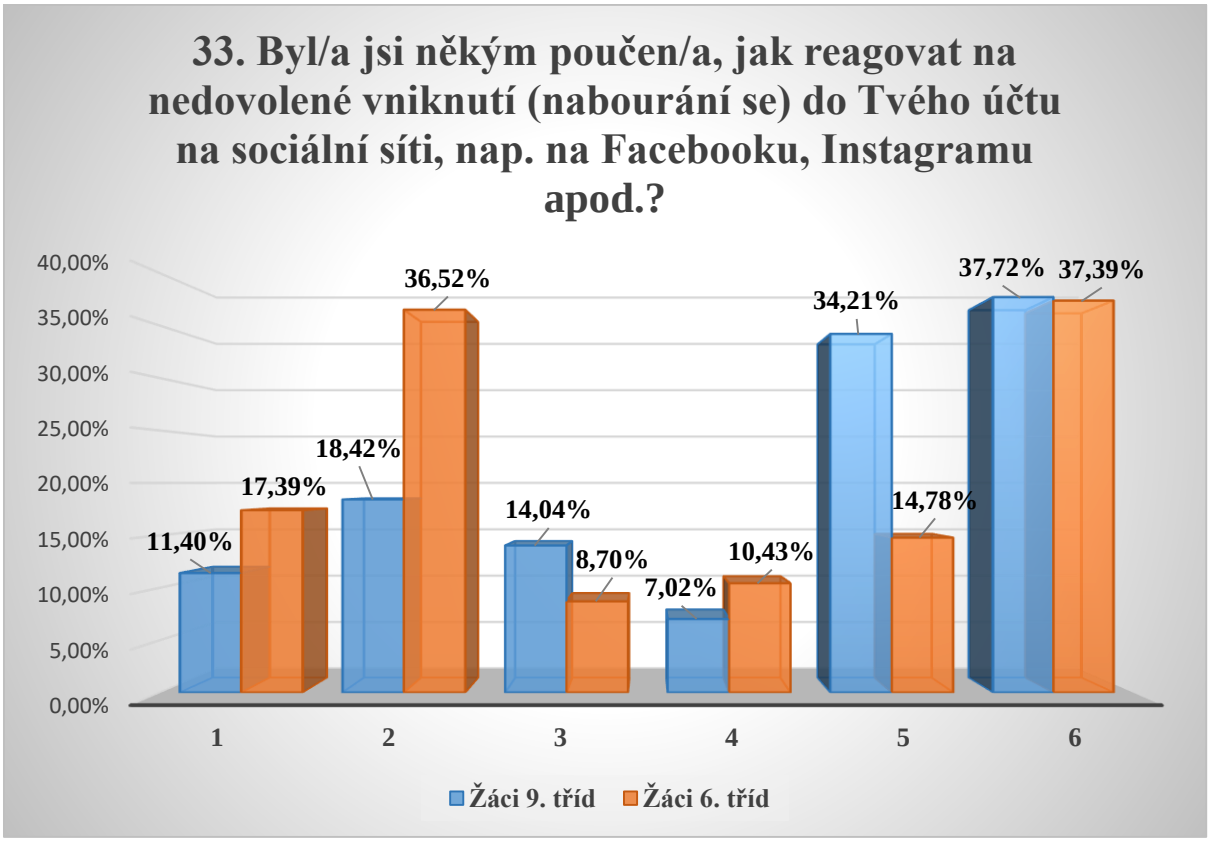
Téměř 24 % žáků 9. tříd nebylo nikým poučeno, jak reagovat na spam, stejně jako téměř 37 % žáků 6. tříd.

Žáci 9. tříd dále uvedli, že o tom, jak reagovat na spam byli poučeni ve škole (26 %), rodiči (47 %), kamarádem (téměř 11 %) nebo někým jiným (téměř 9 %), ale také se někteří o to sami zajímali (téměř 23 %).

Žáci 6. tříd dále uvedli, že o tom, jak reagovat na spam byli poučeni ve škole (téměř 22 %), rodiči (37 %), kamarádem (6 %) nebo někým jiným (téměř 10 %), ale také se někteří o to sami zajímali (téměř 15 %).

Zjištěným výsledkem z této položky byla splněna část dílčího cíle diplomové práce *„Byli někým vybraní žáci 6. a 9. tříd základních škol v Prostějově poučeni o vybraném podvodném jednání v IT prostředí?“*

Položka č. 33



Graf č. 40 *– relativní četnost odpovědí na položku č. 33 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–6 v grafu č. 40:

1	Ano, ve škole.
2	Ano, rodiči.
3	Ano, kamarádem.
4	Ano, někým jiným.
5	Sám/a jsem si o tom četl/a, slyšel/a.
6	Ne.

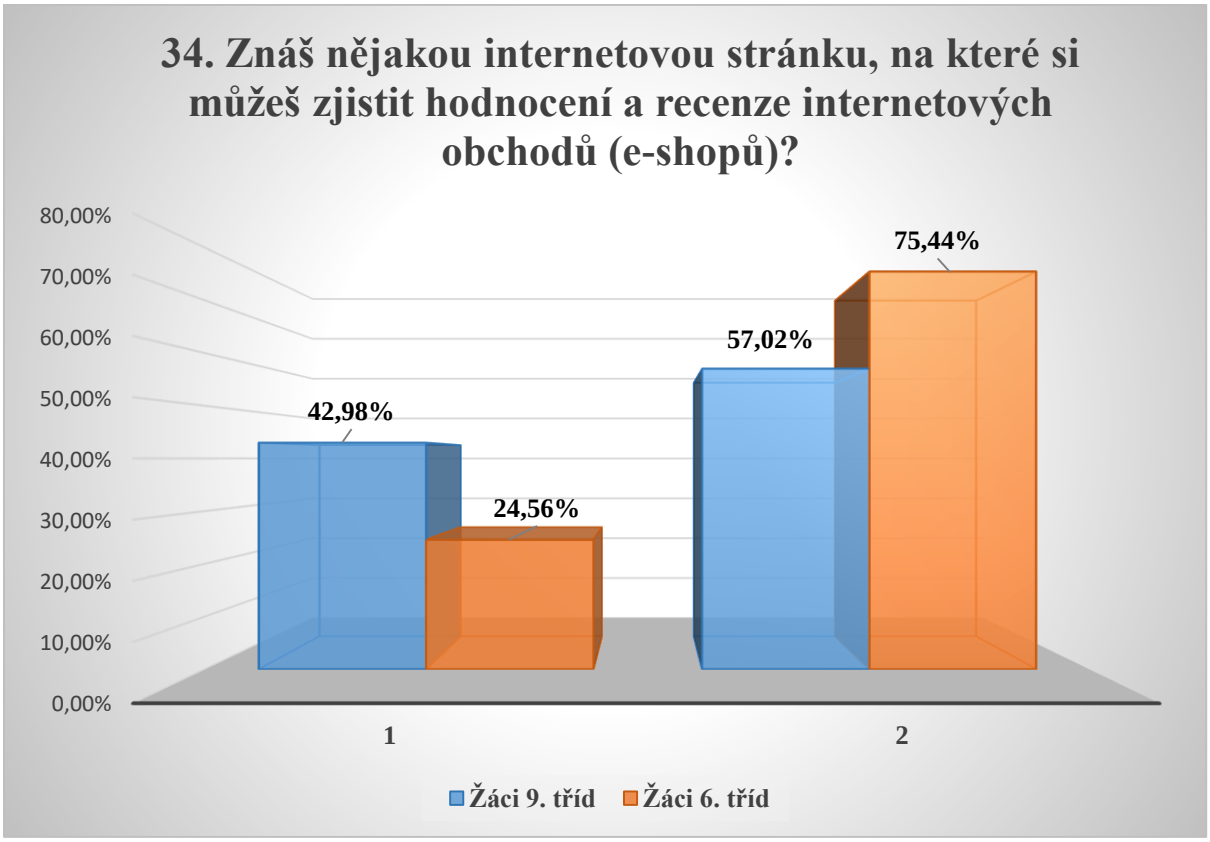
Téměř 38 % žáků 9. tříd nebylo nikým poučeno, jak reagovat na neoprávněné vniknutí to svého účtu na sociální síti, stejně jako 37 % žáků 6. tříd.

Žáci 9. tříd dále uvedli, že o tom, jak reagovat na neoprávněné vniknutí to svého účtu na sociální síti byli poučeni ve škole (11 %), rodiči (18 %), kamarádem (téměř 14 %) nebo někým jiným (téměř 7 %), ale také se někteří o to sami zajímali (34 %).

Žáci 6. tříd dále uvedli, že o tom, jak reagovat na neoprávněné vniknutí to svého účtu na sociální síti byli poučeni ve škole (17 %), rodiči (téměř 37 %), kamarádem (téměř 9 %) nebo někým jiným (10 %), ale také se někteří o to sami zajímali (téměř 15 %).

Zjištěným výsledkem z této položky byla splněna část dílčího cíle diplomové práce *„Byli někým vybraní žáci 6. a 9. tříd základních škol v Prostějově poučeni o vybraném podvodném jednání v IT prostředí?“*

Položka č. 34



***Graf č. 41**– relativní četnost odpovědí na položku č. 34a v dotazníku pro žáky základních škol.*

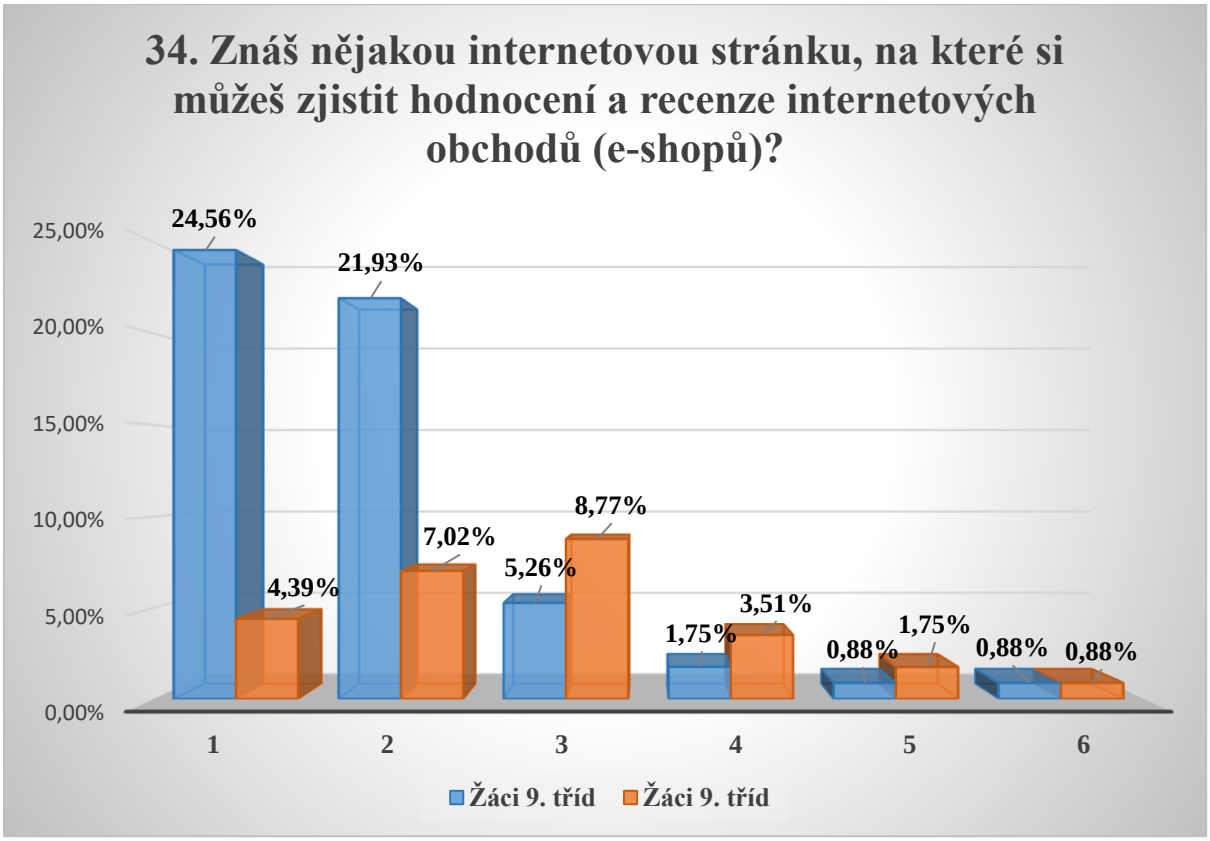
Odpovědi vztahující se k číselným hodnotám 1–2 v grafu č. 41:

1	Ano	**2**	Ne

Téměř v samotném závěru byli žáci dotazováni, zda znají nějakou internetovou stránku, na které si mohou zjistit hodnocení a recenze internetových e-shopů. Pokud byli někým poučeni o rizicích nakupování na internetovém e-shopu, jeden z nejdůležitějších prvků bezesporu je, kde si o takových e-shopech mohou přečíst hodnocení.

57 % žáků 9. tříd uvedlo, že nezná žádnou internetovou stránku, na které si může zjistit hodnocení a recenze internetových e-shopů, stejně jako 75 % žáků 6. tříd.

Položka č. 34



***Graf č. 42**– relativní četnost odpovědí na položku č. 34b v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–6 v grafu č. 42:

1	Heureka.
2	Žáci, kteří odpověděli na tuto položku kladně, že stánky znají, ale přitom neuvedli žádnou odpověď.
3	Alza.

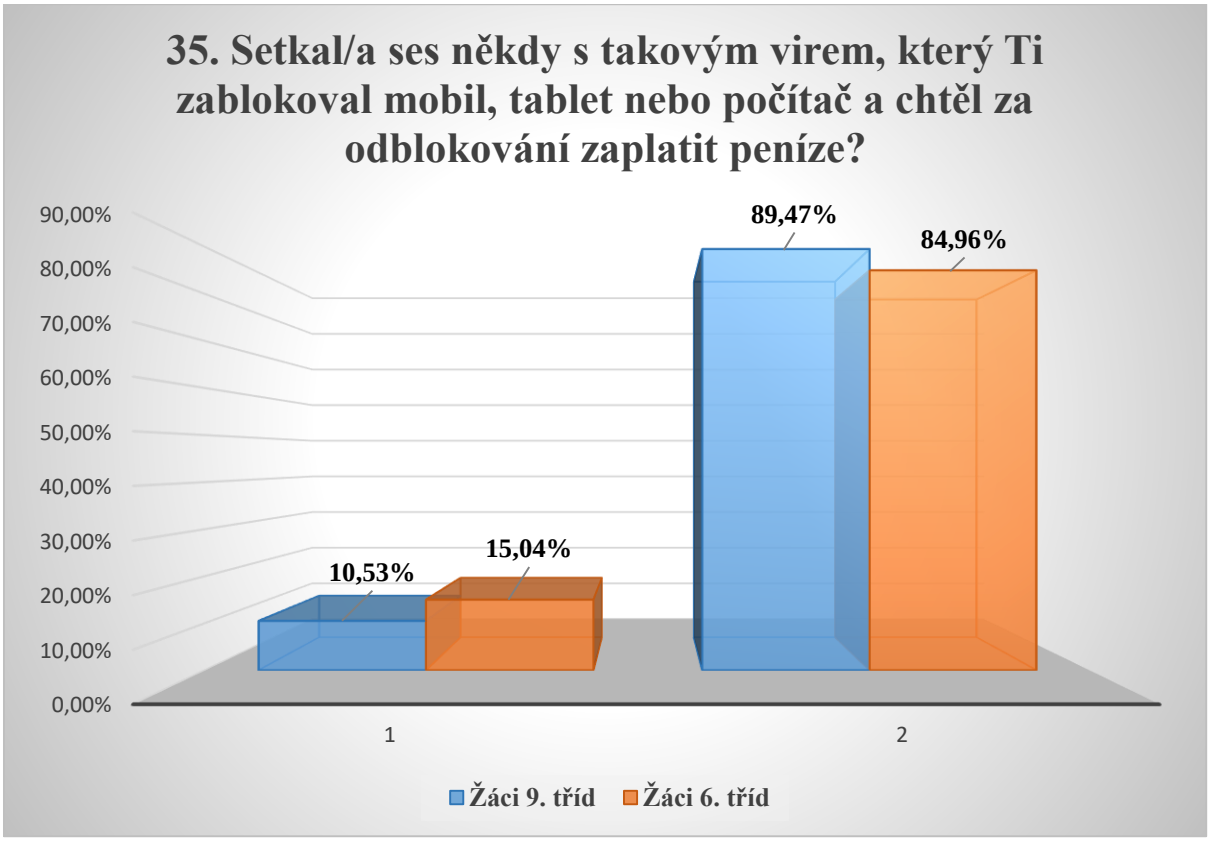
4	CZC.
5	Google play, Google.
6	Wish.

Pakliže žáci odpověděli, že znají nějakou internetovou stránku, kde si e-shop mohou ověřit, bylo provedeno vyhodnocení jejich odpovědí (graf č. 42), které se vztahují k celkovému vzorku respondentů.

Paradoxně téměř 22 % žáků 9. tříd neuvedlo žádnou internetovou stránku, kde lze hodnocení nalézt, stejně jako 7 % žáků 6. tříd.

Téměř 25 % žáků 9. tříd zná internetovou stánku Heureka k ověřování e-shopů, stejně jako 4 % žáků 6. tříd. Dále, ačkoliv žáci uváděli v odpovědi Alza, CZC, Google play, Wish, je třeba poznamenat, že se jedná právě o internetové obchody (kromě online distribuční služby Google play), na kterých lze nalézt hodnocení a recenze nikoliv e-shopů, ale zboží.

Položka č. 35



***Graf č. 43**– relativní četnost odpovědí na položku č. 35 v dotazníku pro žáky základních škol.*

Odpovědi vztahující se k číselným hodnotám 1–2 v grafu č. 43:

1	Ano	**2**	Ne

Tato závěrečná položka č. 35 byla zaměřena na vyděračský škodlivý program ransomware, zda se s ním žáci základních škol někdy setkali.

Téměř 11 % žáků 9. tříd uvedlo, že se s takovým škodlivým počítačovým programem setkalo, stejně jako 15 % žáků 6. tříd.

Zjištěným výsledkem z této položky byla splněna část dílčího cíle diplomové práce *„Jaký je rozdíl v četnosti cílených útoků pachatele vybraného podvodného jednání v IT prostředí na žáky 6. a 9. tříd na základních školách v Prostějově?“*

10.2 Verifikace hypotéz

Zda mezi proměnnými existuje vztah, ověřujeme pomocí statistických testů významnosti. Na jejich základě rozhodujeme, zda je mezi jevy statisticky významný vztah, čímž vylučujeme výsledek zjištěný pouhou náhodou (Chráska, 2016, s. 63).

Při verifikaci hypotéz využijeme testu dobré shody chví-kvadrát, kterým budeme ověřovat, zda se získané četnosti v pedagogické realitě odlišují od teoretických četností odpovídající nulové hypotéze (Chráska, 2016, s. 64).

HYPOTÉZA 1: **Žáci 9. tříd základních škol v Prostějově častěji nakupují v IT prostředí, než žáci 6. tříd základních škol v Prostějově**.

První hypotéza představuje porovnání četnosti nakupování v IT prostředí mezi vybranými žáky 6. tříd a 9. tříd základních škol v Prostějově. Na základě uvedeného testu bude rozhodnuto, zda jsou mezi oběma skupinami žáků v četnosti nakupování statisticky významné rozdíly. Pro ověřování hypotézy byla použita položka v dotazníku č. 7, 8, 9, 10, 12, 13.

Z věcné hypotézy byla formulována statistická nulová a alternativní hypotéza.

H0: Mezi četností nakupování v IT prostředí žáků 9. tříd a 6. tříd základních škol v Prostějově není rozdíl.

HA: Mezi četností nakupování v IT prostředí žáků 9. tříd a 6. tříd základních škol v Prostějově je rozdíl.

Pokud proměnné jevy, mezi nimiž ověřujeme vztah, mohou nabývat pouze dvou alternativních kvalit (např. žáci častěji nakupují/nenakupují), přichází v úvahu použití čtyřpolní tabulky (Chráska, 2016, s. 76). U každé položky z celkové četnosti respondentů odečteme tedy negativní odpověď (např. nenakupoval/a jsem v e-shopu), čímž získáme pozitivní odpověď (nakupovala jsem v e-shopu).

Tabulka č. 2 – vzor pro stanovení hodnot do vzorce chví-kvadrátu pro čtyřpolní tabulku: (Chráska, 2016, s. 77).

	ANO	NE	∑
Žáci 9. tříd	a	b	a + b
Žáci 6. tříd	c	d	c + d
∑	a + c	b + d	n

Tabulka č. 3 – data pro výpočet chví-kvadrátu pro čtyřpolní tabulku k hypotéze č. 1.

Položka č. 7 **–** nákup na internetu obecně.

	ANO	NE	∑
Žáci 9. tříd	96	19	115
Žáci 6. tříd	70	46	116
∑	166	65	**231**

Položka č. 8 – nákup v internetové aukci.

	ANO	NE	∑
Žáci 9. tříd	19	96	115
Žáci 6. tříd	18	99	117
∑	37	195	**232**

Položka č. 9 – nákup v internetovém bazaru.

	ANO	NE	∑
Žáci 9. tříd	40	74	114
Žáci 6. tříd	25	91	116
∑	65	165	**230**

Položka č. 10 – nákup v e-shopu.

	ANO	NE	∑
Žáci 9. tříd	81	33	114
Žáci 6. tříd	60	57	117
∑	141	90	**231**

Položka č. 12 – nákup přes herní účet.

	ANO	NE	∑
Žáci 9. tříd	48	66	114
Žáci 6. tříd	41	76	117
∑	89	142	**231**

Položka č. 13 – nákup mikrotransakce.

	ANO	NE	∑
Žáci 9. tříd	31	83	114
Žáci 6. tříd	34	83	117
∑	65	166	**231**

Položka č. 12 – nákup přes herní účet.

	SÁM	S RODIČEM	∑
Žáci 9. tříd	30	17	47
Žáci 6. tříd	11	32	43
∑	41	49	**90**

Položka č. 13 – nákup mikrotransakce.

	SÁM	S RODIČEM	∑
Žáci 9. tříd	27	12	39
Žáci 6. tříd	15	22	37
∑	42	34	**76**

Test nezávislosti chví-kvadrát pro čtyřpolní tabulku lze použít pouze tehdy, pokud je celková četnost větší než 40 (Chráska, 2016, s. 76), což je v daném případě splněno.

Pro získání testového kritéria ($\boldsymbol{x^2}$), které bude porovnáno se stanovenou hodnotou 3,841 pro hladinou významnosti 0,05 a 1 stupeň volnosti, použijeme pro jeho výpočet jednoduchý vzorec $\boldsymbol{x^2 = n \frac{(ad-bc)^2}{(a+b)(a+c)(b+c)(c+d)}}$ (Chráska, 2016, s. 77, 234).

Pokud bude vypočítaná hodnota větší, než hodnota hladiny významnosti 3,841, odmítneme nulovou hypotézu a přijmeme hypotézu alternativní. Pokud bude vypočítaná hodnota menší než hodnota hladiny významnosti, není tak statisticky významný rozdíl a přijmeme nulovou hypotézu, respektive odmítneme hypotézu alternativní.

Tabulka č. 4 – výpočet podle chví-kvadrátu k hypotéze č.1.

	Vypočítaná hodnota	**Výsledek**
Pro položku č. 7 – nákup na internetu obecně, odpověď ANO / NE.	$\boldsymbol{x^2}$= 15,283	**Přijata alternativní hypotéza.**
Pro položku č. 8 – nákup v internetové aukci, odpověď ANO / NE.	$\boldsymbol{x^2}$= 0,055	**Přijata nulová hypotéza.**
Pro položku č. 9 – nákup v internetovém bazaru, odpověď ANO / NE.	$\boldsymbol{x^2}$= 5,196	**Přijata alternativní hypotéza.**
Pro položku č. 10 – nákup v e-shopu, odpověď ANO / NE.	$\boldsymbol{x^2}$= 9,490	**Přijata alternativní hypotéza.**
Pro položku č. 12 – nákup přes herní účet, odpověď ANO / NE.	$\boldsymbol{x^2}$= 1,216	**Přijata nulová hypotéza.**
Pro položku č. 13 – nákup mikrotransakce, odpověď ANO / NE.	$\boldsymbol{x^2}$= 0,099	**Přijata nulová hypotéza.**
Pro položku č. 12 – nákup přes herní účet, odpověď SÁM / S RODIČI.	$\boldsymbol{x^2}$= 13,245	**Přijata alternativní hypotéza.**
Pro položku č. 13 – nákup mikrotransakce, odpověď SÁM / S RODIČI.	$\boldsymbol{x^2}$= 6,321	**Přijata alternativní hypotéza.**

Z výsledků lze konstatovat, že žáci 9. tříd na internetu nakupují častěji než žáci 6. tříd. Konkrétně **žáci 9. tříd nakupují častěji v internetových e-shopech a bazarech, než žáci 6. tříd**. Rozdíl v četnosti nakupování na internetových aukcích, obecně přes internetové herní účty

a obecně vylepšení do her, není statisticky významné. Přesto je třeba z výsledků výzkumného šetření konstatovat, že **žáci 9. tříd nakupují přes herní účty a vylepšení do her častěji sami než s rodiči, což je u žáků 6. tříd přesně naopak** (v daných případech byl ověřen statisticky významný rozdíl).

