**UNIVERZITA PALACKÉHO V OLOMOUCI**
**PEDAGOGICKÁ FAKULTA**

# Bakalářská práce

2014 Martin Vyhlídal

**UNIVERZITA PALACKÉHO V OLOMOUCI**

**PEDAGOGICKÁ FAKULTA**

Ústav pedagogiky a sociálních studií

BAKALÁŘSKÁ PRÁCE

Martin Vyhlídal

# Majetková kriminalita na internetu

Olomouc 2014

Vedoucí práce: PhDr. René Szotkowski, Ph.D.

**Prohlášení**

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a použil jen uvedených pramenů a literatury. Souhlasím, aby tato práce byla uložena na Univerzitě Palackého v Olomouci v knihovně Pedagogické fakulty a zpřístupněna ke studijním účelům.

V Olomouci dne 17. června 2014

……

Martin Vyhlídal

Děkuji PhDr. René Szotkowskému, Ph.D. za odborné vedení práce, poskytnutí řady dobrých rad a materiálových podkladů, jeho ochotu, vstřícnost a trpělivost, kterou mi věnoval a bez které by tato práce nevznikla.

# OBSAH

# Úvod

Internet je v současné době rozšířen do většiny domácností v České republice. Operátoři poskytující telekomunikační služby se předhánějí ve výhodnějších nabídkách, které mimo levného volání nabízejí také lákavé nabídky internetových tarifů, které si může dovolit snad opravdu každý.

Přístup k internetu již dlouho není podmíněn vlastnictvím stolního počítače, jak tomu bylo v minulosti. Nyní je internet dostupný téměř v každém mobilním telefonu, tabletu, netbooku či notebooku a nově také ze SMART televizorů, prostřednictvím herních a multimediálních zařízení.

Wi-Fi[1] připojení k síti internet nabízí zdarma celá řada právnických i fyzických osob v rámci svého podnikání, ale i státní orgány prosazující veřejný zájem.

Přístup k internetu poskytuje jeho uživatelům širokou škálu využití, ať už se jedná o rychlé získání informací, pohodlné nakupování, celosvětovou komunikaci, přístup ke vzdělání, různorodou zábavu a mnoho dalšího.

Internet má však i své stinné stránky. Jeho anonymitu využívají osoby se společensky nežádoucími úmysly, ať už se jedná o násilné, mravností nebo majetkové delikventy.

Dle policejních statistik se na internetu nejčastěji páchá právě majetková trestná činnost a to podvody, kterých bylo v první polovině roku 2013 zaevidováno v České republice na 714 případů. Druhé místo bylo ve stejném období připisováno mravnostním trestným činům, kterých bylo zaevidováno 117 případů[2].

Jen z tohoto poměrně krátkého časového úseku je zřetelné, jak je majetková kriminalita na internetu oproti ostatním druhům kriminality rozšířena.

Jelikož řadu let pracuji u Policie České republiky, kde jsem v poslední době osobně registroval nárůst této kriminality a navíc mě tato problematika zajímá i osobně, rozhodl jsem se bakalářskou práci zpracovat právě na téma „Majetková kriminalita na internetu“.

K tomu, abychom mohli účinným způsobem vyrazit do ofenzívy proti internetové kriminalitě nejen majetkového charakteru, je třeba vychovávat a vzdělávat především uživatele internetu. Skupina těchto uživatelů nemá prakticky žádné věkové hranice. Vzdělávání populace v dané problematice na všech věkových úrovních je velice obsáhlé téma.

---

1 Wireles Fidelity – bezdrátová síť pro vysokorychlostní síťové připojení (Nádběla, 2006, s. 479)

2 Přehled nejčastěji páchaných trestných činů za první polovinu roku 2013 – viz. příloha č. 1.

Vzhledem k uvedenému a také proto, že práce je vedena pod hlavičkou Pedagogické fakulty Univerzity Palackého v Olomouci, směřuje spíše do oblasti primární prevence osob mladistvých, částečně i nezletilců a to především v její praktické části.

Právě tato skupina osob je vnímána jako náchylnější k tomu stát se obětí této kriminality nebo jejím pachatelem.

Cílem teoretické části práce je definovat majetkovou kriminalitu na internetu s důrazem na její nejrozšířenější způsob provedení, dále zjistit, jaký byl vývoj této kriminality nejen na našem území a hlavně poskytnout výčet existujících způsobů prevence eliminující její další rozšiřování se zaměřením na vzdělávání mladistvých.

Teoretická část práce sice přesahuje do oblasti kriminality, avšak tento přesah kompenzuji částí praktickou, která je zaměřena naopak na oblast vzdělávací - pedagogickou.