HYPOTÉZA 2: **Žáci 9. tříd základních škol v Prostějově jsou častěji cílem útoku pachatele vybraného podvodného jednání v IT prostředí, než žáci 6. tříd základních škol v Prostějově.**

Velmi podstatné zjištění pro účely této diplomové je, zda se žáci základních škol vůbec osobně setkali s určitými formami podvodného jednání, o kterých pojednává tato diplomová práce. Pokud ano, je třeba ověřit, zda existuje statisticky významný rozdíl mezi četností cílených útoků pachatele vybraného podvodného jednání v IT prostředí na žáky 9. tříd a 6. tříd základních škol v Prostějově. Z tohoto důvodu byla vytvořena statistická nulová a alternativní hypotéza. Pro ověřování byla použita položka v dotazníku č. 20, 21, 22, 24, 25, 27, 35.

H0: Mezi četností cílených útoků pachatele vybraného podvodného jednání v IT prostředí na žáky 9. tříd a 6. tříd základních škol v Prostějově není rozdíl.

HA: Mezi četností cílených útoků pachatele vybraného podvodného jednání v IT prostředí na žáky 9. tříd a 6. tříd základních škol v Prostějově je rozdíl.

Tabulka č. 5 – data pro výpočet chví-kvadrátu pro čtyřpolní tabulku k hypotéze č. 2.

Položka č. 20 – vznikla majetková škoda.

	ANO	NE	∑
9. třída	5	108	113
6. třída	5	112	117
∑	10	220	**230**

Položka č. 20 – zavirovaný odkaz.

	ANO	NE	∑
9. třída	7	106	113
6. třída	5	112	117
∑	12	218	**230**

Položka č. 20 – hacking účtu.

	ANO	NE	∑
9. třída	12	101	113
6. třída	7	110	117
∑	19	211	**230**

Položka č. 20 – kontakt z falešného účtu.

	ANO	NE	∑
9. třída	28	85	113
6. třída	5	112	117
∑	33	195	**230**

Položka č. 21 – podveden při nákupu zboží.

	ANO	NE	∑
9. třída	6	108	114
6. třída	1	115	116
∑	7	223	**230**

Položka č. 22 – doručení spamu, scamu.

	ANO	NE	∑
9. třída	82	32	114
6. třída	43	70	113
∑	125	102	**227**

Položka č. 24 – podvodné prozvánění.

	ANO	NE	∑
9. třída	13	101	114
6. třída	20	96	116
∑	33	197	**230**

Položka č. 25 – phishing – odkaz.

	ANO	NE	∑
9. třída	31	84	115
6. třída	17	99	116
∑	48	183	**231**

Položka č. 27 – žádost o podvodnou platbu.

	ANO	NE	∑
9. třída	5	109	114
6. třída	2	114	116
∑	7	223	**230**

Položka č. 35 – výskyt ransomware.

	ANO	NE	∑
9. třída	12	102	114
6. třída	17	96	113
∑	29	198	**227**

Tabulka č. 6 – výpočet hodnot podle chví-kvadrátu k hypotéze č. 2.

	Vypočítaná hodnota	**Výsledek**
Položka č. 20 – podvodem vznikla majetková škoda, odpověď ANO / NE.	$\boldsymbol{x^2}$= 0,031	**Přijata nulová hypotéza.**
Položka č. 20 – kliknutí na podvodný zavirovaný odkaz, odpověď ANO / NE.	$\boldsymbol{x^2}$= 0,429	**Přijata nulová hypotéza.**
Položka č. 20 – hacking účtu, odpověď ANO / NE.	$\boldsymbol{x^2}$= 1,630	**Přijata nulová hypotéza.**
Položka č. 20 – kontaktování z falešného účtu na Facebooku, odpověď ANO / NE.	$\boldsymbol{x^2}$= 19,868	**Přijata alternativní hypotéza.**
Položka č. 21 – podveden při nákupu zboží, odpověď ANO / NE.	$\boldsymbol{x^2}$= 3,774	**Přijata nulová hypotéza.**
Položka č. 22 – doručení spamu, scamu, odpověď ANO / NE.	$\boldsymbol{x^2}$= 26,320	**Přijata alternativní hypotéza.**
Položka č. 24 – podvodné prozvánění, odpověď ANO / NE.	$\boldsymbol{x^2}$= 1,594	**Přijata nulová hypotéza.**
Položka č. 25 – doručení nevyžádané zprávy s odkazem na přihlášení – phishing, odpověď ANO / NE.	$\boldsymbol{x^2}$= 5,308	**Přijata alternativní hypotéza.**
Položka č. 27 – žádost o podvodnou platbu, odpověď ANO / NE.	$\boldsymbol{x^2}$= 1,380	**Přijata nulová hypotéza.**
Položka č. 35 – zablokování ransomware, odpověď ANO / NE.	$\boldsymbol{x^2}$= 1,039	**Přijata nulová hypotéza.**

Žáci 9. tříd se setkali častěji s falešným profilem na Facebook, phishingem a nevyžádanými zprávami (spam, scam), než žáci 6. tříd. Mezi četností cílených útoků pachatele ostatního zkoumaného podvodného jednání v IT prostředí vůči žákům 9. tříd a 6. tříd základních škol v Prostějově tedy statisticky významný rozdíl není.

11 Diskuze a závěry z výzkumného šetření

V této kapitole jsou stručněji analyzovány výsledky z dotazníkového šetření a jsou porovnány se zjištěným aktuálním stavem v daných oblastech, jak je uvedeno v kapitole č 7. Zhodnocení aktuálního stavu zkoumané problematiky.

Preventivní programy proti podvodnému jednání v IT prostředí na základních školách

Vyhlídal ve své bakalářské práci zaměřené na majetkovou kriminalitu na internetu, výzkumným šetřením od 30 školních metodiků prevence základních škol v Olomouckém kraji zjistil, že 90 % těchto škol nemělo preventivní programy zaměřené přímo na majetkovou kriminalitu na internetu (Vyhlídal, 2014, s. 53–54). Z výsledků této práce bylo zjištěno, že téměř 82 % základních škol v Prostějově nemá preventivní programy přímo proti podvodům v prostředí informačních a komunikačních technologií (dále IT), které se mezi majetkovou kriminalitu řadí. Rozdíl 8 % mohl vzniknout díky malému počtu respondentům v této práci (pouze 11), nebo pomalým zaváděním prevence v této oblasti (za 4 roky).

V zásadě lze konstatovat, že **v *naprosté většině základních škol, které byly předmětem zkoumání, chybí preventivní programy zaměřené na kyberkriminalitu, potažmo podvodné jednání***. Přitom téměř 73 % školních metodiků prevence v Prostějově se shodlo, že takový program by přivítali.

Platební možnosti žáků základních škol v IT prostředí

Podvody v IT prostředí jsou mnohdy zaměřeny na placení přes internet a z dotazníkového šetření této práce vyplynulo, že ***48 % žáků 9. tříd a 15 % žáků 6. tříd má možnost provést platbu přes internet***, ať už vlastní platební kartou, internetovým bankovnictvím, platební kartou rodičů, tak prostřednictvím platebních brán např. Paypal, Gopay apod. Jelikož nebylo zjištěno, že by se někdo tímto tématem výzkumně zabýval, nelze výsledky práce porovnat s jinými výsledky.

Vlastnictví platební karty

Ve své bakalářské práci prováděla Hejduková (2017, s. 36–40) výzkumné šetření mezi 92 žáky 8. a 9. tříd základní školy Slatiňany a mimo jiné zjistila, že z daného vzorku vlastnilo platební kartu 15,2 % žáků ZŠ.

Z vlastního výzkumného šetření provedeného mezi 117 žáky 6. a 115 žáky 9. tříd bylo však zjištěno, že ***téměř 37 % žáků 9. tříd uvedlo, že platební kartu vlastní, stejně jako 10 %***

žáků 6. tříd. Oproti výsledkům Hejdukové je u žáků 9. tříd rozdíl téměř 22 %, což je výrazný rozdíl. V dané věci mohl být výsledek ovlivněn shrnutím žáků 8. a 9. tříd a prováděným šetřením v odlišné lokalitě na území České republiky. Prostějov má téměř 44.000 obyvatel, kdežto Slatiňany 4.200 obyvatel.

Platba platební kartou, zkušenosti s internetovým bankovnictvím

Zjištěním v této práci bylo, že téměř ***60 % žáků 9. tříd uvedlo, že někdy platební kartou platilo, v případě žáků 6. tříd to bylo 33 %.*** Dané výsledky opět nebylo možno porovnat s jinými výzkumy či průzkumy.

Při zjišťování zkušenosti s přihlašováním k internetovému bankovnictví ***téměř 32 % žáků 9. tříd uvedlo, že se někdy přihlásilo k internetovému bankovnictví, stejně jako téměř 8 % žáků 6. tříd***. Zajímavé zjištění bylo, že téměř 25 % žáků 9. tříd se přihlašovalo k vlastnímu bankovnímu účtu a téměř 8 % žáků 9. tříd se přihlašovalo k bankovnímu účtu rodičů. Dané výsledky nebylo možno porovnat s jinými výzkumy. Pakliže však Český statistický úřad (2017b, s. 96) uvádí, že využívání internetové bankovnictví neustále roste, kdy v roce 2017 jej využilo obecně již 52 % Čechů, což představuje 2/3 osob využívající internet a v severských zemích internetové bankovnictví používá dokonce až 80 % osob, nelze vyloučit v budoucnu ještě častějšího využívání internetového bankovnictví žáky, stejně jako obecně Čechů.

Nakupování a platba za zboží v IT prostředí

Pokud se budeme zabývat otázkou nakupování žáků základních škol na internetu, opět nebyly zjištěny žádné relevantní výzkumy zaměřené přímo na žáky. Pouze Eibensteiner (2015, s. 36, 39) ve své diplomové práci zaměřené na komunikaci zjistil od 118 žáků 8. a 9. tříd základních škol v Uherském Hradišti, že 5,1 % žáků využívá internet i k nakupování.

Zjištěním z výzkumného šetření této práce však bylo zjištěno, že ***83 % žáků 9. tříd někdy něco přes internet nakoupilo, stejně jako 60 % žáků 6. tříd***. Nejčastěji žáci nakupovali oblečení, hry, elektroniku a sportovní věci, což mimo her odpovídá i zjištění Českého statistického úřadu (2017b, s. 108–111) obdobně jako jejich zjištěný obdobný a publikovaný výsledek, že 79 % Čechů ve věkové skupině mezi 16–24 lety alespoň jednou na internetu nakoupilo.

Pokud se budeme zabývat otázkou, kdo provádí platby v případě nakupování zboží žáky na internetu, lze částečně potvrdit tvrzení autorů McCarthy a Weldon-Siviy (2013, s. 143), že osoby mladší 18 let si online zboží mnohdy sami vyberou, ale zaplatí to rodiče.

Z výsledků této práce bylo zjištěno, že za téměř 70 % žáků 9. tříd zaplatili za zboží nakoupené přes internet někdy rodiče, stejně jako za téměř 67 % žáků 6. tříd. Rovněž bylo podstatné zjištění, že 57 % žáků 9. tříd uvedlo, že sami někdy zaplatili zboží, které přes internet zakoupili, stejně jako 20 % žáků 6. tříd.

Pokud bychom se zabývali podrobněji otázkou, kde přesně žáci základních škol někdy nakupovali, tak bylo zjištěno následující:

Téměř 17 % žáků 9. tříd má nějakou zkušenost s nákupem v aukci, stejně jako 15 % žáků 6. tříd.

35 % žáků 9. tříd někdy nakupovalo v internetovém bazaru, stejně jako téměř 22 % žáků 6. tříd.

71 % žáků 9. tříd někdy nakupovalo v internetovém obchodě, stejně jako téměř 51 % žáků 6. tříd.

42 % žáků 9. tříd uvedlo, že někdy nakoupilo přes nějaký herní účet, stejně jako 35 % žáků 6. tříd, 26 % žáků 9. tříd nakupovalo přes herní účet samo, stejně jako 9 % žáků 6. tříd. S rodiči nakupovalo přes herní účet 15 % žáků 9. tříd a 27 % žáků 6. tříd.

27 % žáků 9. tříd uvedlo, že někdy nakoupilo herní vylepšení, stejně jako 29 % žáků 6. tříd, téměř 24 % žáků 9. tříd nakupovalo takové herní vylepšení samo, stejně jako téměř 13 % žáků 6. tříd. S rodiči nakupovalo téměř 11 % žáků 9. tříd a téměř 19 % žáků 6. tříd.

Výše uváděné výsledky z práce ohledně placení a nakupování přes internet žáky základních škol opět nebylo možno porovnat s žádnými jinými výzkumy či výzkumným šetřením, respektive nebyly zjištěny žádné takové výzkumy zaměřené přímo na nakupování či placení zboží přes internet ze strany žáků 2. stupně základních škol.

Ověřování prodávajícího subjektu žáky základních škol

To, že se žáci pohybují v prostředí internetových inzercí, může napovědět i zjištění z dotazníkového šetření této práce, že téměř ***44 % žáků 9. tříd uvedlo, že někdy přes internet něco prodávalo, stejně jako téměř 26 % žáků 6. tříd***. Jelikož nebylo zjištěno, že by se někdo tímto tématem zabýval, nelze opět výsledky práce porovnat s jinými výsledky.

Nejčastější podvody na internetu jsou spojeny s nakupováním v internetových aukcích a v současné době zejména v internetových bazarech a e-shopech. Proto bylo jedním z dílčích cílů práce zjistit, jak si žáci vlastně ověřují prodávající subjekt, aby nebyli podvedeni.

Při dotazování ohledně ověřování e-shopů žáci 9. tříd uváděli, že si hledají jeho hodnocení (47 %), informace o něm (25 %), pročítají si obchodní podmínky (téměř 23 %),

hledají dobu existence e-shopu (téměř 8 %), 18 % žáků 9. tříd uvedlo, že si e-shopy nijak neověřuje a 14 % ani neví jak a kde.

Žáci 6. tříd uváděli, že si o e-shopu hledají hodnocení (20 %), informace (13 %), pročítají si obchodní podmínky (téměř 11 %), hledají dobu existence e-shopu (téměř 4 %), 10 % žáků 6. tříd si e-shopy nijak neověřuje a 10 % ani neví jak a kde.

Je důležité poznamenat, že při ověřování e-shopu je třeba se nezaměřovat pouze na jeden ověřovací aspekt. Z hlediska hodnocení si mohou podvodníci mnohdy pozitivní hodnocení sami psát. Velmi důležitým prvkem je ověřování doby existence e-shopu, (podvodné e-shopy existují pouze krátce) i pročítání obchodních podmínek (např. možnost osobního vyzvednutí).

Pokud byli žáci dotazníkového šetření dotazování, zda znají nějakou internetovou stránku, na které si mohou ověřit vůbec hodnocení e-shopu, ***57 % žáků 9. tříd uvedlo, že nezná žádnou internetovou stránku, na které si může zjistit hodnocení a recenze internetových e-shopů, stejně jako 75 % žáků 6. tříd.*** Přitom ale ***pouze téměř 25 % žáků 9. tříd uvedlo, že zná internetovou stánku Heureka k ověřování e-shopů, stejně jako 4 % žáků 6. tříd***. Dále, ačkoliv žáci uváděli v odpovědi např. Alza, CZC, Google play, Wish, je třeba poznamenat, že se jedná právě o internetové obchody (kromě online distribuční služby Google play), na kterých lze nalézt hodnocení a recenze nikoliv e-shopů, ale zboží.

V případě ověřování internetových bazarů žáci 9. tříd uváděli, že si o prodejci inzerátu v bazaru hledají hodnocení (téměř 23 %), prohlíží si další nabídky prodejce (15 %), dotazují se na možnost osobního převzetí (7 %), telefonují na kontakt (6 %). Téměř 17 % žáků 9. tříd si prodejce v bazaru neověřuje, 6 % neví jak a kde

Žáci 6. tříd uváděli, že si o prodejci inzerátu v bazaru hledají hodnocení (téměř 8 %), prohlíží si další nabídky prodejce (téměř 9 %), dotazují se na možnost osobního převzetí (téměř 4 %), telefonují na kontakt (4 %). Téměř 9 % žáků 6. tříd si prodejce bazaru neověřuje, 6 % neví jak a kde.

V případě ověřování prodejce internetového bazaru je stejně jako v případě e-shopu třeba nezaměřovat se na jeden ověřovací aspekt. Vhodné je se dotazovat na možnost osobního převzetí, prohlížet si další nabídky prodejce (lze zjistit např. podle uživatelského jména, emailu, tel. čísla apod.).

V případě ověřování internetových aukcí žáci 9. tříd uváděli, že si čtou hodnocení prodejce aukce (téměř 10 %), prohlíží si další nabídky prodejce (téměř 9 %), dotazují se na možnost osobního převzetí (5 %), telefonují na kontakt (6 %). 11% žáků 9. tříd uvedlo, že si prodejce aukce neověřuje, 5 % neví jak a kde.

Žáci 6. tříd uváděli, že si čtou hodnocení prodejce aukce (4 %), prohlíží si další nabídky prodejce (téměř 1 %), telefonují na kontakt (téměř 1 %). 5% žáků 6. tříd uvedlo, že si prodejce aukce neověřuje, 5 % neví jak a kde.

Veškeré zjištěné výsledky opět nebylo možno porovnat s jinými výzkumy či průzkumy.

Dalším podstatným aspektem bylo zjistit a zároveň ověřit, podle čeho by žáci poznali, že jde o podvodný inzerát např. podvodný prodej mobilního telefonu. Z dotazníkového šetření bylo zjištěno, že ***51 % žáků 9. tříd neví, podle čeho by poznalo podvodný inzerát, stejně jako téměř 72 % žáků 6. tříd.*** Od 49 % žáků 9. tříd byla tedy získána kladná odpověď, stejně jako od 28 % žáků 6. tříd.

Žáci 9. tříd uváděli, že podvodný inzerát by poznali nejčastěji podle velmi nízké ceny (téměř 17 %), podle fotografií stažených z internetu nebo málo fotografií (téměř 16 %), podle chybějících údajů ke zboží či prodejci, např. kontakt (10 %), podle gramatických chyb nebo strojové češtiny (6 %), podle požadavku pouze platby předem na účet (4 %)

Žáci 6. tříd uváděli, že podvodný inzerát by poznali podle velmi nízké ceny (4 %), podle fotografií stažených z internetu nebo málo fotografií (6 %), podle chybějících údajů ke zboží či prodejci, např. kontakt, (téměř 7 %), podle gramatických chyb nebo strojové češtiny (téměř 1%), podle požadavku pouze platby předem na účet (téměř 2 %). 9 % žáků 6. tříd navíc odpovědělo chybnou odpověď, např. že zboží by bylo nabízeno za velmi vysokou cenu, inzerát by byl hodně starý, zboží by bylo nabízeno zdarma.

Veškeré zjištěné výsledky opět nebylo možno porovnat s jinými výzkumy.

Žáci základních škol cílem útoku pachatele podvodného jednání

Z dotazníkového šetření této práce vyplynulo, že ***44 % žáků 9. tříd bylo někdy nějakým způsobem na internetu podvedeno, stejně jako téměř 19 % žáků 6. tříd.***

Žáci 9. tříd uváděli, že jim někdo psal z falešného facebookového účtu (téměř 25 %), přišla jim podvodná zpráva (22 %), někdo se jim „*naboural*“ do nějakého účtu (téměř 11 %), někdo je podvedl a klikli na zavirovaný odkaz (6 %), vlivem podvodu jim vznikla majetková škoda (4 %), někomu jinému jejich vlivem vznikla majetková škoda (téměř 3 %), přišli o osobní údaje či fotografie (téměř 1 %).

Žáci 6. tříd uváděli, že jim přišla podvodná zpráva (téměř 8 %), někdo se jim „*naboural*“ do nějakého účtu (6 %), někdo je podvedl a klikli na zavirovaný odkaz (4 %), vlivem podvodu jim vznikla majetková škoda (4 %), někdo jim psal z falešného facebookového účtu (4 %), někomu jinému jejich vlivem vznikla majetková škoda (téměř 1 %), přišli o osobní údaje či fotografie (téměř 1 %).

Při dotazování, zda byli žáci přímo podvedeni při nákupu zboží, uvedlo kladnou odpověď 5 % žáků 9. tříd a téměř 1 % žáků 6. tříd. Téměř 18 % žáků 9. tříd, stejně jako 6 % žáků 6. tříd se navíc setkalo s podvodem při nákupu zboží u někoho ze svého okolí.

Přesto, že zjištěné výsledky opět nebylo možno porovnat s jinými výzkumy, Společnost ESET zabývající se antivirovou ochranou společně se společností Seznam.cz realizovala v prosinci 2017 průzkum ohledně internetového nakupování, v němž bylo zjištěno, že 4 % z 1030 respondentů byli při internetovém nakupování podvedeni (ESET, 2017), což je obdobný výsledek (relativní četnost), jako v případě žáků 9. tříd.

Společnost Intel ve svém průzkumu zjistila od více než 1000 uživatelů, že 74 % Čechů včetně seniorů, někdy obdrželo prostřednictvím internetu podvodnou zprávu (Janouš, 2014).

V případě konkrétního dotazování na podvodné zprávy mezi žáky základních škol v Prostějově z dotazníkového šetření vyplynulo, že ***téměř 72 % žákům 9. tříd byla doručena nevyžádaná zpráva (spam nebo scam), stejně jako 38 % žákům 6. tříd***. Zjištění společnosti Intel tedy téměř odpovídá výsledkům zjištěným v případě žáků 9. tříd.

Dále ***11 % žáků 9. tříd uvedlo, že se setkalo s podvodným prozváněním (wangiri), stejně jako 17 % žáků 6. tříd.*** Zjištěné výsledky opět nebylo možno porovnat s jinými výzkumy.

V případě dotazování žáků základních škol na doručení nevyžádané zprávy s přiloženým odkazem na přihlášení např. do banky, na Facebook nebo herní účet (možný phishing), ***27 % žáků 9. tříd stejně jako 15 % žáků 6. tříd uvedlo, že jim přišla nevyžádaná zpráva s odkazem na takové přihlášení***.

Přesto, že zjištěné výsledky opět nebylo možno porovnat s jinými výzkumy či průzkumy, zajímavé srovnání se nabízí s uživateli antivirové ochrany Kaspersky Lab, kdy tato společnost v roce 2017 zaznamenala pokus o přesměrování na phishingové stránky u 16 % svých uživatelů (Securelist.com, 2018). Uvedených 16 % tedy muselo na takový odkaz kliknout a muselo být chráněno antivirovou ochranu spočívající i v ochraně přímo před phishingem.

V dotazníku pro žáky základních škol byla taktéž položka imitující jednoduchý phishing pomocí SMS zprávy (smishing). Žáci dotazníkového šetření v Prostějově byli dotazování, pokud by jim byla doručena SMS zpráva, že byl napaden jejich facebookový účet a musí se přihlásit přes nabízený odkaz, zda by to udělali. ***Téměř 10 % žáků 9. tříd uvedlo, že přes takovou SMS zprávu, by se ke svému účtu přihlásilo, stejně jako téměř 9 % žáků 6. tříd.*** Jak by tedy žáci reagovali např. na obdobnou zprávu s nabídkou nové hry právě teď v akci zdarma ke stažení, ve které by byl odkaz k přihlášení na určitý herní účet?

Při dotazování žáků, zda v případě písemného oslovení na Facebooku by svému kamarádovi zaslali 20,- Kč na bankovní účet (jedná se o značné riziko podvodu), z dotazníku

vyplynulo, že ***46 % žáků 9. tříd by si neověřilo, zda je oslovil skutečně kamarád s požadavkem zaslání platby, stejně jako téměř 64 % žáků 6. tříd***. Dané zjištění obdobně odpovídá zjištění doc. Kopeckého (2017c), který uvádí, že 49,49 % dětí si neověřuje identitu svých spolužáků, kteří je o přátelství žádají (Kopecký, 2017c). Přitom bylo z dotazníkového šetření v této práci zjištěno, že téměř 17 % žáků 9. tříd a 4 % žáků 6. tříd se setkalo s tím, že je někdo přes sociální síť žádal o zaslání drobné platby nebo přeposlání kódu.

Při dotazování na skutečnost, zda se žáci setkali s vyděračským virem ransomware, ***téměř 11 % žáků 9. tříd uvedlo, že se s takovým škodlivým počítačovým programem setkalo, stejně jako 15 % žáků 6. tříd***. Zjištěné výsledky nebylo možno porovnat se žádným výzkumem ani průzkumem.

Informovanost žáků o vybraných podvodných formách

Přesto, že bylo z dotazníkového šetření této diplomové práce zjištěno, že většina základních škol nemá preventivní programy proti podvodnému jednání v IT prostředí, byli žáci 6. a 9. tříd pro komplexnost dotazníkového šetření dotazování, zda byli poučeni, na co si dávat pozor při internetovém nakupování; zda byli poučeni co je to podvodná metoda phishing; zda byli poučení, co je to scam; zda byli poučeni, jak reagovat na spam; zda byli poučení, jak reagovat na nedovolené vniknutí do jejich účtu na sociální síti (hacking).

Z dotazníkového šetření vyplynulo, mimo jiné následující:

69 % žáků 9. tříd, stejně jako 57 % žáků 6. tříd uvedlo, že nebylo ve škole poučeno, na co si dávat pozor při internetovém nakupování.

96 % žáků 9. tříd, stejně jako 96 % žáků 6. tříd uvedlo, že nebylo ve škole poučeno, co je to phishing, přičemž 82 % žáků 9. tříd a téměř 89 % žáků 6. tříd neví, co to phishing vůbec je**.**

93 % žáků 9. tříd, stejně jako téměř 96 % žáků 6. tříd uvedlo, že nebylo ve škole poučeno, co je to scam, přičemž téměř 52 % žáků 9. tříd a 65 % žáků 6. tříd neví, co to vůbec scam je.

74 % žáků 9. tříd, stejně jako téměř 78 % žáků 6. tříd uvedlo, že nebylo ve škole poučeno, jak reagovat na nevyžádané zprávy (spam, scam).

89 % žáků 9. tříd, stejně jako téměř 83 % žáků 6. tříd uvedlo, že nebylo ve škole poučeno, jak reagovat na nedovolené vniknutí do účtu na sociální síti.

Zjištěné výsledky nebylo možno porovnat opět se žádným zjištěným výzkumem, výzkumným šetřením či průzkumem.

Závěr

Tato práce se zabývala podvodným jednáním v prostředí informačních a komunikačních technologií (dále IT) se zaměřením na žáky 2. stupně základních škol. Hlavním cílem teoretické části práce bylo vytvořit přehledný, ucelený a aktuální soubor teoretických vstupů o podvodném jednání v IT prostředí z hlediska protiprávního jednání. Teoretická část vycházela z analýzy odborné literatury, publikací, článků, zákonných norem, metodických doporučení, výzkumných zjištění a dalších relevantních zdrojů. Jednotlivé kapitoly a podkapitoly představovaly dílčí cíle teoretické části a byly seřazeny tak, aby na sebe navazovaly a zároveň v komplexu naplňovaly hlavní cíl. V první kapitole byly tak vymezeny základní pojmy spojené s IT, podvodným jednáním a kriminalitou. Dále byl popsán historický vývoj podvodů v IT prostředí. Třetí kapitola se zabývala trestněprávní stránkou podvodného jednání z hlediska právní úpravy České republiky. Další kapitola popsala jednotlivé formy podvodných praktik v IT prostředí s přesahem na podvodné formy zaměřené na seniory. Pátá kapitola se věnovala samotným pachatelům, jejich obětem a odpovědností žáků základních škol za podvodné jednání. Poslední kapitola teoretické části se zabývala preventivním působením před tímto druhem kriminality na úrovni státu, školy, rodiny a vybraných subjektů. Veškeré stanovené cíle teoretické části se podařilo splnit.

V empirické části bylo hlavním cílem zjistit u vybraných žáků 6. a 9. tříd základních škol 2. stupně v Prostějově, zda znají rizika podvodného jednání v IT prostředí, zda se s podvodným jednáním setkali a zda mají v tomto prostředí zkušenosti s obchodováním. V empirické části práce byl nejprve zhodnocen současný stav zkoumané problematiky. Dále bylo charakterizováno realizované výzkumné šetření a popsány a zdůvodněny použité metody. Po stanovení dílčích cílů, deskriptivních problémů, relačních problémů a hypotéz bylo provedeno dotazníkové šetření nejen mezi vybranými žáky základních škol, ale rovněž mezi školními metodiky prevence. Výsledky výzkumného šetření byly přehledně předestřeny v předposlední kapitole č. 10 a poslední kapitola tvořila diskuzi a závěry z výzkumného šetření. Empirické cíle práce byly rovněž splněny.

Nejvyšší podíl ze všech páchaných trestných činů v IT prostředí tvoří podvodná jednání páchaná prostřednictvím internetu. Kyberkriminalita je přitom stále na vzestupu a představuje celosvětový problém. V současné době se navíc komunita pachatelů tohoto druhu kriminality významně změnila. Kolouch (2016, s. 183) uvádí, že se již nejedná o jednotlivce, ale o profesionály, kteří svoji činnost páchají s cílem profitu nebo jsou zapojeni do organizovaného zločinu. Veškerá společnost je závislá na Internetu, přičemž právě kyberkriminalita se stala

výnosným businessem, avšak uživatelé, kteří využívají informační a komunikační technologie, jsou mnohdy pouze minimálně gramotní.

Naprostá většina dnešních žáků základních škol se přitom na internetu běžně pohybuje a nejen že využívá sociální sítě, mobilní telefony a elektronickou komunikaci, mnozí z nich také v tomto prostředí nakupují různé zboží, používají platební karty, přihlašují se k herním účtům, internetovému bankovnictví a přichází do styku prakticky se všemi citlivými údaji jako dospělí, což představuje rizika, kterými se tato práce zabývá. S některými podvodnými praktikami se žáci setkali, setkávají a setkávat budou. Dnes existují podvodné praktiky zaměřené přímo na seniory a vzhledem k neustálému vývoji IT a vývoji podvodných praktik nelze spoléhat na to, že podvodné formy zaměřené přímo na žáky základních škol nevzniknou.

Tato diplomová práce se zabývala riziky v IT prostředí a obohacuje zejména zjištěním aktuálního stavu a informovaností žáků 2. stupně základních škol o dané problematice. Z výsledků práce jasně vyplynulo, že rizikům podvodného jednání v IT prostředí není věnována dostatečná pozornost. Bylo zjištěno, že v naprosté většině chybí preventivní působení na základních školách, minimálně před riziky uvedené v této práci, stejně tak existuje pramálo realizovaných výzkumných šetření a výzkumů v dané oblasti. Přitom každá v této práci uvedená jednotlivá podvodná forma v IT prostředí by mohla být předmětem či námětem samostatného výzkumu nebo vysokoškolské absolventské práce.

Nejdůležitějším elementem v edukaci dětí jsou bezesporu rodiče. O rodiče se ale nelze opírat a doufat, že právě oni budou na své děti v oblasti kyberkriminality preventivně působit a pružně reagovat na veškerá nebezpečí v kyberprostoru. Vývoj IT je velmi progresivní a každý člověk není a nemůže být znalým všeho, a proto hraje klíčovou roli škola.

Erudovaní odborníci navíc klíč ke správné edukaci žáků v této oblasti mají. Jedná se o přímou terénní edukaci včetně představování modelových kazuistik realizovanou externími lektory, kteří se konkrétním tématem intenzivně zabývají a jsou schopni zodpovědět žákům případné dotazy. Pro efektivní primární prevenci je navíc nezbytné ji realizovat v úzké spolupráci s dalšími subjekty, které musí mít v dané oblasti dostatečné vědomosti, znalosti a zkušenosti, což dokazují výzkumy, šetření i praxe.

Jedním z mála projektů, který se takovou edukací a primární prevencí zabývá, je projekt E-Bezpečí. Jeho cílovými skupinami tak nejsou zcela správně pouze žáci základních škol, ale taktéž učitelé, vychovatelé, studenti, preventisté sociálně patologických jevů, metodici prevence, pracovníci OSPOD, policisté, manažeři prevence kriminality a v neposlední řadě také rodiče. Pro všechny tyto cílové skupiny daného projektu, ale rovněž pro další výzkumná šetření a výzkumy, nechť je tato diplomová práce námětem výchovně vzdělávacího účelu.

Seznam použitých zdrojů

Aktuální hrozby a bezpečnostní rizika. In: **Vodafone.cz** [online]. **2018** [cit. 2018-05-08]. Dostupné z: https://www.vodafone.cz/pece/osobni-a-firemni/otazky/bezpecnost/aktualni-hrozby/?page=0

Android version market share distribution among smartphone owners as of September 2017. In: **Statista – The portal for statistics** [online]. Hamburg: statista. **2017** [cit. 2017-12-10]. Dostupné z: https://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/

Aukro.cz [online]. 2018 [cit. 2018-01-07]. Dostupné z: https://aukro.cz

BÉLÍK, Václav a Stanislava HOFERKOVÁ. Prevence rizikového chování ve školním prostředí: pro studenty pomáhajících oborů. Brno: Tribun EU, 2016. ISBN 978-80-263-1015-0.

BRITZ, Marjie. Computer forensics and cyber crime: an introduction. Third Edition. Boston: Pearson, 2013. ISBN 978-0-13-267771-4.

BUCKLEY, Sean. Google says the best phishing scams have a 45-percent success rate. In: Engadget.com [online]. 2014 [cit. 2017.11. 15]. Dostupné z: https://www.engadget.com/2014/11/08/google-says-the-best-phishing-scams-have-a-45-percent-success-r/

Certifikovaní poskytovatelé. In: **Národní ústav pro vzdělávání** [online]. **2018** [cit. 2018-02-22]. Dostupné z: http://www.nuv.cz/modules/catalog//index.php?h=product&id_catalog=15&search%5Bproduct_name%5D=&attributeData%5B40%5D=&attributeData%5B33%5D%5B%5D=100&attributeData%5B33%5D%5B%5D=101&attributeData%5B33%5D%5B%5D=102&attributeData%5B29%5D%5B%5D=63&attributeData%5B30%5D%5B%5D=82&filter=filtruj

Čtyři z deseti Čechů nakupují v čínských e-shopech, počet okradených meziročně stoupl. In: **ESET** [online]. **2017** [cit. 2018-03-24]. Dostupné z: https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy1/tiskove-zpravy/ctyri-z-deseti-cechu-nakupuji-v-cinskych-e-shopech-pocet-okradenych-mezirocne-stoupl/

E-bezpečí pro seniory. In: **E-bezpečí** [online]. **2016** [cit. 2017-12-17]. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/1228

E-bezpečí pro seniory. In: **E-bezpečí** [online]. **2017** [cit. 2017-12-17]. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/1228

EIBENSTEINER, Jiří. Komunikace žáků 8. a 9. tříd v prostředí internetu. Brno, 2015. Diplomová práce. Masarykova Univerzita, Pedagogická fakulta. Vedoucí práce PhDr. Josef Lukas, Ph. D.

ECKERTOVÁ, Lenka a Daniel DOČEKAL. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. 1. vyd. Brno: Computer Press, 2013. 224 s. ISBN 978-80-251-3804-5

FISCHER, Slavomil a Jiří ŠKODA. Sociální patologie: závažné sociálně patologické jevy, příčiny, prevence, možnosti řešení. 2., rozš. a aktualiz. vyd. Praha: Grada, 2014. Psyché. ISBN 978-80-247-5046-0.

FISCHER, Slavomil a Jiří ŠKODA. Sociální patologie: analýza příčin a možnosti ovlivňování závažných sociálně patologických jevů. Vyd. 1. Praha: Grada, 2009. 218 s. Psyché. ISBN 978-80-247-2781-3.

GAVORA, Peter. Úvod do pedagogického výskumu. 4. vydání. Bratislava: Univerzita Komenského, 2008. 272 s. ISBN 978-80-223-2391-8.

GIANNAKOURIS, Konstantinos. Ageing characterises the demographic perspectives of the European societies. Eurostat Statistic in focuc. In: Eurostat [online]. 2008 [cit. 2017-12-17]. Dostupné z: http://ec.europa.eu/eurostat/web/products-statistics-in-focus/-/KS-SF-08-072

Global spam volume as percentage of total e-mail traffic from 2007 to 2016. In: **Statista – The portal for statistics** [online]. **2018a** [cit. 2018-03-24]. Dostupné z: https://www.statista.com/statistics/420400/spam-email-traffic-share-annual/

Global spam volume as percentage of total e-mail traffic from January 2014 to September 2017, by month**.** In: **Statista – The portal for statistics** [online]. **2018b** [cit. 2018-03-24]. Dostupné z: https://www.statista.com/statistics/420391/spam-email-traffic-share/

GŘIVNA, Tomáš a Radim POLČÁK (eds). Kyberkriminalita a právo. Praha: Auditorium, 2008, ISBN 978-80-9037-867-4.

HEJDUKOVÁ, Martina. Platební styk. Hradec Králové, 2017. Bakalářská práce. Univerzita Hradec Králové, Fakulta informatiky a managementu. Vedoucí práce Ing. Jaroslava Dittrichová, Ph.D.

HONUS, Aleš. Platíme až 30 Kč za obálku, lákal inzerát. Podvodník obral 17 tisíc lidí o milióny. In: Novinky.cz [online]. 2016 [cit. 2017-12-07]. Dostupné z: http://www.novinky.cz/krimi/392358-platime-az-30-kc-zaobalku- lakal-inzerat-podvodnik-obral-17-tisic-lidi-o-miliony.html

CHALUPOVÁ, Kateřina, Michaela ŠTEFUNKOVÁ a Jaroslav ŠEJVL. Základy prevence kriminality pro pedagogické pracovníky. Praha: Klinika adiktologie, 1. lékařská fakulta Univerzity Karlovy v Praze a Všeobecná fakultní nemocnice v Praze. Togga, 2012. Monografie. ISBN 978-80-87258-96-5.

Channel collision: drivers of online and in-store shopping are not as sharply divided as you think In: **Gfk.com** [online]. **2016** [cit. 2018-01-11]. Dostupné z: http://www.gfk.com/insights/press-release/drivers-of-online-and-in-store-shopping-are-not-as-sharply-divided-as-you-think/

CHRÁSKA, Miroslav. Metody pedagogického výzkumu: základy kvantitativního výzkumu. 2., aktualizované vydání. Praha: Grada, 2016. 254 stran. Pedagogika. ISBN 978-80-247-5326-3.

Informace o projektu. In: **E-Bezpečí** [online]. **2008-2018** [cit. 2018-02-27]. Dostupné z: https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu

Informace o projektu. In: **Kraje pro bezpečný internet** [online]. 2018 [cit. 2018-05-25]. Dostupné z: http://www.kpbi.cz/o-projektu

JANÁKOVÁ, Barbora. Internetoví podvodníci loni připravili Čechy o 1,2 miliardy. In: Novinky.cz [online]. 2015 [cit. 2017-12-07]. Dostupné z: https://www.novinky.cz/internet-a-pc/378544-internetovi-podvodnici-loni-pripravili-cechy-o-1-2-miliardy.html

JANOUŠ, Vilém. Šmejdi se zdokonalují. Okrádají na internetu. In: deník.cz [online]. 2014 [cit. 2017-12-17]. Dostupné z: https://www.denik.cz/z_domova/smejdi-se-zdokonaluji-okradaji-na-internetu-20141126.html

JANSA, Lukáš, Petr OTEVŘEL, Jiří ČERMÁK, Petr MALIŠ, Petr HOSTAŠ, Michal MATĚJKA a Ján MATEJKA. Internetové právo. Brno: Computer Press, 2016. ISBN 978-80-251-4664-4.

Jednotlivé druhy kyberkriminality. In: **Policie ČR** [online]. **2017** [cit. 2018-01-14]. Dostupné z: http://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti. 2. aktualizované vyd. Praha: AFCEA, 2015. ISBN 978-80-7251-39m7-0.

JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

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

KOPECKÝ, Kamil. Co je Hoax. In: E-Bezpečí [online]. 2008 [cit. 2017-12-20]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/hoax-spam/91-25

KOPECKÝ, Kamil, René SZOTKOWSKI a Veronika KREJČÍ. Nebezpečí internetové komunikace III. 1. vyd. Olomouc: Pedagogická fakulta, Univerzita Palackého v Olomouci, 2012. 60 s. ISBN 978-80-244-3087-4.

KOPECKÝ, Kamil. Podvodné mobilní platby na Facebooku. In: E-bezpeci.cz [online]. 2013 [cit. 2018-01-16]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/sociotechnika/774-podvodne-platby-na-facebooku

KOPECKÝ, Kamil a René SZOTKOWSKI. Senioři jako oběti internetové kriminality. In: E-Bezpečí [online]. Olomouc: Univerzita Palackého v Olomouci. 2013 [cit. 2017-12-17]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/dali-rizika/1058-seniori-jako-obeti

KOPECKÝ, Kamil. Senioři jako oběti internetové kriminality. In: E-Bezpečí [online]. 2015a [cit. 2017-12-17]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/dali-rizika/1058-seniori-jako-obeti

KOPECKÝ, Kamil. České děti a Facebook 2015 výzkumná zpráva [online]. 2015b [cit. 2018-01-16]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/cat_view/27-

KOPECKÝ, Kamil a kol. Rizikové formy chování českých a slovenských dětí v prostředí internetu. 1. vydání. Olomouc: Univerzita Palackého v Olomouci, 2015. 169 stran. Monografie. ISBN 978-80-244-4861-9

KOPECKÝ, Kamil. Romance Scams opět řádí – terčem jsou tradičně senioři. In: E-Bezpečí [online]. 2016 [cit. 2017-12-17]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/sociotechnika/1156-romance-scam

KOPECKÝ, Kamil. Modrá velryba – hra motivující děti k sebevražednému jednání? Obyčejný podvod. In: E-Bezpečí [online]. 2017a [cit. 2017-12-20]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/socialni-sit/1230-modra-velryba

KOPECKÝ, Kamil. U dětí 1. stupně ZŠ dominuje YouTube. Facebook jej předežene až ve 14 letech věku dítěte. In: E-Bezpeci.cz [online]. 2017b [cit. 2018-01-16]. Dostupné z: https://www.e-bezpeci.cz/index.php/veda-a-vyzkum/1256-facebook-vs-youtube

KOPECKÝ, Kamil. Klonování profilů jako klasická invazivní technika funguje velmi dobře na děti. V polovině případů si neověřují, zda je o přátelství žádají skutečně jejich spolužáci a kamarádi z reálného světa. In: E-Bezpeci.cz [online]. 2017c [cit. 2018-01-16]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/sociotechnika/1253-klonovani-profilu

KOTÁSEK, Jiří a kol. Národní program rozvoje vzdělávání v České republice: bílá kniha. [Praha]: Tauris, 2001. 98 s. ISBN 80-211-0372-8.

KUCHTA, Josef. Kurs trestního práva: trestní právo hmotné: zvláštní část. V Praze: C.H. Beck, 2009. Právnické učebnice. ISBN 978-80-7400-047-8.

KUCHTA, Josef. Aktuální problémy počítačové kriminality včetně její prevence. Časopis pro právní vědu a praxi. [Online]. 2016, č. 1, s. 5-19. [cit. 2017-10-29]. Dostupné z: https://journals.muni.cz/cpvp/article/view/5260

KSHETRI, Nir. The global cybercrime industry: economic, institutional and strategic perspectives. London: Springer, 2010. ISBN 978-3-642-11521-9.

KRAUS, Blahoslav a Jolana HRONCOVÁ. Sociální patologie. Vyd. 2. Hradec Králové: Gaudeamus, 2010. ISBN 978-80-7435-080-1.

KRČMÁŘOVÁ, Barbora. Děti a online rizika: sborník studií. Praha: Sdružení Linka bezpečí, 2012. ISBN 978-80-904920-2-8.

Kyberkriminalita: O stránkách. In: **Prevence kriminality v České republice** [online]. **2018** [cit. 2018-02-22]. Dostupné z: http://www.prevencekriminality.cz/kyberkriminalita-testovaci-provoz/o-strankach/

Kyberkriminalita. In: **Policie ČR** [online]. **2018a** [cit. 2018-02-15]. Dostupné z: http://www.policie.cz/clanek/kyberkriminalita.aspx

MACALÍKOVÁ, Jana. Objevuje se vám na monitoru podezřelé hlášení? In: Policie ČR [online]. 2013 [cit. 2017-12-10]. Dostupné z: http://www.policie.cz/clanek/objevuje-se-vam-na-monitoru-podezrele-hlaseni.aspx

MATĚJKA, Michal. Počítačová kriminalita. Praha: Computer Press, 2002. ISBN 80-7226-419-2.

MATOUŠKOVÁ, Ingrid. Aplikovaná forenzní psychologie. Praha: Grada, 2013, Psyché (Grada). ISBN 978-80-247-4580-0.

MATZNER, Jiří. Falešné e-shopy - 1000 podvedených. In: Policie ČR [online]. 2016 [cit. 2018-01-14]. Dostupné z: http://www.policie.cz/clanek/falesne-e-shopy-1000-podvedenych.aspx

MCCARTHY, Linda a Denise WELDON-SIVIY. Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online. Praha: CZ.NIC, 2013. ISBN 978-80-904248-6-9.

Metodické doporučení k primární prevenci rizikového chování u dětí, žáků a studentů ve školách a školských zařízeních. In: **MŠMT** [online]. **2010** [cit. 2018-02-16]. Dostupné z: http://www.msmt.cz/vzdelavani/socialni-programy/metodicke-dokumenty-doporuceni-a-pokyny

MIOVSKÝ, Michal a kol. Primární prevence rizikového chování ve školství: [monografie. Vyd. 1. Praha: Sdružení SCAN, 2010. 253 s. ISBN 978-80-87258-47-7.

MIOVSKÝ, Michal a kol. Výkladový slovník základních pojmů školské prevence rizikového chování. Druhé, přepracované a doplněné vydání. Praha: Klinika adiktologie 1. LF UK v Praze a VFN v Praze, 2015. 272 stran. Monografie. ISBN 978-80-7422-391-4.

MUSIL, Stanislav. Počítačová kriminalita: nástin problematiky: kompendium názorů specialistů. Praha: Institut pro kriminologii a sociální prevenci, 2000, ISBN 80-86008-80-0.

Na Česko zaútočili prozváněcí podvodníci. In: **Echo24.cz** [online]. **2017** [cit. 2018-01-123]. Dostupné z: https://echo24.cz/a/iSeUw/na-cesko-zautocili-prozvaneci-podvodnici

Národní strategie primární prevence rizikového chování dětí a mládeže na období 2013-2018. In: **MŠMT** [online]. **2013** [cit. 2018-02-16]. http://www.msmt.cz/file/28077

NEWMAN, Lucy. Six teens arrested for virtual crime in Habbo Hotel. In: Technologytell [online]. 2007 [cit. 2017-11-15]. Dostupné z: http://www.technologytell.com/gaming/18923/six-teens-arrested-for-virtual-crime-in-habbo-hotel/

NOVÁKOVÁ, Martina. Senioři v roli oběti a svědka trestného činu. In: Bezpečnostní sbory.cz [online]. 2013 [cit. 2017-12-17]. Dostupné z: http://bezpecnostni-sbory.wbs.cz/clanky/2-2013/seniori_v_roli_obeti.pdf

Odbor prevence kriminality. In: **MVČR** [online]. **2018b** [cit. 2018-02-22]. Dostupné z: http://www.mvcr.cz/clanek/odbor-prevence-kriminality.aspx

O projektu. In: **Bezpečně-online.cz** [online]. **2018** [cit. 2018-02-27]. Dostupné z: https://bezpecne-online.saferinternet.cz/uvod/o-projektu

O projektu. In: **Bezpečný internet.cz** [online]. 2018 [cit. 2018-02-27]. Dostupné z: http://www.bezpecnyinternet.cz/o-projektu/default.aspx

O projektu. In: **Saferinternet.cz** [online]. **2018** [cit. 2018-02-27]. Dostupné z: https://www.saferinternet.cz/info-o-nás/o-nás.html

O nás. In: **Linkabezpečí.cz** [online]. **2018** [cit. 2018-02-27]. Dostupné z: http://spolek.linkabezpeci.cz/o-nas/

O nás. In: **CSIRT.cz** [online]. **2018** [cit. 2018-02-27]. Dostupné z: https://www.csirt.cz/page/3471/o-tymu-csirtcz/

O nás. In: **Národní Centrum Bezpečnějšího internetu** [online]. **2012** [cit. 2018-02-27]. Dostupné z: http://www.ncbi.cz/cs/

O projektu. In: **E-SYNERGIE** [online]. **2011** [cit. 2018-02-22]. Dostupné z: http://www.esynergie.upol.cz/index.php/o-projektu

OREL, Ladislav. Problematika malware a znalost škodlivého kódu u žáků základních škol. Olomouc, 2016. Bakalářská práce. Univerzita Palackého v Olomouci, Pedagogická fakulta, Katedra technické a informační výchovy. Vedoucí práce doc. PhDr. Miroslav Chráska, Ph. D.

OŠKRDALOVÁ, Gabriela. Modelování bezpečnostních rizik elektronického obchodu a elektronického bankovnictví. Brno, 2012. Dizertační práce. Masarykova Univerzita v Brně.

PERDOCH, Jaroslav. Podvodník ženě z Ostravy vybílil účet. Zneužil k tomu sociální síť. In: Moravskoslezsky.denik.cz [online]. 2014 [cit. 2018-01-16]. Dostupné z: https://moravskoslezsky.denik.cz/zlociny-a-soudy/podvodnik-zene-vybilil-ucet-zneuzil-k-tomu-socialni-sit-20141124.html

POZOR! Změna produktových podmínek k 15. 9. 2017. In: **Penezenka.blesk.cz** [online]. **2017** [cit. 2018-01-16]. Dostupné z: http://penezenka.blesk.cz/clanek/ostatni-blesk-penezenka-akce/481206/pozor-zmena-produktovych-podminek-k-15-9-2017

PORADA, Viktor a Jiří STRAUS. Kriminalistika: (výzkum, pokroky, perspektivy). Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013. ISBN 978-80-738-0477-0.

POTŮČEK, Jan. Internet v mobilu používá každý druhý Čech, před viry ho chrání jen každý čtvrtý. In: Novinky.cz [online]. 2017 [cit. 2018-05-06]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/456279-internet-v-mobilu-pouziva-kazdy-druhy-cech-pred-viry-ho-chrani-jen-kazdy-ctvrty.html

Projekt "Buď v bezpečí" – problematika kyberšikany. In: **Policie ČR** [online]. **2016** [cit. 2018-02-22]. Dostupné z: http://www.policie.cz/clanek/projekt-bud-v-bezpeci-problematika-kybersikany.aspx

PRŮCHA, Jan, Jiří MAREŠ a Eliška WALTEROVÁ. Pedagogický slovník. 4., aktualiz. vyd. Praha: Portál, 2003. ISBN 80-7178-772-8.

PRŮCHA, Jan, Eliška WALTEROVÁ a Jiří MAREŠ, Jiří. Pedagogický slovník. 7., aktualiz. a rozš. vyd. Praha: Portál, 2013. 395 s. ISBN 978-80-262-0403-9.

PRŮCHA, Jan a Jaroslav VETEŠKA. Andragogický slovník. 2., aktualiz. a rozš. vyd. Praha: Grada, 2014. ISBN 978-80-247-4748-4.

Příchod hackerů: nigerijský scam „419“. In: **Root.cz** [online]. **1998–2017** [cit. 2017-12-11]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-nigerijsky-scam-419/

RAK, Roman a Viktor PORADA. Kybernetická kriminalita. Praha [Karlovy Vary]: Vysoká škola Karlovy Vary, 2013. ISBN 978-80-87236-16-1.