Hlavním cílem praktické části práce je ověřit dotazníkovou metodou existenci preventivních programů zaměřených na problematiku majetkové kriminality na internetu.

Průzkum byl proveden u školních metodiků prevence na středních školách a gymnáziích v okrese Olomouc a pro porovnání byl realizován také na stejném počtu náhodně vybraných základních škol stejného okresu.

Jelikož se dle mého názoru jedná o aktuální téma, se kterým se mnoho uživatelů internetu dostává stále častěji do styku, věřím, že práce bude přínosem nejen pro širokou veřejnost, ale především pro pedagogické pracovníky, aby jim přiblížila danou problematiku a poskytla alespoň teoretické znalosti, jak ji identifikovat a kde v případě jejího výskytu hledat pomoc.

# I. TEORETICKÁ ČÁST

Hlavním cílem teoretické části práce je definovat majetkovou kriminalitu na internetu s důrazem na její nejrozšířenější způsob provedení, dále zjistit, jaký byl vývoj této kriminality nejen na našem území a hlavně poskytnout výčet existujících způsobů prevence eliminující její další rozšiřování, se zaměřením na vzdělávání mladistvých.

První kapitola teoretické části práce má za cíl vymezit základní pojmy týkající se majetkové kriminality na internetu a její prevence.

Dále považuji za vhodné poskytnout stručný pohled do historie počítačové kriminality, aby si čtenář uvědomil, jakým tempem tento druh kriminality roste, což je obsaženo ve druhé kapitole práce.

Cílem třetí kapitoly práce je popsat trestně právní rovinu majetkové kriminality na internetu se zaměřením na nejčastěji páchaný trestný čin, kterým je podvod.

Čtvrtá kapitola pojednává o aktérech majetkové kriminality na internetu, ať už jde o oběti nebo pachatele, se zaměřením na osoby mladistvé.

Poslední pátá kapitola teoretické části práce popisuje současný stav prevence a vzdělávání v dané problematice.

# 1. VYMEZENÍ ZÁKLADNÍCH POJMŮ

První kapitola bakalářské práce vymezuje základní pojmy, které jsou s majetkovou kriminalitou na internetu a její prevencí úzce spjaty.

Mezi nejdůležitější vědy spojené s problematikou majetkové kriminality patří nepochybně kriminologie a právo. Hovoříme-li o tomto druhu kriminality ve spojení s internetem, je na místě zmínit také základní pojmy technického odvětví informačních technologií a samozřejmě internetu.

V oblasti primární prevence této kriminality zastává hlavní roli především vzdělávání a proto je třeba zmínit také základní pojmy z vědního oboru pedagogiky.

První kapitola nevymezuje veškeré pojmy a definice. Některé jsem z důvodu snadnější orientace zařadil do kapitol, kterých se přímo dotýkají.

## 1.1 Základní pojmy z kriminologie

**Kriminologie** je „*empirická věda o kriminalitě, která má v rámci kriminálních věd nejobecnější postavení"* (Zoubková, 2011, s. 94).

Definice kriminologie není jednotná. Předmětem zkoumání kriminologie je kriminální fenomenologie[3], kriminální etologie[4], osobnost pachatele, viktimologie[5], penologie[6] a kontrola kriminality[7].

Pojem **kriminalita** vyjadřuje zločinnost, tj. nejzávažnější **sociálně-patologický jev.** Kriminologie rozlišuje dvě hlavní definice pojmu kriminalita. Užší legální definici, která vychází z trestního práva, kde kriminalitou je souhrn jednání, kvalifikovaných jako trestné činy uvedené ve zvláštní části trestního zákoníku, a širší definici sociologickou, která může obsahovat i jevy, které jsou pro společnost sice velice škodlivé, ale jejichž skutková podstata není uvedena ve zvláštní části trestního zákoníku (Zoubková, 2011). Mezi takové jevy se řadí např. záškoláctví, alkoholismus, drogová závislost apod. Tyto jevy nemusí přímo

[3] Zaměřuje se na popis kriminality, její struktury, jejích forem apod. (Zoubková, 2011).

[4] Zaměřuje se na vysvětlování kriminogenních (rizikových) faktorů a situací, příčin a okolností kriminality (Zoubková, 2011)

[5] Zabývá se osobností oběti, vztahy mezi pachatelem a obětí, pomocí obětem apod. (Zoubková, 2011).

[6] Věda o trestu, jeho výkonu a jeho účincích (Zoubková, 2011).