Rejstřík škol a školských zařízení. In: MŠMT [online]. 2018 [cit. 2018-02-27]. Dostupné z: https://profa.uiv.cz/rejskol/

Republikový výbor pro prevenci kriminality. In: **MVČR** [online]. **2018a** [cit. 2018-02-22]. Dostupné z: http://www.mvcr.cz/clanek/rvppk-republikovy-vybor-pro-prevenci-kriminality.aspx

SASÍNOVÁ, Petra. Falešný vnuk lákal od žen úspory. In: iDnes.cz [online]. 2003 [cit. 2017-12-15]. Dostupné z: https://zpravy.idnes.cz/falesny-vnuk-lakal-od-zen-uspory-dot-/krimi.aspx?c=A030805_160307_krimi_jan

SCAM419. In: **Hoax.cz** [online]. **2000-2017** [cit. 2017-12-11]. Dostupné z: http://www.hoax.cz/scam419/

SEDLÁČEK, Jiří. E-komerce, internetový a mobil marketing od A do Z. 1. vyd. Praha: BEN - technická literatura, 2006. 351 s. ISBN 80-7300-195-0.

Senioři. In: **Český statistický úřad** [online]. **2017a** [cit. 2017-12-15]. Dostupné z: https://www.czso.cz/csu/czso/seniori

SHINDER, Debra Littlejohn. Scene of the Cybercrime: Computer Forensics Handbook, USA: Syngress Publishing, 2002. ISBN: 1-931836-65-5.

Slovník. In: **Bezpečný internet.cz** [online]. **2017** [cit. 2017-12-10]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/default.aspx

SMEJKAL, Vladimír, Tomáš SOKOL a Martin VLČEK. Počítačové právo. Praha: C. H. Beck, 1995. Právo a hosp. ISBN 80-7049-101-9.

SMEJKAL, Vladimír. Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. Trestněprávní revue, roč. 6/2003. s 161-167. ISSN 1213-5313.

SMEJKAL, Vladimír. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. ISBN 978-80-7380-501-2.

SMOLÍK, Josef a Alena KAJANOVÁ. Prevence kriminality páchané na seniorech pohledem studujících univerzity třetího věku [online]. 2012 [cit. 2017-12-17]. Dostupné z: http://casopis-zsfju.zsf.jcu.cz/prevence-urazu-otrav-a-nasili/clanky/1~2012/192-prevence-kriminality-pachane-na-seniorech-pohledem-studujicich-univerzity-tretiho-veku

Spam and phishing in 2017. In: **Securelist.com** [online]. **2018** [cit. 2018-03-24]. Dostupné z: https://securelist.com/spam-and-phishing-in-2017/83833/

Statistiky kriminality – dokumenty. Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2014 (ve srovnání s rokem 2013). In: **MVČR** [online]. **2015** [cit. 2017-12-16]. Dostupné z: http://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx

Statistiky kriminality – dokumenty. Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2016 (ve srovnání s rokem 2015). In: **MVČR** [online]. **2017** [cit. 2017-12-16]. Dostupné z: http://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx

Statistika skimmingu. In: **Policie ČR** [online]. **2018c** [cit. 2018-03-24]. Dostupné z: http://www.policie.cz/clanek/statistika-skimmingu.aspx

Statistické přehledy kriminality za rok 2017. In: **Policie ČR** [online]. **2018b** [cit. 2017-03-23]. Dostupné z: http://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2017.aspx

Statistiky řešených incidentů. IN: **CSIRT.CZ** [online]. **2018** [cit. 2017-12-15]. Dostupné z: https://www.csirt.cz/page/2635/statistiky-resenych-incidentu/

STRAŠILOVÁ, Petra. Malware obsažený ve falešných exekučních výzvách. In: Policie ČR [online]. 2014 [cit. 2017-12-11]. Dostupné z: http://www.policie.cz/clanek/malware-obsazeny-ve-falesnych-exekucnich-vyzvach.aspx

Strategie vzdělávací politiky České republiky do roku 2020. In: **MŠMT** [online]. **2014a** [cit. 2018-02-16]. Dostupné z: http://www.msmt.cz/uploads/Strategie_2020_web.pdf

Strategie digitálního vzdělávání do roku 2020. IN: **MŠMT** [online]. **2014b** [cit. 2018-02-27]. Dostupné
z: http://www.vzdelavani2020.cz/images_obsah/dokumenty/strategie/digistrategie.pdf

Strategie prevence kriminality v České republice na léta 2016 až 2020. In: **MVČR** [online]. **2016** [cit. 2018-02-22]. Dostupné z: http://www.mvcr.cz/clanek/strategie-prevence-kriminality-v-ceske-republice-na-leta-2016-az-2020.aspx

ŠÁMAL, Pavel. Trestní zákoník: komentář. Praha: C. H. Beck, 2009. Velké komentáře. ISBN 978-80-7400-109-3.

ŠIMÍČKOVÁ ČÍŽKOVÁ, Jitka et al. Přehled vývojové psychologie. 2. vyd. Olomouc: Unverzita Palackého v Olomouci, 2008. 175 s. ISBN 978-80-244-2141-4

ŠTEINEROVÁ, Jana. Falešný vnuk požadované finance nezískal. In: Policie ČR [online]. 2017 [cit. 2017-12-15]. Dostupné z: http://www.policie.cz/clanek/or-kladno-zpravodajstvi-falesny-vnuk.aspx

ŠVEC, Štefan a kol. Metodológia vied o výchove : kvantitatívno-scientické a kvalitatívno-humanitné prístupy v edukačním výskume. Bratislava : Vydavateľstvo Iris,1998, 303 s. ISBN 80-88778- 73-5.

TOMÁŠEK, Jan. Úvod do kriminologie: jak studovat zločin. Vyd. 1. Praha: Grada, 2010. 214 s. ISBN 978-80-247-2982-4.

UNESCO. Developing and Using Indicators of ICT Use in Education [online]. Bangkok: UNESCO Asia and Pacific Regional Bureau for Education. 2003. 49 s. [cit. 2017-09-05]. Dostupné http://www.unescobkk.org/fileadmin/user_upload/ict/e-books/ICTedu/ictedu.pdf

Usnesení Nejvyššího soudu ČR ze dne 18. února 2015, sp. zn. 5 Tdo 1630/2014. Kraken.slv.cz [online]. 2015a [cit. 2017-12-07]. Dostupné z: http://kraken.slv.cz/5Tdo1630/2014

Usnesení Nejvyššího soudu ČR ze dne 13. května 2015, sp. zn. 8 Tdo 518/2015. Kraken.slv.cz [online]. 2015b [cit. 2017-12-07]. Dostupné z: http://kraken.slv.cz/8Tdo518/2015

Usnesení Nejvyššího soudu ČR ze dne 2. července 2015, sp. zn. 7 Td 33/2015. Kraken.slv.cz [online]. 2015c [cit. 2017-12-07]. Dostupné z: http://kraken.slv.cz/7Td33/2015

Usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky

VÁLKOVÁ, Helena a Josef KUCHTA. Základy kriminologie a trestní politiky. 2. vyd. V Praze: C. H. Beck, 2012. Beckovy mezioborové učebnice. ISBN 978-80-7400-429-2.

V dubnu přibývalo detekcí exploitu DoublePulsar, šiřitele ransomwaru WannaCry. In: **ESET** [online]. **2018** [cit. 2018-05-06]. Dostupné z: https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/v-dubnu-pribyvalo-detekci-exploitu-doublepulsar-siritele-ransomwaru-wannacry/

VENGLÁŘOVÁ, Martina. Senioři: prevence. Příloha časopisu Policista. IN: MVČR [online] 2007 (6). [cit. 2017-12-17]. Dostupné z: http://www.mvcr.cz/clanek/policista-626975.aspx?q=Y2hudW09NA%3d%3d

VOŘÍŠEK, Lukáš. Phishing v praxi, aneb jak jsem nachytal české studenty. In: CDR.cz [online]. 2012 [cit. 2017-12-15]. Dostupné z: https://cdr.cz/clanek/phishing-jak-jsem-nachytal-ceske-studenty-nova-maturita

Vyhláška č. 72/2005 Sb., o poskytování poradenských služeb ve školách a školských poradenských zařízeních

VYHLÍDAL, Martin. Majetková kriminalita na internetu. Olomouc. 2014. Bakalářská práce. Univerzita Palackého v Olomouci, Pedagogická fakulta. Vedoucí práce PhDr. René Szotkowski, Ph.D.

Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci za období 2017. In: **Český statistický úřad** [online]. **2017b** [cit. 2018-01-08]. Dostupné z: https://www.czso.cz/documents/10180/46014700/06200417.pdf/a0bd4497-d2b6-450b-95f0-2f70c50786d5?version=1.1

Vývoj obratu v e-commerce od roku 2013. In: **APEK.cz** [online]. **2017** [cit. 2018-01-10]. Dostupné z: https://www.apek.cz

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů.

Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů, ve znění pozdějších předpisů.

Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, ve znění pozdějších předpisů.

Zákon č. 251/2016 Sb., o některých přestupcích, ve znění pozdějších předpisů.

Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

Zákon č. 141/1961 Sb., o trestní řízení soudním (trestní řád), ve znění pozdějších předpisů.

Zákon č. 359/1999 Sb., o sociálně-právní ochraně dětí, ve znění pozdějších předpisů.

Zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), ve znění pozdějších předpisů.

ZOUBKOVÁ, Ivana. Kriminologický slovník. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2011, ISBN 978-807-3803-124.

ZOUNEK, Jiří a Klára ŠEĎOVÁ. Učitelé a technologie: mezi tradičním a moderním pojetím. Brno: Paido, 2009. ISBN 978-80-7315-187-4.

ŽÍDEK, Bohumír. V Česku řádí noví internetoví podvodníci. Jak jim nenaletět? In: Novinky.cz [online]. 2018 [cit. 2018-01-13]. Dostupné z: https://www.novinky.cz/ekonomika/459805-v-cesku-radi-novi-internetovi-podvodnici-jak-jim-nenaletet.html

Seznam zkratek

APEK – Asociace pro elektronickou komerci

CSIRT – Computer Security Incident Response Team

ČR – Česká republika

LZPS – Listina základních práv a svobod

MŠMT – Ministerstvo školství mládeže a tělovýchovy

MVČR – Ministerstvo vnitra České republiky

NCBI – Národní centrum bezpečnějšího internetu

IT – informační technologie (pro účely této práce informační a komunikační technologie)

ICT – informační a komunikační technologie

OPK – Odbor prevence kriminality (spadající pod Ministerstvo vnitra České republiky)

OSPOD – Orgán sociálně-právní ochrany dětí

OSN – Organizace spojených národů

PDA – Personal Digital Assistant (osobní digitální asistent)

Pdf – Pedagogická fakulta

RVP – Rámcový vzdělávací program

RVP ZV – Rámcový vzdělávací program pro základní vzdělávání

Sb. – Sbírka zákonů

SŠ – střední škola

ŠVP – školní vzdělávací program

URL – Uniform Resource Locator (soubor znaků sloužících k identifikaci přesného umístění informací na internetu)

UPOL – Univerzita Palackého v Olomouci

UNESCO – Organizace OSN pro vzdělávání, vědu a kulturu

ZŠ – základní škola

Seznam grafů

Seznam tabulek

Seznam obrázků

Seznam příloh

Příloha č. 1 – původní dotazník pro žáky základních škol použitý při pilotní studii.

Vážení žáci,

v České republice je zaznamenáván každým rokem nárůst podvodů páchaných prostřednictvím informačních a komunikačních technologií, zejména na internetu. Dané důvody nás vedly k provedení dotazníkového šetření na podobné téma.

Získané informace budou využity pro zjištění aktuálního stavu v oblasti prevence před uvedenou kriminalitou, proto Tě prosíme o úplné a pravdivé vyplnění tohoto anonymního dotazníku. Při jeho vyplňování se řiď pokyny v závorkách. Děkujeme za spolupráci.

Za výzkumný tým Michal Jančík, policista vyšetřující trestnou činnost a zároveň student Pedagogické fakulty, Univerzity Palackého v Olomouci, obor Veřejná správa.

1. **Máš možnost někomu přes internet poslat peníze na bankovní účet, např. zaplatit za hru nebo elektroniku?** (Můžeš zakřížkovat i více odpovědí)

	Ano, internetovým bankovnictvím.		Ano, vlastní platební kartou.
	Ano, platební kartou rodičů.		Ano, platební kartou kamaráda.
	Ano, platební kartou dědečka/babičky.		Já sám ne.
	Ano, přes Paypal, Gopay, PayU apod.		Nevím.

2. **Vlastníš platební kartu?** (Zakřížkuj jednu odpověď)

	ANO		NE

3. **Platil/a jsi někdy platební kartou?** (Zakřížkuj jednu odpověď)

	ANO		NE

4. **Pokud jsi platil/a někdy platební kartou, kde to bylo?** (Můžeš zakřížkovat i více odpovědí)

	Na internetu, za nákup v obchodě (e-shopu).		V obchodě.
	Na internetu, za nákup přes inzerát v bazaru.		V restauraci.
	Na internetu, za nákup v aukci.		Na poště nebo někde jinde.
	Na internetu, za nákup počítačové hry.		Nikdy jsem neplatil/a platební kartou.

5. **Přihlašoval/a ses někdy k bankovnímu účtu na internetu (internetové bankovnictví)?** (Můžeš zakřížkovat i více odpovědí)

	Ano, k vlastnímu bankovnímu účtu.		Ano, k bankovnímu účtu dědečka/babičky.
	Ano, k bankovnímu účtu rodičů.		Ano, k bankovnímu účtu někoho jiného.
	Ano, k bankovnímu účtu kamaráda.		Ne.

6. **Chtěl/a jsi někdy něco koupit přes internet, např. hru, mobil, tablet, oblečení?** (Zakřížkuj jednu odpověď)

	ANO		NE
	NEVÍM		

7. **Koupil/a jsi někdy něco přes internet?** (Můžeš zakřížkovat i více odpovědí)

	Ano, hry.		Ano, sportovní věci.
	Ano, vylepšení do her.		Ano, hračky.
	Ano, elektroniku.		Ano, jiné věci.
	Ano, oblečení.		Nenakupoval/a jsem přes internet.

8. **Nakupoval/a jsi někdy v internetové aukci, např. na Aukru?** (Můžeš zakřížkovat i více odpovědí)

	Ano, sám/a jsem nakupoval/a.		Ano, s kamarádem jsem nakupoval/a.
	Ano, s rodičem jsem nakupoval/a.		Ano, s někým jiným jsem nakupoval/a.
	Ano, s dědečkem/babičkou jsem nakupoval/a.		Nenakupoval/a jsem.

9. **Nakupoval/a jsi někdy v internetovém bazaru, např. Bazoš?** (Můžeš zakřížkovat i více odpovědí)

	Ano, sám/a jsem nakupoval/a.		Ano, s kamarádem jsem nakupoval/a.
	Ano, s rodičem jsem nakupoval/a.		Ano, s někým jiným jsem nakupoval/a.
	Ano, s dědečkem/babičkou jsem nakupoval/a.		Nenakupoval/a jsem.

10. **Nakupoval/a jsi někdy v internetovém obchodě (e-shopu), např. Alza, TS Bohemia, MALL apod.?** (Můžeš zakřížkovat i více odpovědí)

	Ano, sám/a jsem nakupoval/a.		Ano, s kamarádem jsem nakupoval/a.
	Ano, s rodičem jsem nakupoval/a.		Ano, s někým jiným jsem nakupoval/a.
	Ano, s dědečkem/babičkou jsem nakupoval/a.		Nenakupoval/a jsem.

11. **Máš nějaký svůj herní účet?** (Můžeš zakřížkovat i více odpovědí)

	Ano, Steam		Ano, App store.
	Ano, Playstation Network.		Ano, Microsoft Store.
	Ano, Xbox Live.		Ano, mám ale jiný účet.
	Ano, Google Play.		Ne, nemám žádný podobný herní účet.

12. **Nakupoval/a jsi někdy něco přes nějaký herní účet např. přes Steam, Origin, PlayStation Network, Xbox Live, Google play apod.?** (Můžeš zakřížkovat i více odpovědí)

	Ano, sám/a jsem tam nakupoval/a.		Ano, s kamarádem jsem tam nakupoval/a.
	Ano, s rodičem jsem tam nakupoval/a.		Ano, s někým jiným jsem tam nakupoval/a.
	Ano, s dědečkem/babičkou jsem nakupoval/a.		Nenakupoval/a jsem.

13. **Nakupoval/a jsi někdy nějaké vylepšení (mikrotrasakce) do počítačové hry? Např. do League of Legends, World of Tank nebo jiné hry.** (Můžeš zakřížkovat i více odpovědí)

	Ano, sám/a jsem si to koupil/a.		Ano, ale někdo jiný mi to koupil.
	Ano, ale rodiče mi to koupili.		Ano, sám/a jsem si to koupil/a, bez vědomí rodičů, z jejich platební karty.
	Ano, ale dědeček/babička mi to koupili.		Ano, sám/a jsem si to koupil/a, bez vědomí dědečka/babičky, z jejich platební karty.
	Ano, ale kamarád mi to koupili.		Nenakupoval/a jsem nic takového.

14. **Pokud jsi nakoupil/a něco přes internet, kdo zboží zaplatil?** (Můžeš zakřížkovat i více odpovědí)

	Sám.		Kamarád.
	Rodiče.		Někdo jiný.
	Dědeček/babička.		Nenakupoval/a jsem přes internet.

15. **Ověřuješ si nějak internetový obchod (e-shop) před nákupem zboží?** (Můžeš zakřížkovat i více odpovědí)

	Neověřuji.		Ano, čtu si obchodní podmínky.
	Neověřuji, nevím, jak a kde.		Ano, předem telefonuji na kontakt.
	Ano, hledám a čtu si jeho hodnocení.		Ano, hledám jak dlouho e-shop existuje.
	Ano, hledám o něm informace na internetu.		Nenakupuji v e-shopech.

16. Ověřuješ si prodejce na internetovém bazaru před nákupem zboží?(Můžeš zakřížkovat i více odpovědí)

	Neověřuji.		Ano, hledám a čtu si hodnocení prodejce.
	Neověřuji, nevím ani jak.		Ano, dotazuji se na možnost osobního převzetí.
	Neověřuji, komunikuji jen přes email.		Ano, telefonuji na kontakt, vyptávám se na zboží.
	Ano, prohlížím si i další nabídky prodejce.		Nenakupuji v internetových bazarech.

17. Ověřuješ si prodejce internetové aukce před nákupem zboží? (Můžeš zakřížkovat i více odpovědí)

	Neověřuji.		Ano, hledám a čtu si hodnocení prodejce.
	Neověřuji, nevím ani jak.		Ano, dotazuji se na možnost osobního převzetí.
	Neověřuji, komunikuji jen přes email.		Ano, telefonuji na kontakt, vyptávám se na zboží.
	Ano, prohlížím si další nabídky prodejce.		Nenakupuji v internetových aukcích.

18. Prodával/a jsi někdy něco přes internet? (Zakřížkuj jednu odpověď)

	ANO		NE

19. Podle čeho bys poznal/a, že jde o podvodný inzerát např. podvodný prodej mobilního telefonu?

Pokud víš, napiš stručnou odpověď:

20. Byl/a jsi někdy podveden/a na internetu? (Můžeš zakřížkovat i více odpovědí)

	Ano, přišel/přišla jsem o peníze nebo jiný majetek (vznikla mi majetková škoda).		Ano, přišel/přišla jsem tím o své osobní údaje, heslo, fotky, videa, apod.
	Ano, ale někdo jiný díky mě přišel o peníze (např. rodiče, dědeček, babička, kamarád).		Ano, někdo se mi naboural do facebookového, herního, bankovního či jiného účtu nebo emailu.
	Ano, mobil, počítač nebo tablet se mi nakazil virem.		Ano, psal mi někdo z falešného profilu na Facebooku.
	Přímo ne, ale přišla mi podvodná zpráva nebo email.		Ne.

21. Setkal/a ses někdy s podvodem při nákupu zboží přes internet? (Můžeš zakřížkovat i více odpovědí)

	Ano, byl/a jsem podveden/a přímo já.		Ne, ale vím o těchto podvodech.
	Ano, podvedli někoho z mého okolí (rodina, kamarád, známý, apod.).		Ne, nesetkal/a jsem se s tím.

22. Přišel Ti někdy nevyžádaný email od neznámého odesílatele (spam)? (Můžeš zakřížkovat i více odpovědí)

	Ano, někdo se chtěl semnou seznámit.		Ano, přišla mi reklama.
	Ano, přišla zpráva, že jsem něco vyhrál/a.		Ano, někdo mi nabízel, že si můžu vydělat peníze
	Ano, přišla podvodná výzva, že dlužím peníze		Ano, přišla, ale týkala se něčeho jiného.
	Ano, přišla mi podvodná faktura k zaplacení.		Ne, nepřišla.
	Ano, přišla mi nějaká nabídka zboží.		Ne, nemám email

23. Pokud jsi obdržel/a takový nevyžádaný email, jak jsi na něj reagoval/a? (Můžeš zakřížkovat i více odpovědí)

	Bez přečtení jsem ho a vymazal/a.		Přečetl/a jsem ho a klikl/a na přílohu nebo odkaz v této zprávě.
	Přečetl/a jsem ho a vymazal/a.		Nepřišel mi žádný takový email.
	Přečetl/a jsem ho a odepsal/a.		Nemám email.

24. Prozvánělo Tě na mobil někdy cizí tel. číslo, na které jsi zatelefonoval/a zpět a přišel/a o peníze? (Zakřížkuj jednu odpověď)

	ANO		NE

25. Poslal Ti někdy někdo nevyžádaný email nebo odkaz do mobilu, aby ses přes něj někam přihlásil, např. do banky, na Facebook, na herní účet apod.)? (Můžeš zakřížkovat i více odpovědí)

	Ano, ale nepřihlásil/a jsem se přes odkaz.		Ne, nic takového mi nepřišlo.
	Ano, přihlásil/a jsem se přes odkaz.		Nevím. Nejsem si vědom/a.

26. Kdyby tě poprosil kamarád přes Facebook, abys mu co nejdřív poslal 20,- Kč na bankovní účet, že to opravdu velmi nutně potřebuje, udělal/a bys to? (Můžeš zakřížkovat i více odpovědí)

	Poslal/a bych mu to já sám/a ze svého bankovního účtu nebo mojí platební karty.		Poprosil/a bych rodiče nebo někoho jiného, aby mu to oni sami poslali.
	Poprosil/a bych rodiče o platební kartu a poslal/a bych mu to já sám/a.		Nejdřív bych si ověřil/a, jestli mi napsal skutečně můj kamarád.
	Poprosil/a bych dědečka/babičku o platební kartu a poslal/a bych mu to já sám/a.		Nereagoval/a bych na to.
	Poprosil/a bych kamaráda nebo někoho jiného o platební kartu a poslal/a bych mu to já sám/a.		Nemám možnost mu to poslat, nebo bych to odmítl/a poslat.

27. Žádal Tě někdy někdo (např. kamarád) přes sociální síť (např. přes Facebook) o zaslání drobné platby nebo přeposlání nějakého kódu z mobilu? (Zakřížkuj jednu odpověď)

	Ano, byl to podvod, přišel/přišla jsem o peníze.		Ano, ale podvod to nebyl.
	Ano, byl to podvod, ale nereagoval/a jsem na to.		Nikdo to po mně nikdy nechtěl.

28. Kdyby Ti přišla SMS zpráva (nebo zpráva do messengeru), že byl tvůj Facebookový účet napaden a musíš se k němu přihlásit přes odkaz v této SMS zprávě, udělal/a bys to? (Zakřížkuj jednu odpověď)

	ANO		NE

29. Byl/a jsi někým poučen/a, na co si dávat pozor při internetovém nakupování, abys nebyl/a podveden/a, např. v internetovém bazaru, v aukci, v e-shopu? (Můžeš zakřížkovat i více odpovědí)

	Ano, ve škole.		Ano, někým jiným.
	Ano, rodiči.		Ne, ale sám/a jsem o tom četl/a, slyšel/a.
	Ano, kamarádem.		Ne, nikým.

30. Byl/a jsi někým poučen/a, co je to phishing? (Můžeš zakřížkovat i více odpovědí)

	Ano, ve škole.		Ano, někým jiným.
	Ano, rodiči.		Ne, ale sám/a jsem o tom četl/a, slyšel/a.
	Ano, kamarádem.		Nevím co je to phishing.

31. Byl/a jsi někým poučen/a, co je to scam? (Můžeš zakřížkovat i více odpovědí)

	Ano, ve škole		Ano, někým jiným
	Ano, rodiči		Ne, ale sám/a jsem o tom četl/a, slyšel/a.
	Ano, kamarádem		Nevím co je to scam

32. Byl/a jsi někým poučen/a, jak reagovat na nevyžádaný email (spam) od cizí osoby? (Můžeš zakřížkovat i více odpovědí)

	Ano, ve škole.		Ano, někým jiným.
	Ano, rodiči.		Ne, ale sám/a jsem o tom četl/a, slyšel/a.
	Ano, kamarádem.		Ne.

33. Byl/a jsi někým poučen/a, jak reagovat na nedovolené vniknutí (nabourání se) do Tvého účtu na sociální síti, nap. na Facebooku, Instagramu apod.? (Můžeš zakřížkovat i více odpovědí)

	Ano, ve škole.		Ano, někým jiným.
	Ano, rodiči.		Nemám účet na Facebooku.
	Ano, kamarádem.		Ne.

34. Znáš nějakou internetovou stránku, na které si můžeš zjistit hodnocení a recenze internetových obchodů (e-shopů)? (Zakřížkuj jednu odpověď)

	ANO		NE

Pokud ano, napiš kterou:_____

35. Setkal/a ses někdy s virem, který Ti by zablokoval mobil, tablet nebo počítač a chtěl za odblokování zaplatit peníze? (Zakřížkuj jednu odpověď)

	ANO		NE

Jsem: (Zakřížkuj jednu odpověď)

	Dívka		Chlapec

Chodím do (Zakřížkuj jednu odpověď)

	6. třídy		9. třídy

Můj věk je (doplň) …….. let

Děkuji za vyplnění :o)

Příloha č. 2 – dotazník pro žáky základních škol, finální podoba po úpravě.

Vážení žáci,

v České republice je zaznamenáván každým rokem nárůst podvodů páchaných prostřednictvím informačních a komunikačních technologií, zejména na internetu. Dané důvody nás vedly k provedení dotazníkového šetření na podobné téma.

Získané informace budou využity pro zjištění aktuálního stavu v oblasti prevence před uvedenou kriminalitou, proto Tě prosíme o úplné a pravdivé vyplnění všech položek tohoto anonymního dotazníku. Při jeho vyplňování se řiď pokyny v závorkách. Děkujeme za spolupráci.

Za výzkumný tým Michal Jančík, policista vyšetřující trestnou činnost a zároveň student Pedagogické fakulty, Univerzity Palackého v Olomouci, obor Veřejná správa.

1. **Máš možnost někomu přes internet poslat peníze na bankovní účet, např. zaplatit za hru nebo elektroniku?** (Můžeš zakřížkovat i více odpovědí)

1	Ano, internetovým bankovnictvím.	5	Ano, vlastní platební kartou.
2	Ano, platební kartou rodičů.	6	Ano, platební kartou kamaráda.
3	Ano, platební kartou dědečka/babičky.	7	Já sám/a ne.
4	Ano, přes Paypal, Gopay, PayU apod.	8	Nevím.

2. **Vlastníš platební kartu?** (Zakřížkuj jednu odpověď)

1	ANO	2	NE

3. **Platil/a jsi někdy platební kartou?** (Zakřížkuj jednu odpověď)

	ANO		NE

4. **Pokud jsi platil/a někdy platební kartou, kde to bylo?** (Můžeš zakřížkovat i více odpovědí)

	Na internetu, za nákup v obchodě (e-shopu).		V obchodě.
	Na internetu, za nákup přes inzerát v bazaru.		V restauraci.
	Na internetu, za nákup v aukci.		Na poště nebo někde jinde.
	Na internetu, za nákup počítačové hry.		Nikdy jsem neplatil/a platební kartou.

5. **Přihlašoval/a ses někdy k bankovnímu účtu na internetu (internetové bankovnictví)?** (Můžeš zakřížkovat i více odpovědí)

	Ano, k vlastnímu bankovnímu účtu.		Ano, k bankovnímu účtu dědečka/babičky.
	Ano, k bankovnímu účtu rodičů.		Ano, k bankovnímu účtu někoho jiného.
	Ano, k bankovnímu účtu kamaráda.		Ne.

6. **Chtěl/a jsi někdy něco koupit přes internet, např. hru, mobil, tablet, oblečení?**
(Zakřížkuj jednu odpověď)

	ANO
	NEVÍM

	NE

7. **Nakoupil/a jsi někdy něco přes internet? Pokud ano, co to bylo?** (Můžeš zakřížkovat i více odpovědí)

	Ano, hry.
	Ano, vylepšení do her.
	Ano, elektroniku.
	Ano, oblečení.

	Ano, sportovní věci.
	Ano, hračky.
	Ano, jiné věci.
	Nenakupoval/a jsem nic přes internet.

8. **Nakupoval/a jsi někdy v internetové aukci, např. na Aukru?** (Můžeš zakřížkovat i více odpovědí)

	Ano, sám/a jsem nakupoval/a.
	Ano, s rodičem jsem nakupoval/a.
	Ano,s dědečkem/babičkou jsem nakupoval/a.

	Ano, s kamarádem jsem nakupoval/a.
	Ano, s někým jiným jsem nakupoval/a.
	Nenakupoval/a jsem.

9. **Nakupoval/a jsi někdy v internetovém bazaru, např. na Bazoši?** (Můžeš zakřížkovat i více odpovědí)

	Ano, sám/a jsem nakupoval/a.
	Ano, s rodičem jsem nakupoval/a.
	Ano, s dědečkem/babičkou jsem nakupoval/a.

	Ano, s kamarádem jsem nakupoval/a.
	Ano, s někým jiným jsem nakupoval/a.
	Nenakupoval/a jsem.

10. **Nakupoval/a jsi někdy v internetovém obchodě (e-shopu), např. Alza, TS Bohemia, MALL apod.?** (Můžeš zakřížkovat i více odpovědí)

	Ano, sám/a jsem nakupoval/a.
	Ano, s rodičem jsem nakupoval/a.
	Ano, s dědečkem/babičkou jsem nakupoval/a.

	Ano, s kamarádem jsem nakupoval/a.
	Ano, s někým jiným jsem nakupoval/a.
	Nenakupoval/a jsem.

11. **Máš nějaký svůj herní účet?** (Můžeš zakřížkovat i více odpovědí)

	Ano, Steam
	Ano, Playstation Network.
	Ano, Xbox Live.
	Ano, Google Play.

	Ano, App store.
	Ano, Microsoft Store.
	Ano, mám ale jiný účet.
	Ne, nemám žádný podobný herní účet.

12. **Nakupoval/a jsi někdy přes nějaký herní účet např. přes Steam, Origin, PlayStation Network, Xbox Live, Google play apod.?** (Můžeš zakřížkovat i více odpovědí)

	Ano, sám/a jsem si to nakoupil/a
	Ano, s rodičem jsem tam nakupoval/a.
	Ano, s dědečkem/babičkou jsem nakupoval/a.

	Ano, s kamarádem jsem tam nakupoval/a.
	Ano, s někým jiným jsem tam nakupoval/a.
	Nenakupoval/a jsem.

13. **Nakupoval/a jsi někdy nějaké vylepšení (mikrotrasakce) do počítačové hry za skutečné peníze? Např. do League of Legends, World of Tanks nebo jiné hry.** (Můžeš zakřížkovat i více odpovědí)

	Ano, sám/a jsem tam nakupoval/a.		Ano, s někým jiným jsem tam nakupoval/a.
	Ano, s rodičem jsem tam nakupoval/a.		Ano, sám/a jsem si to koupil/a, bez vědomí rodičů, z jejich platební karty.
	Ano, s dědečkem/babičkou jsem nakupoval/a.		Ano, sám/a jsem si to koupil/a, bez vědomí dědečka/babičky, z jejich platební karty.
	Ano, s kamarádem jsem tam nakupoval/a.		Nenakupoval/a jsem nic takového.

14. **Pokud jsi nakoupil/a něco přes internet, kdo zboží zaplatil?** (Můžeš zakřížkovat i více odpovědí)

	Já sám/a.		Kamarád.
	Rodiče.		Někdo jiný.
	Dědeček/babička.		Nenakupoval/a jsem nic přes internet.

15. **Ověřuješ si nějak internetový obchod (e-shop) před nákupem zboží, abys nebyl/a podveden/a?** (Můžeš zakřížkovat i více odpovědí)

	Neověřuji.		Ano, čtu si obchodní podmínky.
	Nevím jak a kde bych měl/a.		Ano, předem telefonuji na kontakt.
	Ano, hledám a čtu si jeho hodnocení.		Ano, hledám jak dlouho e-shop existuje.
	Ano, hledám o něm informace na internetu.		Nenakupuji v e-shopech.

16. **Ověřuješ si prodejce na internetovém bazaru před nákupem zboží, abys nebyl/a podveden/a?** (Můžeš zakřížkovat i více odpovědí)

	Neověřuji.		Ano, hledám a čtu si hodnocení prodejce.
	Nevím jak a kde bych měl/a.		Ano, dotazuji se na možnost osobního převzetí.
	Neověřuji, komunikuji jen přes email.		Ano, telefonuji na kontakt, vyptávám se na zboží.
	Ano, prohlížím si i další nabídky prodejce.		Nenakupuji v internetových bazarech.

17. **Ověřuješ si prodejce internetové aukce před nákupem zboží, abys nebyl/a podveden/a?** (Můžeš zakřížkovat i více odpovědí)

	Neověřuji.		Ano, hledám a čtu si hodnocení prodejce.
	Nevím jak a kde bych měl/a..		Ano, dotazuji se na možnost osobního převzetí.
	Neověřuji, komunikuji jen přes email.		Ano, telefonuji na kontakt, vyptávám se na zboží.
	Ano, prohlížím si další nabídky prodejce.		Nenakupuji v internetových aukcích.

18. **Prodával/a jsi někdy něco přes internet?** (Zakřížkuj jednu odpověď)

	ANO - prodával		NE - neprodával

19. Podle čeho bys poznal/a, že jde o podvodný inzerát např. podvodný prodej mobilního telefonu? (Pokud víš, napiš stručnou odpověď):

20. Byl/a jsi někdy nějakým způsobem podveden/a na internetu? (Můžeš zakřížkovat i více odpovědí)

	Ano, přišel/přišla jsem o peníze nebo jiný majetek (vznikla mi majetková škoda).		Ano, přišel/přišla jsem tím o své osobní údaje, heslo, fotky, videa, apod.
	Ano, ale někdo jiný díky mě přišel o peníze (např. rodiče, dědeček, babička, kamarád).		Ano, někdo se mi naboural do facebookového, herního, bankovního či jiného účtu nebo emailu.
	Ano, někdo mě podvedl a klikl/a jsem na zavirovaný odkaz, obrázek, stránku, apod.		Ano, psal mi někdo z falešného profilu na Facebooku.
	Přišla mi podvodná zpráva nebo email.		Ne.

21. Setkal/a ses někdy s podvodem při nákupu zboží přes internet? (Můžeš zakřížkovat i více odpovědí)

	Ano, byl/a jsem podveden/a přímo já.		Vím, že takové podvody existují.
	Ano, podvedli někoho z mého okolí (rodina, kamarád, známý, apod.).		Ne, nesetkal/a jsem se s tím.

22. Přišel Ti někdy nevyžádaný email od neznámého odesílatele (spam)? (Můžeš zakřížkovat i více odpovědí)

	Ano, někdo se chtěl semnou seznámit.		Ano, přišel/a, ale neotvíral/a jsem ho.
	Ano, přišla zpráva, že jsem něco vyhrál/a.		Ano, někdo mi nabízel, že si můžu vydělat peníze
	Ano, přišla podvodná výzva, že dlužím peníze		Ano, přišel, ale týkal se něčeho jiného.
	Ano, přišla mi podvodná faktura k zaplacení.		Ne, nepřišel.
	Ano, přišla mi nabídka zboží nebo reklama.		Nemám email.

23. Pokud jsi obdržel/a takový nevyžádaný email, jak jsi na něj reagoval/a? (Můžeš zakřížkovat i více odpovědí)

	Nečetl/a jsem ho a vymazal/a.		Přečetl/a jsem ho a klikl/a na přílohu nebo odkaz v této zprávě.
	Přečetl/a jsem ho a vymazal/a.		Nepřišel mi žádný takový email.
	Přečetl/a jsem ho a odepsal/a.		Nemám email.

24. Prozvánělo Tě na mobil někdy cizí tel. číslo ze zahraničí, na které jsi poté zatelefonoval/a a přišel/a o peníze nebo kredit za drahé volání)? (Zakřížkuj jednu odpověď)

	ANO		NE

25. Poslal Ti někdy někdo nevyžádaný email nebo odkaz do mobilu, aby ses přes něj někam přihlásil, např. do banky, na Facebook, na herní účet apod.)? (Můžeš zakřížkovat i více odpovědí)

	Ano, ale nepřihlásil/a jsem se přes odkaz.		Ne, nic takového mi nepřišlo.
	Ano, přihlásil/a jsem se přes odkaz.		Nevím. Nejsem si vědom/a.

26. Kdyby tě poprosil kamarád přes Facebook, abys mu rychle poslal 20,- Kč na bankovní účet, že to opravdu velmi nutně potřebuje, udělal/a bys to? (Můžeš zakřížkovat i více odpovědí)

	Poslal/a bych mu to já sám/a ze svého bankovního účtu nebo mojí platební karty.		Poprosil/a bych rodiče nebo někoho jiného, aby mu to oni sami poslali.
	Poprosil/a bych rodiče o platební kartu a poslal/a bych mu to já sám/a.		Nejdřív bych si ověřil/a, jestli mi napsal skutečně můj kamarád.
	Poprosil/a bych dědečka/babičku o platební kartu a poslal/a bych mu to já sám/a.		Nereagoval/a bych vůbec na to.
	Poprosil/a bych kamaráda nebo někoho jiného o platební kartu a poslal/a bych mu to já sám/a.		Odmítl/a bych to poslat.

27. Žádal Tě někdy někdo (např. kamarád) přes sociální síť (např. přes Facebook) o zaslání drobné platby nebo přeposlání nějakého kódu z mobilu? (Zakřížkuj jednu odpověď)

	Ano, byl to podvod, přišel/přišla jsem o peníze.		Ano, ale podvod to nebyl.
	Ano, byl to podvod, ale nereagoval/a jsem na to.		Nikdo to po mně nikdy nechtěl.

28. Kdyby Ti přišla SMS zpráva (nebo zpráva do messengeru), že byl tvůj Facebookový účet napaden a musíš se k němu přihlásit přes odkaz v této SMS zprávě, udělal/a bys to? (Zakřížkuj jednu odpověď)

	ANO		NE

29. Byl/a jsi někým poučen/a, na co si dávat pozor při internetovém nakupování, abys nebyl/a podveden/a, např. v internetovém bazaru, v aukci, v e-shopu? (Můžeš zakřížkovat i více odpovědí)

	Ano, ve škole.		Ano, někým jiným.
	Ano, rodiči.		Sám/a jsem si o tom četl/a, slyšel/a.
	Ano, kamarádem.		Ne, nikým.

30. Byl/a jsi někým poučen/a, co je to podvodná metoda phishing? (Můžeš zakřížkovat i více odpovědí)

	Ano, ve škole.		Ano, někým jiným.
	Ano, rodiči.		Sám/a jsem si o tom četl/a, slyšel/a.
	Ano, kamarádem.		Nevím co je to phishing.

31. Byl/a jsi někým poučen/a, co je to scam? (Můžeš zakřížkovat i více odpovědí)

	Ano, ve škole		Ano, někým jiným
	Ano, rodiči		Sám/a jsem si o tom četl/a, slyšel/a.
	Ano, kamarádem		Nevím co je to scam

32. Byl/a jsi někým poučen/a, jak reagovat na nevyžádaný email (spam) od cizí osoby? (Můžeš zakřížkovat i více odpovědí)

	Ano, ve škole.		Ano, někým jiným.
	Ano, rodiči.		Sám/a jsem si o tom četl/a, slyšel/a.
	Ano, kamarádem.		Ne.

33. Byl/a jsi někým poučen/a, jak reagovat na nedovolené vniknutí (nabourání se) do Tvého účtu na sociální síti, nap. na Facebooku, Instagramu, do emailu apod.? (Můžeš zakřížkovat i více odpovědí)

	Ano, ve škole.		Ano, někým jiným.
	Ano, rodiči.		Sám/a jsem si o tom četl/a, slyšel/a.
	Ano, kamarádem.		Ne.

34. Znáš nějakou internetovou stránku, na které si můžeš zjistit hodnocení a recenze internetových obchodů (e-shopů)? (Zakřížkuj jednu odpověď)

	ANO		NE

Pokud ano, napiš
kterou:_____

35. Setkal/a ses někdy s takovým virem, který Ti zablokoval mobil, tablet nebo počítač a chtěl za odblokování zaplatit peníze? (Zakřížkuj jednu odpověď)

	ANO		NE

Jsem: (Zakřížkuj jednu odpověď)

	Dívka		Chlapec

Chodím do (Zakřížkuj jednu odpověď)

	6. třídy		9. třídy

Můj věk je (doplň) …….. let

Děkuji za vyplnění ☺

Příloha č. 3 – výsledky dotazníkového šetření podrobně.

První číselná hodnota za každou odpovědí představuje četnost odpovědí žáků 9. tříd, druhá číselná hodnota za lomítkem představuje četnost odpovědí žáků 6. tříd.

1. Máš možnost někomu přes internet poslat peníze na bankovní účet, např. zaplatit za hru nebo elektroniku? *Na tuto položku odpovědělo 114 žáků 9. tříd a 114 žáků 6. tříd.*

1. Ano, internetovým bankovnictvím. *Četnost odpovědí 20/8.*
2. Ano, platební kartou rodičů. *Četnost odpovědí 24/10.*
3. Ano, platební kartou dědečka/babičky. *Četnost odpovědí 2/0.*
4. Ano, přes Paypal, Gopay, PayU apod. *Četnost odpovědí 16/9.*
5. Ano, vlastní platební kartou. *Četnost odpovědí 28/6.*
6. Ano, platební kartou kamaráda. *Četnost odpovědi1 2/0.*
7. Já sám/a ne. *Četnost odpovědí 57/81.*
8. Nevím. *Četnost odpovědí 2/16.*

2. Vlastníš platební kartu? *Na tuto položku odpovědělo 115 žáků 9. tříd a 117 žáků 6. tříd.*

1. ANO. *Četnost odpovědí 42/12.*
2. NE. *Četnost odpovědí 73/105.*

3. Platil/a jsi někdy platební kartou? *Na tuto položku odpovědělo 114 žáků 9. tříd a 117 žáků 6. tříd.*

1. ANO. *Četnost odpovědí 68/39.*
2. NE. *Četnost odpovědí 46/78.*

4. Pokud jsi platil/a někdy platební kartou, kde to bylo? *Na tuto položku odpovědělo 113 žáků 9. tříd a 116 žáků 6. tříd.*

1. Na internetu, za nákup v obchodě (e-shopu). *Četnost odpovědí 27/9.*
2. Na internetu, za nákup přes inzerát v bazaru. *Četnost odpovědí 2/1.*
3. Na internetu, za nákup v aukci. *Četnost odpovědí 0/0.*
4. Na internetu, za nákup počítačové hry. *Četnost odpovědí 15/14.*
5. V obchodě. *Četnost odpovědí 57/29.*
6. V restauraci. *Četnost odpovědí 11/5.*
7. Na poště nebo někde jinde. *Četnost odpovědí 11/1.*
8. Nikdy jsem neplatil/a platební kartou. *Četnost odpovědí 47/76.*

5. Přihlašoval/a ses někdy k bankovnímu účtu na internetu (internetové bankovnictví)? *Na tuto položku odpovědělo 114 žáků 9. tříd a 116 žáků 6. tříd.*

1. Ano, k vlastnímu bankovnímu účtu. *Četnost odpovědí 28/4.*
2. Ano, k bankovnímu účtu rodičů. *Četnost odpovědí 9/5.*
3. Ano, k bankovnímu účtu kamaráda. *Četnost odpovědí 1/0.*
4. Ano, k bankovnímu účtu dědečka/babičky. *Četnost odpovědí 1/0.*
5. Ano, k bankovnímu účtu někoho jiného. *Četnost odpovědí 0/0.*
6. Ne. *Četnost odpovědí 78/107.*

6. Chtěl/a jsi někdy něco koupit přes internet, např. hru, mobil, tablet, oblečení? *Na tuto položku odpovědělo 115 žáků 9. tříd a 117 žáků 6. tříd.*

1. ANO. *Četnost odpovědí 99/92.*
2. NE. *Četnost odpovědí 8/21.*
3. NEVÍM. *Četnost odpovědí 8/4.*

7. Nakoupil/a jsi někdy něco přes internet? Pokud ano, co to bylo? *Na tuto položku odpovědělo 115 žáků 9. tříd a 116 žáků 6. tříd.*

1. Ano, hry. *Četnost odpovědí 36/32.*
2. Ano, vylepšení do her. *Četnost odpovědí 20/21.*
3. Ano, elektroniku. *Četnost odpovědí 35/28.*
4. Ano, oblečení. *Četnost odpovědí 60/32.*
5. Ano, sportovní věci. *Četnost odpovědí 32/16.*
6. Ano, hračky. *Četnost odpovědí 3/8.*
7. Ano, jiné věci. *Četnost odpovědí 37/15.*
8. Nenakupoval/a jsem nic přes internet. *Četnost odpovědí 19/46.*

8. Nakupoval/a jsi někdy v internetové aukci, např. na Aukru? *Na tuto položku odpovědělo 115 žáků 9. tříd a 117 žáků 6. tříd.*

1. Ano, sám/a jsem nakupoval/a. *Četnost odpovědí 2/0.*
2. Ano, s rodičem jsem nakupoval/a. *Četnost odpovědí 16/16.*
3. Ano, s dědečkem/babičkou jsem nakupoval/a. *Četnost odpovědí 1/1.*
4. Ano, s kamarádem jsem nakupoval/a. *Četnost odpovědí 2/3.*
5. Ano, s někým jiným jsem nakupoval/a. *Četnost odpovědí 2/0.*
6. Nenakupoval/a jsem. *Četnost odpovědí 96/99.*

9. Nakupoval/a jsi někdy v internetovém bazaru, např. Bazoš? *Na tuto položku odpovědělo 114 žáků 9. tříd a 116 žáků 6. tříd.*

1. Ano, sám/a jsem nakupoval/a. *Četnost odpovědí 8/1.*
2. Ano, s rodičem jsem nakupoval/a. *Četnost odpovědí 33/24.*
3. Ano, s dědečkem/babičkou jsem nakupoval/a. *Četnost odpovědí 2/2.*
4. Ano, s kamarádem jsem nakupoval/a. *Četnost odpovědí 3/0.*
5. Ano, s někým jiným jsem nakupoval/a. *Četnost odpovědí 0/0.*
6. Nenakupoval/a jsem. *Četnost odpovědí 74/91.*

10. Nakupoval/a jsi někdy v internetovém obchodě (e-shopu), např. Alza, TS Bohemia, MALL apod.? *Na tuto položku odpovědělo 114 žáků 9. tříd a 117 žáků 6. tříd.*

1. Ano, sám/a jsem nakupoval/a. *Četnost odpovědí 36/5.*
2. Ano, s rodičem jsem nakupoval/a. *Četnost odpovědí 58/55.*
3. Ano, s dědečkem/babičkou jsem nakupoval/a. *Četnost odpovědí 6/5.*
4. Ano, s kamarádem jsem nakupoval/a. *Četnost odpovědí 4/0.*
5. Ano, s někým jiným jsem nakupoval/a. *Četnost odpovědí 7/2.*
6. Nenakupoval/a jsem. *Četnost odpovědí 33/57.*

11. Máš nějaký svůj herní účet? *Na tuto položku odpovědělo 114 žáků 9. tříd a 115 žáků 6. tříd.*

1. Ano, Steam. *Četnost odpovědí 41/41.*
2. Ano, Playstation Network. *Četnost odpovědí 14/12.*
3. Ano, Xbox Live. *Četnost odpovědí 25/14.*
4. Ano, Google Play. *Četnost odpovědí 77/77.*
5. Ano, App store. *Četnost odpovědí 31/13.*
6. Ano, Microsoft Store. *Četnost odpovědí 40/22.*
7. Ano, mám ale jiný účet. *Četnost odpovědí 21/16.*
8. Ne, nemám žádný podobný herní účet. *Četnost odpovědí 18/26.*

12. Nakupoval/a jsi někdy přes nějaký herní účet např. přes Steam, Origin, PlayStation Network, Xbox Live, Google play apod.? *Na tuto položku odpovědělo 114 žáků 9. tříd a 117 žáků 6. tříd.*

1. Ano, sám/a jsem nakupoval/a. *Četnost odpovědí 30/11.*
2. Ano, s rodičem jsem tam nakupoval/a. *Četnost odpovědí 17/32.*
3. Ano, s dědečkem/babičkou jsem nakupoval/a. *Četnost odpovědí 1/0.*
4. Ano, s kamarádem jsem tam nakupoval/a. *Četnost odpovědí 14/4.*
5. Ano, s někým jiným jsem tam nakupoval/a. *Četnost odpovědí 4/4.*
6. Nenakupoval/a jsem. *Četnost odpovědí 66/76.*

13. Nakupoval/a jsi někdy nějaké vylepšení (mikrotrasakce) do počítačové hry za skutečné peníze? Např. do League of Legends, World of Tanks nebo jiné hry. *Na tuto položku odpovědělo 114 žáků 9. tříd a 117 žáků 6. tříd.*

1. Ano, sám/a jsem si to nakoupil/a. *Četnost odpovědí 27/15.*
2. Ano, s rodičem jsem tam nakupoval/a. *Četnost odpovědí 12/22.*
3. Ano, s dědečkem/babičkou jsem nakupoval/a. *Četnost odpovědí 1/1.*
4. Ano, s kamarádem jsem tam nakupoval/a. *Četnost odpovědí 9/5.*
5. Ano, s někým jiným jsem tam nakupoval/a. *Četnost odpovědí 4/1.*
6. Ano, sám/a jsem si to koupil/a, bez vědomí rodičů, z jejich platební karty. *Četnost odpovědí 1/1.*
7. Ano, sám/a jsem si to koupil/a, bez vědomí dědečka/babičky, z jejich platební karty. *Četnost odpovědí 0/0.*
8. Nenakupoval/a jsem nic takového. *Četnost odpovědí 83/83.*

14. Pokud jsi nakoupil/a něco přes internet, kdo zboží zaplatil? *Na tuto položku odpovědělo 115 žáků 9. tříd a 114 žáků 6. tříd.*

1. Já sám/a. *Četnost odpovědí 66/23.*
2. Rodiče. *Četnost odpovědí 80/76.*
3. Dědeček/babička. *Četnost odpovědí 9/11.*
4. Kamarád. *Četnost odpovědí 9/5.*
5. Někdo jiný. *Četnost odpovědí 4/7.*
6. Nenakoupil/a jsem nikdy nic přes internet. *Četnost odpovědí 17/39.*