[7] Pojem vystihuje vzájemnou vyváženost trestní represe a prevence kriminality (Zoubková, 2011).

s kriminalitou souviset, a proto je nutné k tomuto sociologickému pojetí kriminality přistupovat spíše opatrně (Chalupová, 2012).

Z výše uvedených důvodů budeme dále rozlišovat legální (právní) definici kriminality.

V názvu práce je obsažen pojem „majetková kriminalita“. Zoubková (2011) pod tímto pojmem uvádí, že je součástí obecné kriminality s tím, že jednání je založeno v útoku proti cizímu majetku nejen fyzických, ale i právnických osob. Kriminologický pojem má celkem tři různá pojetí této kriminality, kde první skupinu tvoří trestné činy, které směřují k obohacení pachatele – získání majetku, do této skupiny patří především krádeže, zpronevěry a podvody. Druhou skupinu tvoří trestné činy, pro které je typické poškození majetku, kam patří hlavně poškození cizí věci a třetí skupinu tvoří trestné činy, při kterých pachatel využívá spáchání trestného činu jinou osobou, zejména podílnictví.

Pakliže se pojem majetková kriminalita spojuje s pojmem internet, lze toto sociálně patologické jednání zařadit také pod označení počítačová kriminalita.

Obsah pojmu **počítačové kriminality** nemá oficiální vymezení. Odborníci mají na její definici odlišné názory, avšak shodují se v tom, že počítač může být předmětem i prostředkem útoku.

Podle Smejkala (1995, s. 99) je třeba pod pojmem počítačová kriminalita chápat *„páchání trestné činnosti, v níž figuruje počítač jako souhrn hardwarového a softwarového vybavení data nevyjímaje, 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 movité věci, nebo jako nástroj trestné činnosti“*.

Pojem počítačové kriminality však lze použít také v případech, u kterých byly počítače nebo počítačové sítě použity k tomu, aby usnadnily tradiční formy kriminality. Rozhodným operacionálním prvkem je zde ve všech případech způsob zneužití výpočetní techniky, s přihlédnutím ke specifickým vlastnostem a nadřazenému postavení mezi věcnými prvky způsobu páchání daného trestného činu (Jirovský, 2007).

Kolouch (2013) uvádí, že pojem počítačová kriminalita se v současné době v odborné literatuře téměř nepoužívá, neboť je zavádějící a evokuje k tomu, že tuto kriminalitu lze páchat nejčastěji ve spojení s počítačem osobním. Výstižněji je tato **kriminalita** nyní autory nazývána kriminalitou **informační a komunikační technologie, zkráceně ICT** (angl. Information and Communication Technology), s čímž lze vyslovit souhlas.

O rozšíření pojmu počítačové kriminality na kriminalitu informační se však zmiňuje již Látal v časopise *Policista 3/1998* (Musil, 2000), který poukazuje na skutečnost, že taková

kriminalita existovala ještě dávno před zavedením pojmu počítačová kriminalita, kdy se hovořilo např. o vyzvídání nebo vyzrazování informací.

Označení **informační kriminalita** se používá také v rámci Policie České republiky, která má stejnojmenné útvary zabývající se právě ICT kriminalitou.

Na mezinárodní úrovni se v úmluvách pro trestnou činnost páchanou ICT nejčastěji užívá pojem **kybernetická kriminalita** (Cyber Crime). Nejobecněji je možné tuto kriminalitu definovat jako *„jednání namířené proti počítači, případně síti, nebo jako jednání, při němž je počítač použit jako nástroj pro spáchání trestného činu. Neopomenutelnou skutečností pro to, aby bylo možné uplatnit definici kyberkriminality, je to, že počítačová síť (zejména internet) je pak prostředím, v němž se tato činnost odehrává“* (Kolouch, 2013, s. 10). V souvislosti s pojmem kyberkriminalita se pak hovoří o kyberprostoru, ve kterém je tato kriminalita páchána. Kyberprostorem můžeme chápat prostor, který je vytvořený ICT. Jde o virtuální svět, který je obdobou prostoru reálného (Kolouch, 2013).

**Z výše uvedených definic lze tedy zjednodušeně vyvodit, že majetková kriminalita na internetu je kriminalitou ICT, přičemž se jedná o sociálně patologický jev, jehož pachatelé zneužívají internet za účelem způsobení majetkové škody.**

## 1.2 Základní pojmy z práva

I přesto, že právních norem dotýkajících se majetkové kriminality na internetu je celá řada, považuji za vhodné zmínit v této části práce alespoň některá ustanovení trestního zákoníku (TZ) a zákona o soudnictví ve věcech mládeže (ZSVM), neboť podle těchto právních norem je výše zmiňovaná majetková kriminalita na internetu postihována. Řeč je tedy o trestném činu a provinění v případě mladistvých.