15. Ověřuješ si nějak internetový obchod (e-shop) před nákupem zboží, abys nebyl/a podveden/a? *Na tuto položku odpovědělo 114 žáků 9. tříd a 115 žáků 6. tříd.*

1. Neověřuji. *Četnost odpovědí 21/12.*
2. Nevím jak a kde bych měl/a. *Četnost odpovědí 16/12.*
3. Ano, hledám a čtu si jeho hodnocení. *Četnost odpovědí 54/23.*
4. Ano, hledám o něm informace na internetu. *Četnost odpovědí 29/15.*
5. Ano, čtu si obchodní podmínky. *Četnost odpovědí 26/13.*
6. Ano, předem telefonuji na kontakt. *Četnost odpovědí 7/2.*
7. Ano, hledám jak dlouho e-shop existuje. *Četnost odpovědí 9/5.*
8. Nenakupuji v e-shopech. *Četnost odpovědí 25/63.*

16. Ověřuješ si prodejce na internetovém bazaru před nákupem zboží, abys nebyl/a podveden/a? *Na tuto položku odpovědělo 114 žáků 9. tříd a 117 žáků 6. tříd.*

1. Neověřuji. *Četnost odpovědí 19/10.*
2. Nevím jak a kde bych měl/a. *Četnost odpovědí 7/7.*
3. Neověřuji, komunikuji jen přes email. *Četnost odpovědí 4/2.*
4. Ano, prohlížím si i další nabídky prodejce. *Četnost odpovědí 17/10.*
5. Ano, hledám a čtu si hodnocení prodejce. *Četnost odpovědí 26/9.*
6. Ano, dotazuji se na možnost osobního převzetí. *Četnost odpovědí 8/4.*
7. Ano, telefonuji na kontakt, vyptávám se na zboží. *Četnost odpovědí 7/5.*
8. Nenakupuji v internetových bazarech. *Četnost odpovědí 63/90.*

17. Ověřuješ si prodejce internetové aukce před nákupem zboží, abys nebyl/a podveden/a? *Na tuto položku odpovědělo 114 žáků 9. tříd a 117 žáků 6. tříd.*

1. Neověřuji. *Četnost odpovědí 13/6.*
2. Nevím jak a kde bych měl/a. *Četnost odpovědí 6/6.*
3. Neověřuji, komunikuji jen přes email. *Četnost odpovědí 2/2.*
4. Ano, prohlížím si i další nabídky prodejce. *Četnost odpovědí 10/1.*
5. Ano, hledám a čtu si hodnocení prodejce. *Četnost odpovědí 11/5.*
6. Ano, dotazuji se na možnost osobního převzetí. *Četnost odpovědí 6/0.*
7. Ano, telefonuji na kontakt, vyptávám se na zboží. *Četnost odpovědí 7/1.*
8. Nenakupuji v internetových aukcích. *Četnost odpovědí 88/100.*

18. Prodával/a jsi někdy něco přes internet? *Na tuto položku odpovědělo 114 žáků 9. tříd a 117 žáků 6. tříd.*

1. ANO – prodával. *Četnost odpovědí 50/30.*
2. NE – neprodával. *Četnost odpovědí 64/87.*

19. Podle čeho bys poznal/a, že jde o podvodný inzerát např. podvodný prodej mobilního telefonu? *Na tuto položku odpovědělo 115 žáků 9. tříd a 117 žáků 6. tříd.*

1. Uvedli přímo, že neví. *Četnost odpovědí 8/27.*
2. Neodpověděli. *Četnost odpovědí 51/57.*

1. Chybná odpověď (např. velmi vysoká cena, velmi starý inzerát, po zaplacení by zboží nepřišlo, prodejce koktá, nabízí to zdarma). *Četnost odpovědí 0/11.*

2. Málo údajů k prodejci, chybějící kontakt, nebo nabízenému zboží. *Četnost odpovědí 12/8.*
3. Podaný inzerát by měl chyby v textu. *Četnost odpovědí 7/1.*
4. Nízká cena, výhodná koupě. *Četnost odpovědí 19/5.*
5. Popis zboží v inzerátu by neodpovídal skutečnému zboží. *Četnost odpovědí 2/1.*
6. Fotografie stažená z internetu, málo fotografií nebo žádná fotografie zboží. *Četnost odpovědí* 18/7.
7. Prodejce bude vyžadovat platbu pouze předem. *Četnost odpovědí 5/2.*
8. Nefunkční tel. kontakt prodejce. *Četnost odpovědí 2/1.*

20. Byl/a jsi někdy nějakým způsobem podveden/a na internetu? *Na tuto položku odpovědělo 113 žáků 9. tříd a 117 žáků 6. tříd.*

1. Ano, přišel/přišla jsem o peníze nebo jiný majetek (vznikla mi majetková škoda). *Četnost odpovědí 5/5.*
2. Ano, ale někdo jiný díky mě přišel o peníze (např. rodiče, dědeček, babička, kamarád). *Četnost odpovědí 3/1.*
3. Ano, někdo mě podvedl a klikl/a jsem na zavirovaný odkaz, obrázek, stránku, apod. *Četnost odpovědí 7/5.*
4. Přišla mi podvodná zpráva nebo email. *Četnost odpovědí 25/9.*
5. Ano, přišel/přišla jsem tím o své osobní údaje, heslo, fotky, videa, apod. *Četnost odpovědí 1/1.*
6. Ano, někdo se mi naboural do facebookového, herního, bankovního či jiného účtu nebo emailu. *Četnost odpovědí 12/7.*
7. Ano, psal mi někdo z falešného profilu na Facebooku. *Četnost odpovědí 28/5.*
8. Ne. *Četnost odpovědí 63/95.*

21. Setkal/a ses někdy s podvodem při nákupu zboží přes internet? *Na tuto položku odpovědělo 114 žáků 9. tříd a 116 žáků 6. tříd.*

1. Ano, byl/a jsem podveden/a přímo já. *Četnost odpovědí 6/1.*
2. Ano, podvedli někoho z mého okolí (rodina, kamarád, známý, apod.). *Četnost odpovědí* 20/7.
3. Ne, ale vím, že takové podvody existují. *Četnost odpovědí 57/53.*
4. Ne, nesetkal/a jsem se s tím. *Četnost odpovědí 43/65.*

22. Přišel Ti někdy nevyžádaný email od neznámého odesílatele (spam)? *Na tuto položku odpovědělo 114 žáků 9. tříd a 113 žáků 6. tříd.*

1. Ano, někdo se chtěl semnou seznámit. *Četnost odpovědí 19/8.*
2. Ano, přišla zpráva, že jsem něco vyhrál/a. *Četnost odpovědí 43/17.*
3. Ano, přišla podvodná zpráva, že dlužím peníze. *Četnost odpovědí 5/4.*
4. Ano, přišla mi podvodná faktura k zaplacení. *Četnost odpovědí 5/2.*
5. Ano, přišla mi nabídka zboží nebo reklama. *Četnost odpovědí 51/17.*
6. Ano, přišel/a, ale neotvíral/a jsem ho. *Četnost odpovědí 51/15.*
7. Ano, někdo mi nabízel, že si můžu vydělat peníze. *Četnost odpovědí 18/4.*
8. Ano, přišel, ale týkal se něčeho jiného. *Četnost odpovědí 12/8.*
9. Ne, nepřišel. *Četnost odpovědí 31/66.*
10. Nemám email. *Četnost odpovědí 1/4.*

23. Pokud jsi obdržel/a takový nevyžádaný email, jak jsi na něj reagoval/a? *Na tuto položku odpovědělo 114 žáků 9. tříd a 112 žáků 6. tříd.*

1. Nečetl/a jsem ho a vymazal/a. *Četnost odpovědí 60/17.*
2. Přečetl/a jsem ho a vymazal/a. *Četnost odpovědí 41/27.*
3. Přečetl/a jsem ho a odepsal/a. *Četnost odpovědí 3/1.*
4. Přečetl/a jsem ho a klikl/a na přílohu nebo odkaz v této zprávě. *Četnost odpovědí 3/0.*
5. Nepřišel mi žádný takový email. *Četnost odpovědí 27/65.*
6. Nemám email. *Četnost odpovědí 1/4.*

24. Prozvánělo Tě na mobil někdy cizí tel. číslo ze zahraničí, na které jsi poté zatelefonoval/a a přišel/a o peníze nebo kredit za drahé volání? *Na tuto položku odpovědělo 114 žáků 9. tříd a 116 žáků 6. tříd.*

1. Ano. *Četnost odpovědí 13/20.*
2. Ne. *Četnost odpovědí 101/96.*

25. Poslal Ti někdy někdo nevyžádaný email nebo odkaz do mobilu, aby ses přes něj někam přihlásil, např. do banky, na Facebook, na herní účet apod.? *Na tuto položku odpovědělo 115 žáků 9. tříd a 116 žáků 6. tříd.*

1. Ano, ale nepřihlásil/a jsem se přes odkaz. *Četnost odpovědí 28/15.*
2. Ano, přihlásil/a jsem se přes odkaz. *Četnost odpovědí 6/2.*
3. Ne, nic takového mi nepřišlo. *Četnost odpovědí 45/64.*
4. Nevím. Nejsem si vědom/a. *Četnost odpovědí 39/35.*

26. Kdyby tě poprosil kamarád přes Facebook, abys mu co nejdřív poslal 20,- Kč na bankovní účet, že to opravdu velmi nutně potřebuje, udělal/a bys to? *Na tuto položku odpovědělo 115 žáků 9. tříd a 115 žáků 6. tříd.*

1. Poslal/a bych mu to já sám/a ze svého bankovního účtu nebo mojí platební karty. *Četnost odpovědí 8/3.*
2. Poprosil/a bych rodiče o platební kartu a poslal/a bych mu to já sám/a. *Četnost odpovědí 3/4.*
3. Poprosil/a bych dědečka/babičku o platební kartu a poslal/a bych mu to já sám/a. *Četnost odpovědí 2/0.*
4. Poprosil/a bych kamaráda nebo někoho jiného o platební kartu a poslal/a bych mu to já sám/a. *Četnost odpovědí 1/0.*
5. Poprosil/a bych rodiče nebo někoho jiného, aby mu to oni sami poslali. *Četnost odpovědí 9/7.*
6. Nejdřív bych si ověřil/a, jestli mi napsal skutečně můj kamarád. *Četnost odpovědí 51/41.*
7. Nereagoval/a bych vůbec na to. *Četnost odpovědí 30/42.*
8. Odmítl/a bych to poslat. *Četnost odpovědí 53/50.*

27. Žádal Tě někdy někdo (např. kamarád) přes sociální síť (např. přes Facebook) o zaslání drobné platby nebo přeposlání nějakého kódu z mobilu? *Na tuto položku odpovědělo 114 žáků 9. tříd a 116 žáků 6. tříd.*

1. Ano, byl to podvod, přišel/přišla jsem o peníze. *Četnost odpovědí 1/0.*
2. Ano, byl to podvod, ale nereagoval/a jsem na to. *Četnost odpovědí 4/2.*
3. Ano, ale podvod to nebyl. *Četnost odpovědí 17/3.*
4. Nikdo to po mně nikdy nechtěl. *Četnost odpovědí 95/111.*

28. Kdyby Ti přišla SMS zpráva (nebo zpráva do messengeru), že byl tvůj facebookový účet napaden a musíš se k němu přihlásit přes odkaz v této SMS zprávě, udělal/a bys to? *Na tuto položku odpovědělo 113 žáků 9. tříd a 115 žáků 6. tříd.*

1. ANO. *Četnost odpovědí 11/10.*
2. NE. *Četnost odpovědí 102/105.*

29. Byl/a jsi někým poučen/a, na co si dávat pozor při internetovém nakupování, abys nebyl/a podveden/a, např. v internetovém bazaru, v aukci, v e-shopu? *Na tuto položku odpovědělo 114 žáků 9. tříd a 117 žáků 6. tříd.*

1. Ano, ve škole. *Četnost odpovědí 35/50.*
2. Ano, rodiči. *Četnost odpovědí 53/69.*
3. Ano, kamarádem. *Četnost odpovědí 15/9.*
4. Ano, někým jiným. *Četnost odpovědí 13/9.*
5. Sám/a jsem si o tom četl/a, slyšel/a. *Četnost odpovědí 49/19.*
6. Ne, nikým. *Četnost odpovědí 15/24.*

30. Byl/a jsi někým poučen/a, co je to podvodná metoda phishing? *Na tuto položku odpovědělo 112 žáků 9. tříd a 113 žáků 6. tříd.*

1. Ano, ve škole. *Četnost odpovědí 4/5.*
2. Ano, rodiči. *Četnost odpovědí 1/2.*
3. Ano, kamarádem. *Četnost odpovědí 4/0.*
4. Ano, někým jiným. *Četnost odpovědí 2/0.*
5. Sám/a jsem si o tom četl/a, slyšel/a. *Četnost odpovědí 14/6.*
6. Nevím co je to phishing. *Četnost odpovědí 92/100.*

31. Byl/a jsi někým poučen/a, co je to scam? *Na tuto položku odpovědělo 112 žáků 9. tříd a 115 žáků 6. tříd.*

1. Ano, ve škole. *Četnost odpovědí 8/5.*
2. Ano, rodiči. *Četnost odpovědí 9/8.*
3. Ano, kamarádem. *Četnost odpovědí 20/14.*
4. Ano, někým jiným. *Četnost odpovědí 10/6.*
5. Sám/a jsem si o tom četl/a, slyšel/a. *Četnost odpovědí 24/16.*
6. Nevím co je to scam. *Četnost odpovědí 58/75.*

32. Byl/a jsi někým poučen/a, jak reagovat na nevyžádaný email (spam) od cizí osoby? *Na tuto položku odpovědělo 114 žáků 9. tříd a 115 žáků 6. tříd.*

1. Ano, ve škole. *Četnost odpovědí 30/25.*
2. Ano, rodiči. *Četnost odpovědí 54/43.*
3. Ano, kamarádem. *Četnost odpovědí 12/7.*
4. Ano, někým jiným. *Četnost odpovědí 10/11.*
5. Sám/a jsem si o tom četl/a, slyšel/a. *Četnost odpovědí 26/17.*
6. Ne, nikým. *Četnost odpovědí 27/42.*

33. Byl/a jsi někým poučen/a, jak reagovat na nedovolené vniknutí (nabourání se) do Tvého účtu na sociální síti, např. na Facebooku, Instagramu apod.? *Na tuto položku odpovědělo 114 žáků 9. tříd a 115 žáků 6. tříd.*

1. Ano, ve škole. *Četnost odpovědí 13/20.*
2. Ano, rodiči. *Četnost odpovědí 21/42.*
3. Ano, kamarádem. *Četnost odpovědí 16/10.*
4. Ano, někým jiným. *Četnost odpovědí 8/12.*
5. Sám/a jsem si o tom četl/a, slyšel/a. *Četnost odpovědí 39/17.*
6. Ne. *Četnost odpovědí 43/43.*

34. Znáš nějakou internetovou stránku, na které si můžeš zjistit hodnocení a recenze internetových obchodů (e-shopů)? *Na tuto položku odpovědělo 114 žáků 9. tříd a 114 žáků 6. tříd.*

1. ANO. *Četnost odpovědí 49/28.*
2. NE. *Četnost odpovědí 65/86.*

Pokud ano tak jakou:

1. Heureka. *Četnost odpovědí 28/5.*
2. Neuvedli nic. *Četnost odpovědí 25/8.*
3. Alza. *Četnost odpovědí 6/10.*
4. CZC. *Četnost odpovědí 2/4.*
5. Google. *Četnost odpovědí 1/2.*
6. Wish. *Četnost odpovědí* 1/1.

35. Setkal/a ses někdy s takovým virem, který Ti zablokoval mobil, tablet nebo počítač a chtěl za odblokování zaplatit peníze? *Na tuto položku odpovědělo 114 žáků 9. tříd a 113 žáků 6. tříd.*

1. ANO. *Četnost odpovědí 12/17.*
2. NE. *Četnost odpovědí 102/96.*

Dívka. *Četnost odpovědí 59/59.*
Chlapec. *Četnost odpovědí 56/58.*

Příloha č. 4 – dotazník pro školní metodiky prevence.

Vážení školní metodici prevence,

v České republice je zaznamenáván každým rokem nárůst podvodů páchaných prostřednictvím informačních a komunikačních technologií, zejména na internetu. Dané důvody nás vedly k provedení dotazníkového šetření na dané téma.

Získané informace budou využity pro zjištění aktuálního stavu v oblasti prevence před uvedenou kriminalitou, proto Vás prosíme o úplné a pravdivé vyplnění tohoto anonymního dotazníku. Při jeho vyplňování zakroužkujte jednu odpověď, případně dopište k odpovědi poznámku. Děkujeme za spolupráci.

Za výzkumný tým Michal Jančík, policista vyšetřující trestnou činnost a zároveň student Pedagogické fakulty, Univerzity Palackého v Olomouci, obor Veřejná správa.

---

1. **Vyskytl se na Vaší škole případ podvodného jednání v prostředí informačních a komunikačních technologií, v němž byl žák v roli oběti nebo pachatele?**

ANO, pachatel byl žák.
ANO, oběť (poškozený) byl žák.
NE

Poznámka:

---

2. **Existuje na Vaší základní škole preventivní program zaměřený proti podvodnému jednání[50] v prostředí informačních a komunikačních technologií pro žáky 2. stupně?**

ANO, přímo proti různým podvodům.
ANO, ale jen částečně s jiným preventivním programem prevence (např. s kyberšikanou).
NE

Poznámka:

---

[50] Podvody při nakupování na internetu (aukce, bazary, e-shopy), phishing, pharming, smishing, vishing,wangiri, scam, rizika malware, hoax, skimming, podvodné profily na sociálních sítích.

3. **Pokud existuje na Vaší základní škole takový preventivní program, byl tento program evaluován[51]? Případně napište kým, např. žáky, ředitelem, pedagogy, rodiči apod.**

ANO, byl evaluován.

NE, nebyl evaluován.

NE, nemáme program proti podvodům.

Poznámka:

---

4. **Jaký máte názor k nutnosti preventivního programu zaměřeného přímo proti podvodnému jednání v prostředí informačních a komunikačních technologií pro žáky 2. stupně?**

Stručná odpověď:

---

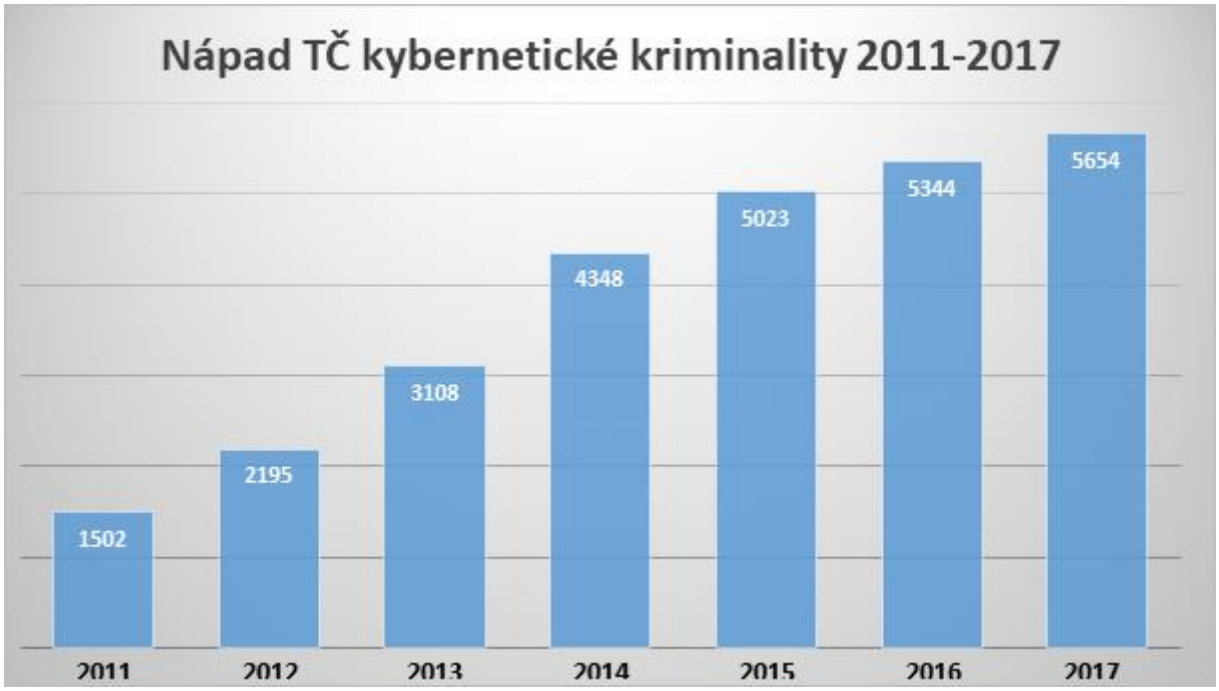
5. **Jak byste řešili, kdyby za Vámi přišel žák, že byl podveden např. při nákupu zboží na internetu?**

Stručná odpověď:

Děkuji za vyplnění.

[51] Evaluace znamená vyhodnocení, posouzení kvality a hodnoty.

Příloha č. 5 – doplňující tabulky a grafy k diplomové práci.



Graf č. 44 *– vývoj kybernetické kriminality 2011–2017 (Policie ČR, 2018a).*

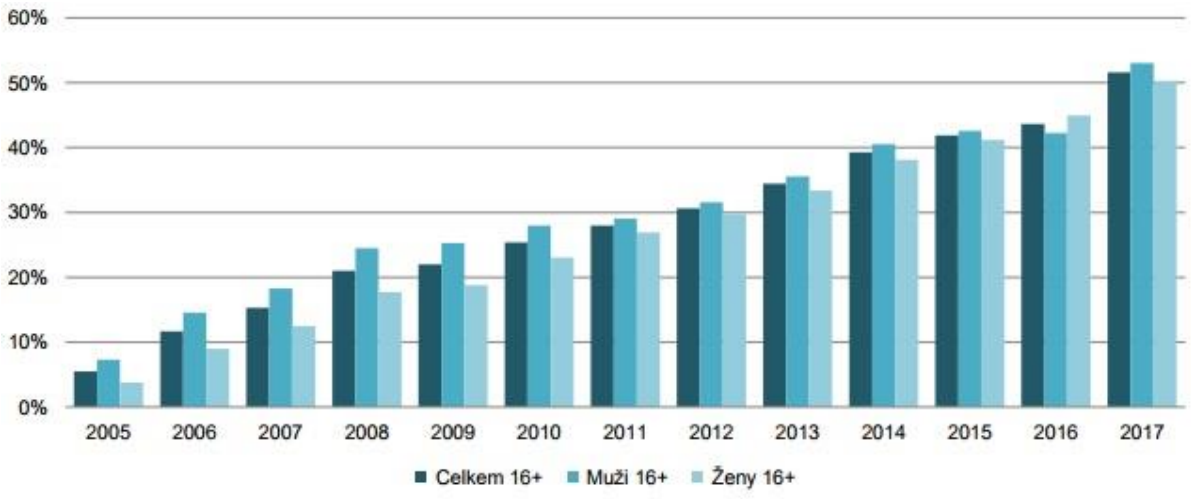
Tabulka č. 7 – vývoj kybernetické kriminality 2011–2017 podrobněji (Policie ČR, 2018a).

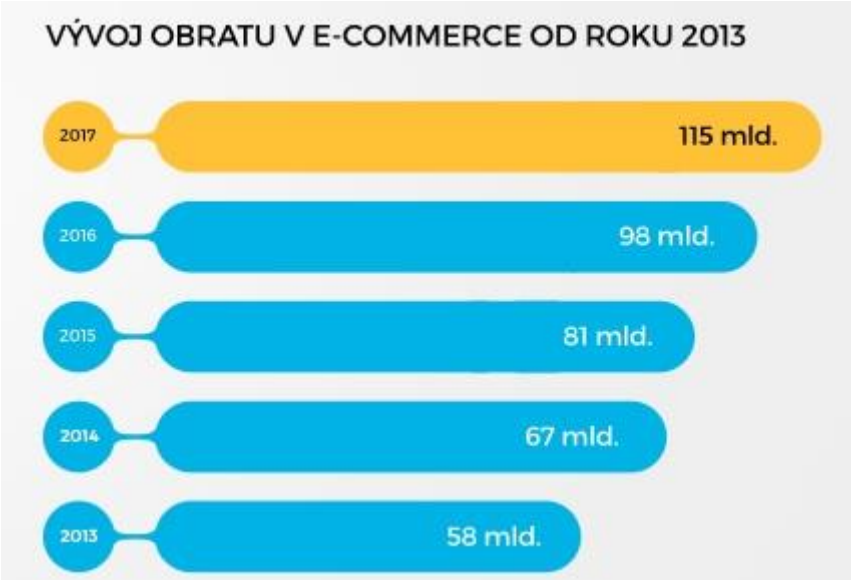
Struktura nápadu	2011	2012	2013	2014	2015	2016	2017
podvodná jednání	917	1303	1863	2478	2932	3235	3140
tj. %	*61,05*	*59,36*	*59,94*	*56,99*	*58,37*	*60,54*	*55,54*
hacking	66	112	220	555	578	534	608
tj. %	*4,39*	*5,10*	*7,08*	*12,76*	*11,51*	*9,99*	*10,75*
mravnostní delikty	132	161	261	314	351	344	561
tj. %	*8,79*	*7,33*	*8,40*	*7,22*	*6,99*	*6,44*	*9,92*
autorskoprávní delikty	155	241	181	262	315	237	296
tj. %	*10,32*	*10,98*	*5,82*	*6,03*	*6,27*	*4,43*	*5,24*
násilné projevy + hate crime	86	111	155	202	230	265	318
tj. %	*5,73*	*5,06*	*4,99*	*4,65*	*4,58*	*4,96*	*5,62*
ostatní	146	267	428	537	617	729	731
tj. %	*9,72*	*12,16*	*13,77*	*12,35*	*12,28*	*13,64*	*12,93*
Celkem nápad IT	**1502**	**2195**	**3108**	**4348**	**5023**	**5344**	**5654**

Tabulka č. 8a – jednotlivci nakupující na Internetu v ČR za období 2012–2017 dle procentuálního podílu z celkového počtu jednotlivců v dané socio-demografické skupině (Český statistický úřad, 2017b).

	2012	2013	2014	2015	2016	2017
Celkem 16+	**30,6**	**34,4**	**39,3**	**41,9**	**43,6**	**51,6**
Celkem 16-74	32,5	36,4	42,5	45,3	47,4	56,1
Pohlaví						
Muži 16+	31,5	35,6	40,5	42,6	42,3	53,0
Ženy 16+	29,8	33,4	38,1	41,2	44,9	50,3
Věková skupina						
16–24 let	46,3	53,9	62,2	60,6	58,7	69,8
25–34 let	54,3	58,3	63,2	66,9	72,0	79,1
35–44 let	43,1	46,9	52,6	59,2	59,4	70,9
45–54 let	27,9	32,4	40,1	41,2	46,6	56,2
55–64 let	15,7	19,8	21,7	25,7	28,3	38,6
65+	3,9	4,5	7,6	8,0	9,7	12,7
Vzdělání (25+)						
Základní	6,0	5,4	6,3	7,8	8,3	12,2
Střední bez maturity	18,7	21,3	23,5	26,6	30,5	35,3
Střední s maturitou + VOŠ	38,5	41,4	45,9	49,2	55,2	59,5
Vysokoškolské	50,7	53,8	61,4	62,1	61,5	77,3
Ekonomická aktivita						
Zaměstnaní	40,0	45,0	50,3	53,8	56,0	66,5
Nezaměstnaní	23,0	27,3	33,8	33,8	31,5	36,7
Ženy na RD*	51,0	55,1	64,6	65,5	72,4	77,6
Studenti	47,7	54,5	62,5	61,4	58,3	68,5
Starobní důchodci	4,7	6,4	8,4	9,9	11,4	14,5
Invalidní důchodci	14,5	15,7	19,4	17,3	22,8	28,4

Tabulka č. 8b – muži a ženy nakupující na Internetu v ČR za období 2005–2017 dle procentuálního podílu z celkového počtu jednotlivců v dané socio-demografické skupně (Český statistický úřad, 2017b).



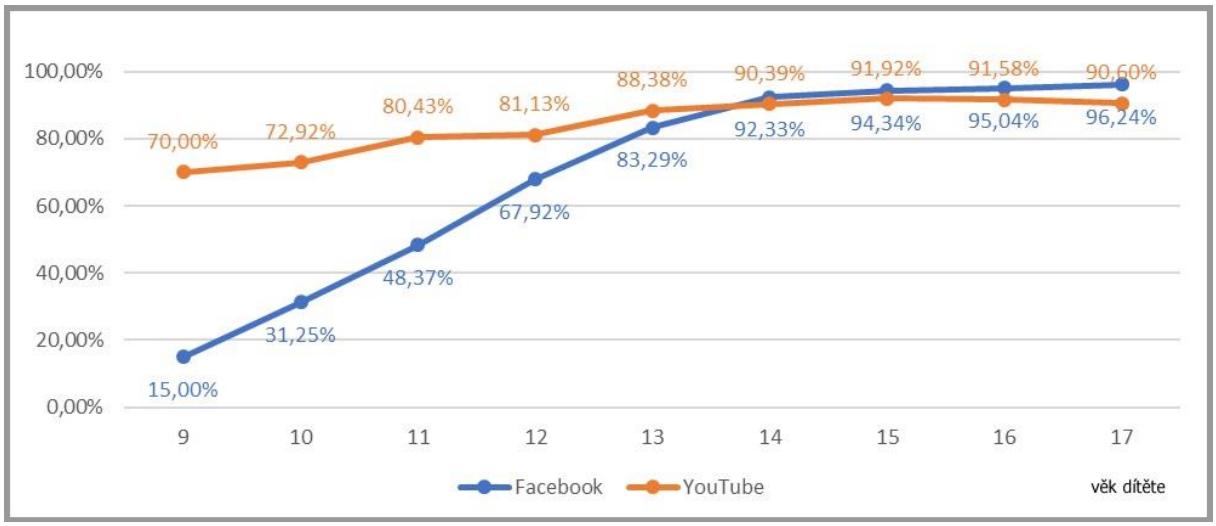


Graf č. 45 *– vývoj obratu e-komerce od roku 2013 (APEK.cz, 2017).*

Tabulka č. 9 – statistiky množství řešených incidentů (CSIRT.CZ, 2018).

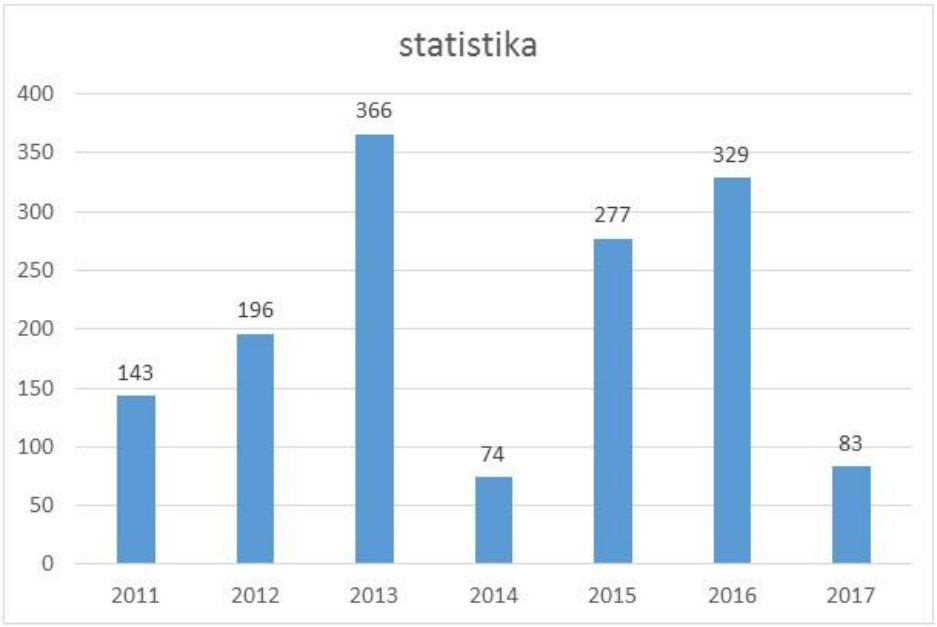
Druhy incidentů (otevřené a zavřené)

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	sum
IDS*				491	3924	2121	2380	3771	9944	13858	2193	38682
Phishing	65	220	209	144	159	175	368	367	363	409	101	2580
Spam	47	28	103	26	43	73	159	108	290	121	30	1028
Malware	53	134	121	10	20	45	117	240	104	99	10	953
Other	1	5	13	62	14	75	102	264	181	200	34	951
Trojan	66	6	26	5	5	12	56	90	79	94		439
Probe		3	14	25	12	26	86	42	13	26	2	249
DOS	2	4	2	2	68	72	32	37	12	14	2	247
Virus		84	99									183
Botnet		3	46	5	8	15		4	71	29		181
Portscan	10	4	1	6	1	3	2	5	6	13	1	52
Pharming							18	3	2	3	1	27
Unknown											1	1
sum	244	491	634	285	330	496	940	1160	1121	1008	182	6891

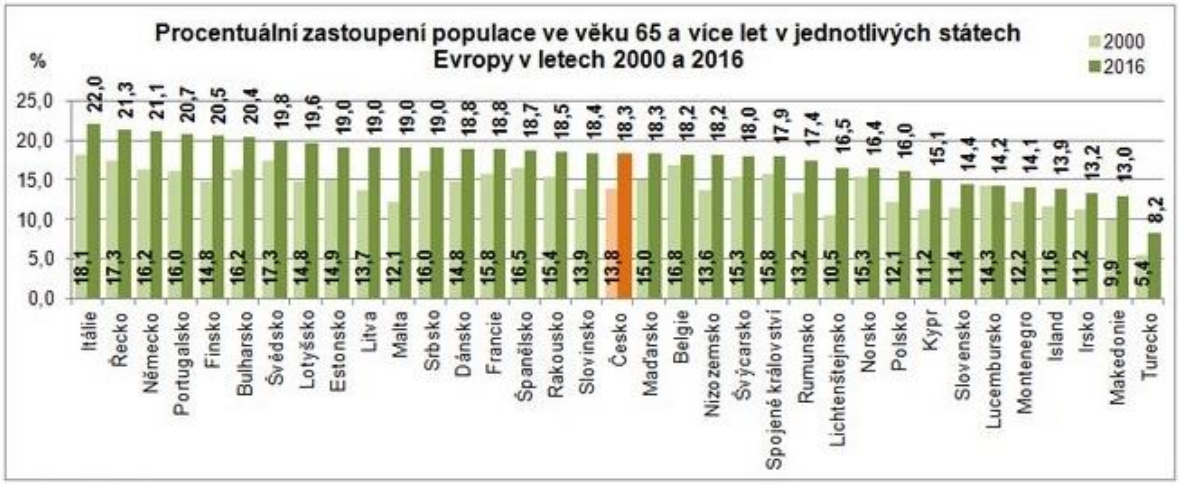


Graf č. 46 *– využívání Facebooku a Youtube podle věku dítěte (Kopecký, 2017b).*

Obrázek č. 1 – náhled na obrazovku počítače, zablokovaného ransomware vydávající se za Policii ČR (Macalíková, 2013).



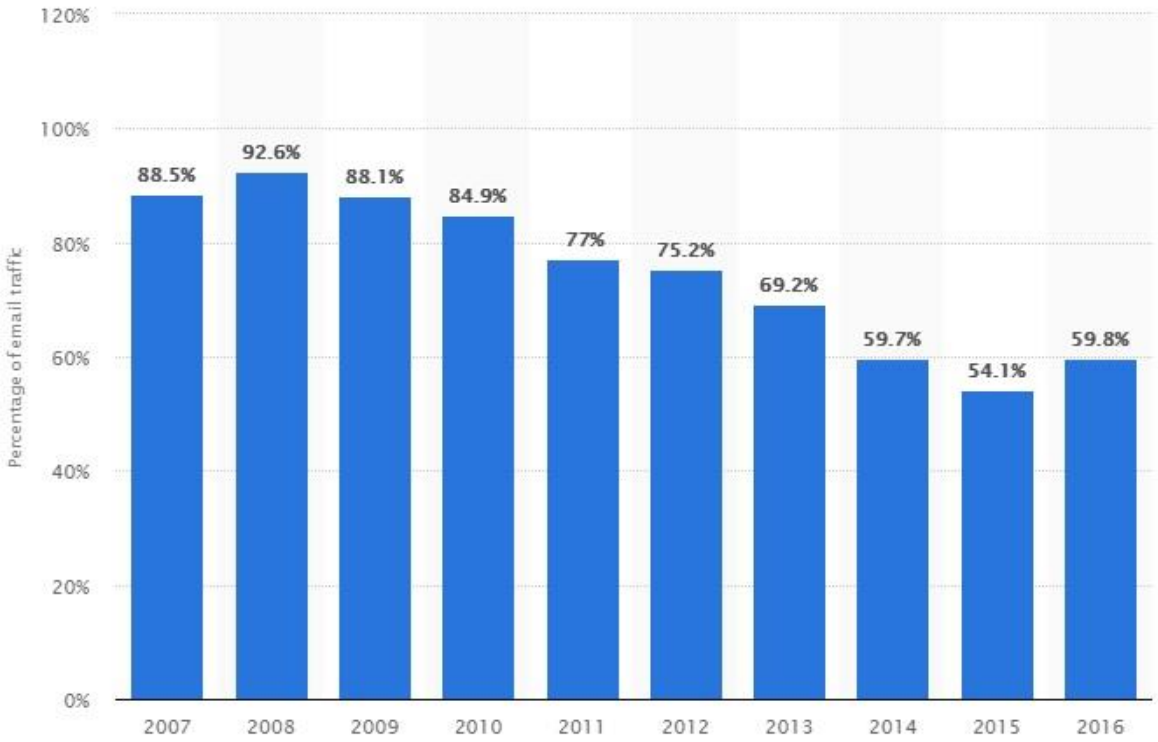
***Graf č. 47** – statistika výskytu skimmingu v ČR za období let 2013–2017 (Policie ČR, 2018c).*



***Graf č. 48** – procentuální zastoupení populace ve věku 65 let a více v jednotlivých státech Evropy za období 2000 a 2016 (Český statistický úřad, 2017a).*

Tabulka č. 10 – podíl z celkového počtu obyvatel ve věku 65 let a více za vybrané roky včetně předpokládaného vývoje vypracoval pro Eurostat Giannakouris (2008).

(%)	2008	2010	2020	2030	2040	2050	2060
EU27	**17.08**	**17.38**	**20.06**	**23.55**	**26.85**	**28.81**	**29.95**
BE	17.04	17.22	19.51	22.87	25.03	25.70	26.52
BG	17.31	17.47	20.34	23.28	26.70	31.26	34.21
CZ	14.64	15.39	20.22	22.94	26.32	30.94	33.38
DK	15.58	16.37	20.11	22.82	24.83	24.47	25.04
DE	20.05	20.57	22.79	27.61	31.06	31.71	32.47
EE	17.16	16.99	18.77	21.74	24.18	27.42	30.72
IE	11.16	11.33	13.28	16.02	19.36	23.74	25.20
EL	18.63	18.85	21.13	24.18	28.40	31.54	31.65
ES	16.61	16.69	18.18	22.13	27.66	32.11	32.34
FX	16.50	16.74	20.19	23.20	25.34	25.62	25.94
IT	20.08	20.34	22.68	26.15	30.82	32.62	32.71
CY	12.39	12.65	15.03	17.95	19.97	23.23	26.17
LV	17.27	17.36	18.57	22.18	25.43	29.58	34.38
LT	15.84	16.05	17.57	22.14	26.34	29.69	34.72
LU	14.15	14.28	16.20	19.57	22.20	22.99	23.57
HU	16.17	16.61	19.82	21.95	24.96	29.35	31.93
MT	13.83	14.76	20.34	24.20	25.69	29.05	32.43
NL	14.72	15.33	19.80	24.10	26.89	26.65	27.25
AT	17.17	17.56	19.36	23.69	27.23	28.17	28.98
PL	13.46	13.56	18.22	22.99	25.90	31.63	36.18
PT	17.42	17.79	20.08	23.25	26.83	30.12	30.85
RO	14.91	14.93	17.43	20.25	25.52	30.93	34.96
SI	16.08	16.62	20.42	25.29	29.08	32.50	33.44
SK	11.98	12.29	16.44	21.27	25.33	31.63	36.12
FI	16.52	17.06	22.41	25.52	26.21	26.81	27.82
SE	17.52	18.16	20.81	22.52	24.27	24.72	26.60
UK	16.10	16.38	18.29	20.55	22.45	22.95	24.74
NO	14.64	15.03	18.10	21.01	23.76	24.39	25.42
CH	16.41	16.93	19.65	23.38	26.13	27.00	28.01



***Graf č. 49** – globální procentuální četnost spamu v emailech v období 2007–2016 (Statista – The portal for statistics, 2018a).*

Příloha č. 6 – úplné znění zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů a úplné znění zákona č. 251/2016 Sb., o některých přestupcích, ve znění pozdějších předpisů.

Zákona č. 40/2009 Sb., trestní zákoník

§ 209 Podvod

(1) Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

(2) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 a byl-li za takový čin v posledních třech letech odsouzen nebo potrestán.

(3) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 větší škodu.

(4) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny,

b) spáchá-li takový čin jako osoba, která má zvlášť uloženou povinnost hájit zájmy poškozeného,

c) spáchá-li takový čin za stavu ohrožení státu nebo za válečného stavu, za živelní pohromy nebo jiné události vážně ohrožující život nebo zdraví lidí, veřejný pořádek nebo majetek, nebo

d) způsobí-li takovým činem značnou škodu.

(5) Odnětím svobody na pět až deset let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu, nebo

b) spáchá-li takový čin v úmyslu umožnit nebo usnadnit spáchání teroristického trestného činu, trestného činu financování terorismu (§ 312d) nebo vyhrožování teroristickým trestným činem (§ 312f).

(6) Příprava je trestná.

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,

b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,
c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo
d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,
bude potrestán odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci.
(3) Odnětím svobody na šest měsíců až čtyři léta, zákazem činnosti nebo propadnutím věci bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2
a) v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, nebo
b) v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat.
(4) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,
b) způsobí-li takovým činem značnou škodu,
c) způsobí-li takovým činem vážnou poruchu v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci,
d) získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo
e) způsobí-li takovým činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem.
(5) Odnětím svobody na tři léta až osm let bude pachatel potrestán,
a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo
b) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 234 Neoprávněné opatření, padělání a pozměnění platebního prostředku

(1) Kdo sobě nebo jinému bez souhlasu oprávněného držitele opatří, zpřístupní, přijme nebo přechovává platební prostředek jiného, zejména nepřenosnou platební kartu identifikovatelnou podle jména nebo čísla, elektronické peníze, příkaz k zúčtování, cestovní šek nebo záruční šekovou kartu, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

(2) Kdo sobě nebo jinému opatří, zpřístupní, přijme nebo přechovává padělaný nebo pozměněný platební prostředek, bude potrestán odnětím svobody na jeden rok až pět let.
(3) Kdo padělá nebo pozmění platební prostředek v úmyslu použít jej jako pravý nebo platný, nebo
kdo padělaný nebo pozměněný platební prostředek použije jako pravý nebo platný,
bude potrestán odnětím svobody na tři léta až osm let.
(4) Odnětím svobody na pět až deset let nebo propadnutím majetku bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1, 2 nebo 3 jako člen organizované skupiny, nebo
b) spáchá-li takový čin ve značném rozsahu.
(5) Odnětím svobody na osm až dvanáct let nebo propadnutím majetku bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1, 2 nebo 3 jako člen organizované skupiny působící ve více státech, nebo
b) spáchá-li takový čin ve velkém rozsahu.
(6) Příprava je trestná.

§ 181 Poškození cizích práv

(1) Kdo jinému způsobí vážnou újmu na právech tím, že
a) uvede někoho v omyl, nebo
b) využije něčího omylu,
bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.
(2) Odnětím svobody až na tři léta bude pachatel potrestán,
a) způsobí-li činem uvedeným v odstavci 1 jinému značnou újmu na právech,
b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo
c) vydává-li se při takovém činu za úřední osobu.
(3) Odnětím svobody na šest měsíců až pět let bude pachatel potrestán,
a) způsobí-li činem uvedeným v odstavci 1 jinému újmu na právech velkého rozsahu, nebo
b) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 182 Porušení tajemství dopravovaných zpráv

(1) Kdo úmyslně poruší tajemství
a) uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením,

b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo

c) neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data,

bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

(2) Stejně bude potrestán, kdo v úmyslu způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch

a) prozradí tajemství, o němž se dozvěděl z písemnosti, telegramu, telefonního hovoru nebo přenosu prostřednictvím sítě elektronických komunikací, který nebyl určen jemu, nebo

b) takového tajemství využije.

(3) Odnětím svobody na šest měsíců až tři léta nebo zákazem činnosti bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,

b) spáchá-li takový čin ze zavrženíhodné pohnutky,

c) způsobí-li takovým činem značnou škodu, nebo

d) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(4) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako úřední osoba,

b) způsobí-li takovým činem škodu velkého rozsahu, nebo

c) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

(5) Zaměstnanec provozovatele poštovních služeb, telekomunikační služby nebo počítačového systému anebo kdokoli jiný vykonávající komunikační činnosti, který

a) spáchá čin uvedený v odstavci 1 nebo 2,

b) jinému úmyslně umožní spáchat takový čin, nebo

c) pozmění nebo potlačí písemnost obsaženou v poštovní zásilce nebo dopravovanou dopravním zařízením anebo zprávu podanou neveřejným přenosem počítačových dat, telefonicky, telegraficky nebo jiným podobným způsobem,

bude potrestán odnětím svobody na jeden rok až pět let, peněžitým trestem nebo zákazem činnosti.

(6) Odnětím svobody na tři léta až deset let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 5 škodu velkého rozsahu, nebo

b) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

Zákona č. 251/2016 Sb., o některých přestupcích

§ 8 přestupek proti majetku

(1) Fyzická osoba se dopustí přestupku tím, že úmyslně

a) způsobí škodu na cizím majetku

1. krádeží,

2. zpronevěrou,

3. **podvodem**, nebo

4. zničením nebo poškozením věci z takového majetku;

pokus tohoto přestupku je trestný,

b) neoprávněně užívá cizí majetek,

c) přisvojí si cizí věc nálezem nebo jinak bez přivolení oprávněné osoby, nebo

d) ukryje, užívá nebo na sebe anebo na jiného převede věc, která byla získána přestupkem spáchaným jinou osobou, nebo to, co za takovou věc bylo opatřeno.

(2) Právnická nebo podnikající fyzická osoba se dopustí přestupku tím, že

a) způsobí škodu na cizím majetku

1. krádeží,

2. zpronevěrou,

3. podvodem, nebo

4. zničením nebo poškozením věci z takového majetku;

pokus tohoto přestupku je trestný,

b) neoprávněně užívá cizí majetek,

c) přisvojí si cizí věc nálezem nebo jinak bez přivolení oprávněné osoby, nebo

d) ukryje, užívá nebo na sebe anebo na jiného převede věc, která byla získána přestupkem spáchaným jinou osobou, nebo to, co za takovou věc bylo opatřeno.

(3) Přestupku podle odstavce 1 písm. a) se dopustí též organizátor, návodce nebo pomocník.

(4) Za přestupek podle odstavců 1 až 3 lze uložit pokutu do 50000 Kč.

(5) Je-li přestupek podle odstavců 1 až 3 spáchán opakovaně po nabytí právní moci rozhodnutí o přestupku podle stejného odstavce, uloží se pokuta do 70000 Kč.

(6) Za přestupek podle odstavce 1 nebo 3 lze uložit omezující opatření.

(7) Řízení o přestupku podle odstavce 1 nebo 3 spáchaném mezi osobami blízkými lze zahájit a v již zahájeném řízení pokračovat pouze se souhlasem osoby přímo postižené spácháním přestupku.

Příloha č. 7 - rady a tipy před podvodným jednáním v prostředí informačních a komunikačních technologií.

Aukční portály

Při nakupování na aukčních portálech je třeba si dávat pozor na následující oblasti:

- **Podezřele nízká cena prodávaného zboží** – na aukčních portále je možné zboží zakoupit v klasické dražbě, nebo bez nutnosti dražby. Na aukčním portále Aukro je taková možnost nákupu označena „*Kup ted*".
- **Platba za zboží pouze předem na účet** – dobírka ani osobní předání není možné, mnohdy nelze ani kontaktovat prodejce zboží, což je velmi rizikové! Aukční portály mohou nabízet také možnost platby na účet prodejce prostřednictvím tzv. PayU (rychlé platby).
- **Prodejce má na aukčním portále krátce založený účet** – nedávno registrovaný prodejce s málo komentáři od nakupujících může představovat možné riziko, obzvláště pokud prodává zboží vysoké hodnoty.
- **Prodejce nemá žádné hodnotící komentáře, nebo minimum** – prodejce, který má minimum komentářů od nakupujících představuje riziko, pokud prodává drahé zboží.
- **Hodnotící komentáře nebo stanoviska má prodejce jen od jednoho či dvou kupujících** – pokud má prodejce mnoho komentářů, ale jen od jednoho či dvou kupujících, jedná se největší pravděpodobností o podvodné komentáře!
- **Prodejce prodával v minulosti levné zboží a najednou začne prodávat drahé nebo velmi žádané zboží** – prodejce tím, že prodá velmi levné zboží, získá kladné hodnotící komentáře. Pokud následně nabízí drahé zboží, představuje toto jednání opět riziko Szotkowski (2016a).

Důležité je rovněž prostudování obchodních podmínek provozu i užívání konkrétního aukčního portálu, abychom věděli jako uživatelé, co je a není dovoleno, na co máme právo, pokud nás jiný uživatel podvede. Na Aukru.cz funguje Program ochrany kupujících. Pokud se uživatel stane obětí podvodu, má možnost kontaktovat pracovníky Aukra.cz a požadovat náhradu škody dokonce v plné výši, která mu bude asi do 14 dní zaplacena. Z tohoto důvodu je podstatné nepodceňovat licenční ujednání u internetových aukčních portálů, abychom eliminovali co nejvíce možnost, že budeme podvedeni (Szotkowski, 2016a).

E-shopy

*„**Na co si dát pozor při nakupování v e-shopu**:*

- *Podezřele nízká cena prodávaného zboží.*
- *Chybějící kontaktní údaje – e-shop na stránkách nemá kontaktní údaje, eventuálně nabízí kontakt jen přes kontaktní formulář.*
- *Nefunkční kontaktní údaje.*
- *Krátká doba registrace domény e-shopu, krátká existence provozovatele e-shopu.*
- *Vlastník domény (provozovatel e-shopu) neuvádí svou identitu, nebo se skrývá.*
- *Chybějící, neúplné, podezřelé, chaotické obchodní podmínky e-shopu.*
- *Chybějící reference e-shopu, chybějící hodnocení e-shopu zákazníky.*
- *Vymyšlené reference e-shopu, vymyšlené hodnocení e-shopu zákazníky.*
- *Záporné reference e-shopu, záporné hodnocení e-shopu zákazníky.*
- *Platba za objednané zboží pouze předem, dobírka není možná – tyto podmínky jsou velice rizikové! Za těchto okolností je tedy lepší najít jiný obchod nabízející stejné zboží, ale se všemi možnostmi plateb za jeho objednání*.“ (Szotkowski, 2016)

Elektronické obchody je vhodné si rovněž ověřovat prostřednictvím Asociace pro elektronickou komerci (apek.cz). Hodnocení a reference internetových obchodů lze pak nalézt na internetových cenových srovnávačích nebo obdobných stránkách, např. heureka.cz, firmy.cz, zboží.cz, nejlepsiceny.cz, apod. Identifikační číslo (IČ nebo IČO) lze na internetu ověřit pak prostřednictvím obchodního rejstříku na www.or.justice.cz.

Před samotným nákupem u on-line prodejců, lze k jejich ověření využít také informací na internetových stránkách České obchodní inspekce. V sekci „*Pro Spotřebitele*“ jsou uváděny „*Rizikové e-shopy.“* Taktéž organizace dTest nabízí bezplatnou možnost ověřování důvěryhodnosti e-shopů, a to na stránce www.dtest.cz/eshopy (Svoboda, 2017).

Před nákupem je vhodné posoudit, jakým způsobem se obchodník prezentuje. Webové stránky „*šité horkou jehlou*“ s gramatickými chybami nám mohou něco napovědět. Také je neprofesionální umístění webu na bezplatném hostingovém serveru, ani používání emailových adres, který si může založit každý (např. seznam.cz, gmail.com, yahoo.com). Také je třeba kontrolovat konečnou cenu zboží/služby, jelikož nejlevnější nabídka neznamená nejnižší celkovou (konečnou) cenu (Oškrdalová, 2012, s. 132–134).

Internetové bazary

„Na co si dát pozor při nakupování na internetových bazarech:

- ***Chybějící autentická fotografie nabízeného zboží*** *– v inzerátu chybí autentická fotografie zboží a prodejce ani po vyžádání fotografii nechce nebo „nemůže“ zaslat.*
- ***Inzerát napsán špatnou češtinou****.*
- ***Inzerát nabízející zboží nebo službu s „nadpřirozeným“ účinkem*** *– produkt nabízející rychlé zhubnutí, rychlé nabytí svalové hmoty, rychlé zvládnutí cizího jazyka apod.*
- ***Podezřele nízká cena nabízeného zboží****.*
- ***Nemožnost osobního předání nebo dobírky*** *– prodejce odmítá předat zboží při osobním kontaktu nebo jej zaslat na dobírku. Často se vymlouvá na špatné zkušenosti s dobírkou apod.*
- ***Platba za zboží pouze předem*** *– prodejce podmiňuje prodej zboží zasláním peněz předem na číslo účtu nebo na elektronickou peněženku (PayPal, PaySec).*
- ***Důvěryhodnost prodávajícího podpořena okopírovanými a zaslanými doklady*** *– podvodníci svou důvěryhodnost často podpoří nabídkou zaslání okopírovaných osobních dokladů. Doklady jsou ovšem často kradené.*
- ***Po zaslání peněz na účet prodejce odmítá zaslat číslo zásilky nebo přestane komunikovat úplně*** *– pokud prodejce na vyzvání odmítá poslat potvrzení o zaslání zásilky, číslo zásilky nebo přestane úplně komunikovat, je velká pravděpodobnost, že jste se stali obětí podvodníka*.“ (Szotkowski, 2016c).

Při přebírání zboží je vhodné zásilku ihned zkontrolovat, zda není poškozena, zda má správnou hmotnost a velikost. Pokud je to možné, zásilku rozbalujte a zkontrolujte při přebírání (Oškrdalová, 2012, s. 136).

Nakupujeme-li přes internet, je rovněž vhodné si veškerou komunikaci s prodejcem uchovat. Pokud pak došlo k podvodu a v balíku není objednané zboží, věc je třeba oznámit co nejdříve na místně příslušné oddělení Policie ČR. Možné je rovněž doručený balík reklamovat přímo u přepravce, čímž se pozdrží převod dobírkové částky.

Phishing

Základem phishingu je prevence a dodržování snadných zásad:

- *V počítači mít vždy nainstalován antivirový program, který umožňuje identifikovat nebezpečné viry v přílohách emailů či jiných zpráv.*
- *Antivirovou ochranou vybavit také svůj smarthone či tablet.*
- *Pro přihlašování do internetového bankovnictví vždy používat oficiální internetové stránky bankovní instituce (nikoli odkazy v emailech).*
- *Pravidelně aktualizovat operační systém i jednotlivé programy.*
- *Neotvírat přílohy emailů z neznámých zdrojů, neklikat na odkazy v těchto emailech.*
- *Při zadávání hesel na internetu kontrolovat, zdali je přenos dat zabezpečen (adresa začíná https://).*
- *Pokud možno nevypínat firewall v operačním systému.*
- *Jakékoli otázky spojené s informacemi o podezřelých platbách vždy konzultovat přímo s bankovní institucí – ideálně osobně či telefonicky.*
- *V případě potřeby navštívit stránky České bankovní asociace (www.czech-ba.cz), která informace o různých formách hackerských útoků zveřejňuje. Ověřovat si informace např. na webových stránkách www.hoax.cz.*
- *V internetovém prohlížeči si aktivovat antiphishingový filtr.“* (Kopecký, 2015b, s. 98).

Ke snížení rizik phishingu lze zmínit, že na všemožné zprávy (sms, emaily, dopisy, telefonáty a další různé vzkazy), vyzývající nás k zadání citlivých údajů, bychom neměli vůbec reagovat. Bankovní a další instituce citlivé údaje touto cestou údaje nepožadují. Pokud je v doručené zprávě odkaz na webové stránky, kam je třeba kliknout a vyplnit formulář, není vhodné na něj vůbec klikat. Při tomto jednání není vyloučen ani útok např. napadnutí počítače. Při přihlašování k elektronickému bankovnictví, sociálním sítím apod. je vhodnější nepoužívat přednastavené adresy, ale tyto přímo vepisovat do adresního řádku. Přitom je důležité dbát na přesnost zadávání a vyloučit překlepy jelikož podvodníci mnohdy užívají stránky podobné originálu. Při nestandartním chování systému je vhodnější operaci přerušit a kontaktovat příslušný subjekt (Oškrdalová, 2012, s. 92–93).

Dalším bezpečnostním aspektem je kontrola pravosti stránek prostřednictvím ověření certifikátu. To lze obvykle provést ve webovém prohlížeči kliknutím na symbol zámku, nacházející se zpravidla v rohu na liště. Ke snížení rizika odčerpání prostředků z účtu je vhodné užívání zasílání autorizačních SMS od banky k zamýšlené transakci. V každém případě

je třeba dodržovat zásady bezpečného užívání počítačového systému a internetu, používat antivirové aktualizované programy, firewally, nestahovat neznámé programy, neklikat na neznámé odkazy apod. (Oškrdalová, 2012, s. 93–94).

Uživatel IT by si měl být vždy vědom i toho, že ukládání přístupových hesel pro následné automatické přihlášení pro něj v elektronickém světě představuje hrozbu a měl by se takového jednání vyvarovat (Oškrdalová, 2012, 107–108).

Falešné profily na Facebooku

Pokud nás někdo přes sociální síť požádá o provedení nějakého úkonu, např. znovupřidání kamaráda, přeposlání kódu, zaslání tel. čísla, přihlášení se k účtu, odeslání platby, v tomto případě Kopecký (2013) upozorňuje, že obecně platí stejná zásada v reálném světě jako na sociální síti „*důvěřuj, ale prověřuj*“. Ideálním řešením je, takové údaje vůbec nepředávat.

*„**Obrana před útoky spojenými s klonovanými profily**:*

- *Nastavit si soukromí na svém účtu tak, aby neznámí lidé neviděli seznam přátel.*
- *Ověřit si identitu žadatele o přátelství - třeba tím, že mu zatelefonujeme.*
- *Nikdy nevyužívat v prostředí sociálních sítí m-platby, nikomu neposílat platební kódy.“* (Kopecký, 2017c).

Hacking účtu sociální sítě

Jak zjistíme, že byl náš účet na sociální síti napaden?

*„Někdy může být těžké zjistit, zda byl náš účet opravdu napaden – zejména v případě, že **útočník provádí pouze malé změny**. Ovšem některé běžné příznaky, že je náš účet v ohrožení, jsou následující:*

- ***Automatické „lajky“**, following, přijmutí nových přátel, oblíbené stránky atd.*
- *Soukromé **zprávy poslané přátelům.***
- *Neočekávaná **oznámení ze sociálních sítí** (např. varování, že byla změněna vaše emailová adresa).*
- *Nákupy, které jste neprovedli, nebo **přidání nových her či aplikací.***
- ***Aktualizace stavu/tweety**, které jste nepsali.*
- ***Změny** v profilu.“* (Objevit.cz, 2013).

Co dělat, pokud je náš účet na sociální síti skutečně v ohrožení?

V takové situaci je třeba zachovat chladnou hlavu, mnohdy získat zpět kontrolu nad svým účtem je jednodušší, než by se mohlo zdát. V takové situaci je nutné provést následující kroky:

- *„Okamžitě změňte heslo ke svému účtu a ujistěte se, že je jedinečné a že ho používáte pouze pro tento účet. Stejně tak změňte i heslo k emailu, na který je účet vázaný.*
- *Navštivte web sociální sítě a odstraňte autentizaci všech aplikací, které neznáte. Pokud se účet i nadále bude chovat nevyzpytatelně, není špatné zvážit zrušení přístupu všem aplikacím.*
- *Zajistěte, aby byla vaše emailová adresa stále nastavena jako výchozí pro váš účet, abyste byli schopni se přihlásit.*
- *Spusťte prohledávání vašeho počítače, abyste se ujistili, že jste nebyli napadeni virem.*
- *Obraťte se na lidi, kterým váš účet psal, a vysvětlete jim, že jste to nebyli vy, kdo odesílal zprávy*
- *Pokud si myslíte, že je příliš pozdě a že jste nad svým účtem již úplně ztratili kontrolu, nevěšte ještě hlavu. Ještě stále tu existuje několik způsobů, které mohou fungovat:*
- *Obnovte heslo pomocí odkazu „Zapomněli jste heslo?“ na titulní straně sociální sítě.*
- *Kontaktujte telefonicky nebo emailem podporu dané sociální sítě.“* (Objevit.cz, 2013).

Pharming

Opatření před pharmingem je obdobný, jako před phishingem. Spočívá tedy v bezpečném užívání počítače, resp. počítačového systému a internetu. Důležitou roli hraje pravidelně aktualizovaný antivirový program, firewall apod. Vhodné je užívání bezpečnostních opatření při provádění transakcí, tedy zasílání autorizačních zpráv SMS od banky při každé zadané transakci a používání tzv. certifikátu. Dále je důležitá fyzická kontrola stránek, aby nedošlo k přesměrování na stránky jiné, podobné. Při jakýchkoliv pochybností je lepší operaci přerušit a kontaktovat banku (Oškrdalová, 2012, s. 96).

Skimming

Při používání platebních karet bychom tedy měli dodržovat určitá základní bezpečnostní pravidla. Ta by měla spočívat v kontrole samotného zařízení, v němž bude karta použita a jeho okolí. Je třeba se přesvědčit, zda na zařízení nedošlo k nějaké úpravě, zda chybí některé kryty nebo jsou zde některá přídavná zařízení navíc. Neméně důležité je pozorovat,

zda místo nebo nás za zády někdo nesleduje. V případě pochybností je vhodnější zvolit storno operace a nepokračovat v ní. Při zadávání PINU je vhodné krytí druhou rukou, což znemožňuje zjištění PINU i případnou kamerou. V případě terminálů bychom neměli kartu nikdy dávat z ruky. Při podezřelém chování kontaktovat banku nebo Policii ČR (Oškrdalová, 2012 s. 87).

Hoax, Spam

- *„Nikdy nevěřme všem informacím, které nám z neznámého zdroje přijdou na e-mail. Vždy si informace ověřujme.*
- *Nikdy nesdělujme neznámým osobám naše osobní informace (PIN, rodné číslo apod.).*
- *Nikdy nedůvěřujme zprávám, které nám naše bankovní instituce posílá e-mailem. Bankovní instituce s klienty v případě důležitého sdělení tímto způsobem zpravidla nekomunikují.*
- *Vše si vždy ověřujme*.“ (Kopecký, 2008).

Jak se proti spamu bránit:

- *„Zbytečně nezveřejňovat svou e-mailovou adresu na internetu, tj. neregistrovat se v podezřelých, neznámých formulářích nebo soutěžích. (Na internetu jsou roboti, kteří sbírají e-mailové adresy za účelem rozesílání spamu.)*
- *Na konci zprávy bývá tlačítko Odhlásit (Unsubscribe). Správně by vás po kliknutí na odhlášení měla tato funkce skutečně odhlásit, ale pokud se jedná o podvodný e-mail, často se přihlásíte jen k odebírání dalších spamových zpráv. Pokud si tedy nejste stoprocentně jisti, že jde o newsletter či obchodní sdělení, k jehož zasílání jste dali dříve souhlas, neklikejte.*
- *Přemýšlejte, buďte ostražití a neotevírejte jakoukoli příchozí spamovou zprávu.*
- *Většina spamů je odesílána z uživatelova počítače bez jeho vědomí, protože je jeho počítač napaden virem. Doporučuje se tedy používat aktualizovaný operační systém + firewall + aktualizovaný antivir, jinak může rozesílat spam i váš počítač.“* (bezpečný internet.cz, 2017).

Jak postupovat, pokud je nám doručen spam:

- *„Vymažte, a to **bez jejich otevírání**, všechny podezřelé e-mailové hlavičky a/nebo e-mailové adresy, které často pocházejí od osob nebo organizací, jež neznáte.*
- *Otevíráte-li **soubory přiložené k elektronické poště**, buďte opatrní. Mohou obsahovat viry, které se aktivují ve chvíli, kdy je takový soubor otevřen.*
- *Instalujte na svém počítači kvalitní **antivirový program** a tzv. **firewall**, přičemž nezapomeňte dbát na jejich pravidelnou aktualizaci. Nedostatečně chráněný počítač může být prostřednictvím internetu někým zneužit k tomu, aby se sám stal rozesílatelem dalších spamů, aniž byste vy sami měli sebemenší tušení, že k něčemu takovému dochází. Ve vaší prodejně s výpočetní technikou jsou tyto programy běžně k dostání. Můžete je rovněž získat od vašeho poskytovatele internetového připojení.*
- *Neváhejte ani s instalací některého z **antispamových filtrů**, které jsou rovněž k dostání v příslušných obchodech. Filtraci spamů si můžete zařídit i prostřednictvím vašeho poskytovatele internetového připojení.*
- *Zřiďte si současně **několik různých elektronických adres**, přičemž vaši hlavní adresu poskytněte pouze těm osobám a organizacím, které znáte a k nimž máte naprostou důvěru.*
- *Je-li po vás požadována nějaká důvěrná informace v e-mailu, který podle všeho pochází od vaší banky nebo od jiného peněžního ústavu (například číslo vašeho bankovního účtu nebo přihlašovací kód), **ověřte si telefonicky**, zda takový požadavek skutečně pochází od uvedené instituce: tento typ žádostí je totiž velmi neobvyklý.*
- *Odesíláte-li svou elektronickou poštou na více e-mailových adres najednou, využívejte funkce **slepých kopií** - ostatní použité adresy se pak příjemcům nezobrazují.*
- *Příjem spamu můžete ohlásit úřadu, který má kompetence se touto věcí zabývat a disponuje právem takovou činnost penalizovat (viz OECD v oddíle Legislativa týkající se spamu).*
- *Chcete-li mít jistotu, že obsah vašich e-mailů by měl znát pouze a jenom jejich adresát, **kódujte** své důležité e-maily pomocí **šifrovacích programových prostředků**. Je to obdoba zapečetění dopisu odeslaného klasickou poštou.“* (Úřad pro ochranu osobních údajů, 2013).

Čeho bychom se měli vyvarovat:

- *„**Nenakupujte! Neodpovídejte!** Na spam nereagujte. Neobjednávejte a nekupujte produkty ani služby nabízené touto cestou a nereagujte ani na přihlašovací / odhlašovací (suscribe/unsuscribe) zaškrtávací políčka zobrazená ve spamových e-mailech nebo na odkazovaných webových stránkách. Nákupy, které vycházejí ze spamových nabídek leda podpoří a posílí nekalý spamový byznys. "Odhlášení" (tedy odmítnutí nabídky) slouží v tomto případě pouze k tomu, aby se spamer ujistil, že odeslal svůj e-mail na platnou elektronickou adresu. Takovou adresu pak může zahrnout do své databáze.*
- *Nereagujte ani na **falešná oznámení o virové nákaze** (tzv. **hoax**). Taková oznámení vás chtějí donutit, abyste učinili opatření proti údajným virům. Ve skutečnosti však o žádnou hrozbu počítačového viru nejde. Naopak samotné otevření této zprávy může váš počítač poškodit. V této souvislosti vás podobné zprávy často vyzývají, abyste je posílali dále, co největšímu počtu lidí. Hoax se tak šíří cestou řetězové reakce a může ohrozit i počítače dalších adresátů.*
- *Buďte opatrní, poskytujete-li někomu prostřednictvím elektronické pošty či internetu důvěrné informace o vaší osobě (číslo bankovního účtu, PIN kód, přihlašovací heslo apod. Raději si dobře rozmyslete, zda je poskytnutí těchto údajů nezbytné a zda osoba nebo organizace, která po vás takové údaje požaduje, je skutečně tím, za koho se vydává.*
- *Buďte ostražití i v situaci, kdy dáváte k dispozici vaše kontaktní informace (např. e-mailovou adresu, telefonní číslo, číslo faxu apod.). Dobře si zvažte, komu takové informace dáváte a kdo k nim pak může mít přístup.“* (Úřad pro ochranu osobních údajů, 2013).

Malware

Malwaru a dalších škodlivých programů se lze zbavit, nebo zcela zabránit jejich vniknutí do počítačového systému pomocí kvalitních antivirových programů. Takových programů však existuje celá řada a uživatel mnohdy neví, jaký je mezi nimi rozdíl. Vhodné je tedy sledovat jejich recenze a ověřená srovnání, které nabízí např. společnost Virus Bulletin (virusbulletin.com). V České republice se popisem a srovnáním těchto programů zabývá Antivirové centrum (antivirovecentrum.cz).

Kvalitní antivirových program nás ochrání nejen před nejrůznějšími druhy malware a viry, ale také např. před spamem, phishingem, neoprávněným používáním webkamery,

neoprávněným zašifrováním našich souborů (ransomware), nezvanými uživateli domácí sítě apod. Mohou rovněž pomáhat vyhledávat zařízení v případě ztráty/odcizení nebo šifrovat a bezpečně ukládat hesla a data v počítačovém systému.

Mezi kvalitní výrobce antivirových programů patří např. společnost ESET, která se pravidelně umisťuje na prvních místech při testování mezi antiviry od jiných společností (Antivirové centrum, 2018). Společnost ESET dokonce nabízí možnost zdarma a bez registrace základní kontroly počítače online přes internet službou ESET Online Scanner. Mobilní telefony a tablety zajišťuje pak Eset Mobile Security (ESET, 2018).

Wangiri

*„Na neznámá telefonní čísla ze zahraničí nikdy **nevolejte zpět**. Šlo by o zpoplatněný hovor podle cen volání do zahraničí.*“ Pokud hovor omylem stihneme zvednout, nic se neděje, za příchozí hovory nic neplatíme (pokud jsme v ČR nebo v EU). Na tyto hovory je nejlepší vůbec nereagovat. Podvodníci mohou telefonní čísla ale měnit, proto nelze zcela zabránit tomu, aby k prozvonění nedošlo (Vodafone.cz, 2018).

Pokud do zahraničí obvykle nevoláme a chceme mít jistotu, že omylem nezavoláme nazpět na takováto čísla, můžeme si odchozí volání do zahraničí zablokovat, a to například přes mobilního operátora (Vodafone.cz, 2018).

Seznam pramenů použitých v přílohách:

Aktuální hrozby a bezpečnostní rizika. In: Vodafone.cz [online]. 2018 [cit. 2018-05-08]. Dostupné z: https://www.vodafone.cz/pece/osobni-a-firemni/otazky/bezpecnost/aktualni-hrozby/?page=0

Co dělat, když je váš účet na sociální síti hacknutý. In: **Objevit.cz** [online]. **2013** [cit. 2018-04-27]. Dostupné z: http://objevit.cz/hacknuty-ucet-na-socialni-siti-t40102

ESET Online Scanner zkontroluje váš počítač. In: **ESET** [online]. 2018 [cit. 2018-04-15]. Dostupné z: https://www.eset.com/cz/online-scanner/

GIANNAKOURIS, Konstantinos. Ageing characterises the demographic perspectives of the European societies. Eurostat Statistic in focuc. In: Eurostat [online]. 2008 [cit. 2017-12-17]. Dostupné z: http://ec.europa.eu/eurostat/web/products-statistics-in-focus/-/KS-SF-08-072

Global spam volume as percentage of total e-mail traffic from 2007 to 2016. In: **Statista – The portal for statistics** [online]. **2018a** [cit. 2018-03-24]. Dostupné z: https://www.statista.com/statistics/420400/spam-email-traffic-share-annual/

Jak se bránit nevyžádaným e-mailům (leták OECD). In: **Úřad pro ochranu osobních údajů** [online]. 2013 [cit. 2018-01-16]. Dostupné z: https://www.uoou.cz/jak-se-branit-nevyzadanym-e-mailum-letak-oecd/ds-1495/p1=1495

KOPECKÝ, Kamil. Co je Hoax. In: E-bezpečí [online]. 2008 [cit. 2017-12-20]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/hoax-spam/91-25

KOPECKÝ, Kamil. Podvodné mobilní platby na Facebooku. In: E-bezpeci.cz [online]. 2013 [cit. 2018-01-16]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/sociotechnika/774-podvodne-platby-na-facebooku

KOPECKÝ, Kamil. České děti a Facebook 2015 výzkumná zpráva [online]. 2015b [cit. 2018-01-16]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/cat_view/27-

KOPECKÝ, Kamil. Klonování profilů jako klasická invazivní technika funguje velmi dobře na děti. V polovině případů si neověřují, zda je o přátelství žádají skutečně jejich spolužáci a kamarádi z reálného světa. In: E-bezpeci.cz [online]. 2017c [cit. 2018-01-16]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/sociotechnika/1253-klonovani-profilu

KOPECKÝ, Kamil. U dětí 1. stupně ZŠ dominuje YouTube. Facebook jej předežene až ve 14 letech věku dítěte. In: E-bezpeci.cz [online]. 2017b [cit. 2018-01-16]. Dostupné z: https://www.e-bezpeci.cz/index.php/veda-a-vyzkum/1256-facebook-vs-youtube

Kyberkriminalita. In: **Policie ČR** [online]. **2018a** [cit. 2018-02-15]. Dostupné z: http://www.policie.cz/clanek/kyberkriminalita.aspx

MACALÍKOVÁ, Jana. Objevuje se vám na monitoru podezřelé hlášení? In: Policie ČR [online]. 2013 [cit. 2017-12-10]. Dostupné z: http://www.policie.cz/clanek/objevuje-se-vam-na-monitoru-podezrele-hlaseni.aspx

OŠKRDALOVÁ, Gabriela. Modelování bezpečnostních rizik elektronického obchodu a elektronického bankovnictví. Brno, 2012. Dizertační práce. Masarykova Univerzita v Brně.

Senioři. In: **Český statistický úřad** [online]. **2017a** [cit. 2017-12-15]. Dostupné z: https://www.czso.cz/csu/czso/seniori

Spam. In: **Bezpečný internet.cz** [online]. 2018 [cit. 2018-02-27]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/e-mail/spam.aspx

Srovnání antivirových programů, srovnání antivirů. In: **Antivirové centrum** [online]. 2018 [cit. 2018-04-15]. Dostupné z: https://www.antivirovecentrum.cz/aktuality/srovnani-antiviru.aspx

Statistika skimmingu. In: **Policie ČR** [online]. **2018c** [cit. 2018-03-24]. Dostupné z: http://www.policie.cz/clanek/statistika-skimmingu.aspx

Statistiky řešených incidentů. In: **CSIRT.CZ** [online]. **2018** [cit. 2017-12-15]. Dostupné z: https://www.csirt.cz/page/2635/statistiky-resenych-incidentu/

SZOTKOWSKI, René. Rizika nakupování na aukčních portálech. In: E-bezpečí [online]. 2016a [cit. 2018-04-13]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/dali-rizika/1200-rizika-aukce

SZOTKOWSKI, René. Rizika nakupování v e-shopech In: E-bezpečí [online]. 2016b [cit. 2018-04-13]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/dali-rizika/1199-rizika-eshopy

SZOTKOWSKI, René. Rizika nakupování v internetových bazarech nebo inzertních portálech. In: E-bezpečí [online]. 2016c [cit. 2018-04-15]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/dali-rizika/1201-rizika-bazary

SVOBODA, Jakub. Jak se vyhnout podvodným e-shopům. In: Novinky.cz [online]. 2017 [cit. 2018-04-13]. Dostupné z: https://www.novinky.cz/finance/455359-jak-se-vyhnout-podvodnym-e-shopum.html

Vývoj obratu v e-commerce od roku 2013. In: **APEK.cz** [online]. **2017** [cit. 2018-01-10]. Dostupné z: https://www.apek.cz

Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci za období 2017. In: **Český statistický úřad** [online]. **2017b** [cit. 2018-01-08]. Dostupné z: https://www.czso.cz/documents/10180/46014700/06200417.pdf/a0bd4497-d2b6-450b-95f0-2f70c50786d5?version=1.1