Pakliže je jednání pachatele společensky škodlivé a nepostačuje uplatnění odpovědnosti podle jiného právního předpisu (např. zákon o přestupcích), hovoříme o trestných činech.

*„Trestným činem je protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně.*

*K trestní odpovědnosti za trestný čin je třeba úmyslného zavinění, nestanoví-li trestní zákon výslovně, že postačí zavinění z nedbalosti“* (TZ § 13/1, 2).

Co se týče osob mladistvých, tzn. osob ve věku od 15 do 18 let (ZSVM §2d), tak podmínky za jejich protiprávní činy uvedené v trestním zákoně, opatření ukládána za takové protiprávní činy, postup, rozhodování a výkon soudnictví ve věcech mládeže, upravuje

ZSVM. V této právní normě je mimo jiné uvedeno v ust. § 6, že trestný čin spáchaný mladistvým se nazývá proviněním.

I přesto, že práce je zaměřena především na začlenění majetkové kriminality na internetu do systému vzdělávání na středních školách a gymnáziích, považuji za vhodné zmínit, že žáci základních škol, kteří v době spáchání činu nedovršili patnáctý rok svého věku, nejsou za svá jednání trestně odpovědní (TZ § 25). V těchto případech již nehovoříme o spáchání trestného činu, nýbrž o spáchání činu jinak trestného.

Konkrétní skutkové podstaty trestných činů, které se dělí na přečiny a zločiny jsou uvedeny ve zvláštní části TZ – zde hovoříme o právu hmotném.

Postup orgánů činných v trestním řízení upravuje trestní řád (TŘ) – zde hovoříme o právu procesním.

Závěrem této kapitoly je právní norma, kterou nelze opomenout a to Zákon o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon – ŠZ). Právě tento zákon upravuje předškolní, základní, střední, vyšší odborné a některé jiné vzdělávání ve školách a školských zařízeních, stanoví podmínky, za nichž se vzdělávání a výchova (dále jen "vzdělávání") uskutečňuje, vymezuje práva a povinnosti fyzických a právnických osob při vzdělávání a stanoví působnost orgánů vykonávajících státní správu a samosprávu ve školství (ŠZ § 1).

Chceme-li tedy začlenit majetkovou kriminalitu do systému vzdělávání, je třeba objasnit samotný systém vzdělávacích programů. O tomto pojednává § 3 ŠZ, kde je mimo jiné uvedeno, že Národní program vzdělávání (NPV) zpracovává Ministerstvo školství, mládeže a tělovýchovy (MŠMT). Pro každý obor vzdělání v základním a středním vzdělávání a pro předškolní, základní umělecké a jazykové vzdělávání se vydávají rámcové vzdělávací programy (RVP) a vzdělávání v jednotlivé škole a školském zařízení se uskutečňuje podle školních vzdělávacích programů (ŠVP).

Potřeba vzdělávání osob mladistvých v problematice majetkové kriminality na internetu by tedy měla být obsažena v cílech ŠVP, pakliže by nebyla obsažena přímo v RVP.

## 1.3 Základní pojmy z informačních technologií a internetu

Jelikož hovoříme o kriminalitě informační a komunikační technologie, kterou je možné páchat prostřednictvím nebo s pomocí výpočetní techniky, resp. počítače, je na místě definovat, co si pod pojmem **počítač** vlastně představit, jak jej charakterizovat.

Definice tohoto pojmu spadá do technického odvětví informačních technologií (IT). Předmětem tohoto technického odvětví je hardware a software počítače. Definic pojmu počítač existuje několik.

Nádběla (2006, s. 353) definuje počítač, jako „*stroj na zpracování dat (informací). Většinou zahrnuje funkční systém skládající se z monitoru, klávesnice, myši a počítačové skříně s interními mechanikami, základní deskou, procesorem, rozšiřujícími kartami, napájecím zdrojem a rozvodovými kabely“.*

Kuchta (2009, s. 224) uvádí, že *„počítačem je 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“.*

**Počítačovým systémem** je pak dle Koloucha (2013) funkční jednotka složená z jednoho nebo několika počítačů a připojeného programu, využívající paměťové médium pro všechny nebo alespoň část programů a dat nezbytných pro vykonání programů.

Stejný autor pak na straně 16 uvádí jako příklad počítačového systému mimo počítač také mobilní telefony, bankomaty, herní konzole, SMART televizory a dokonce i internet.

Obecně lze říci, že počítač se skládá z **hardwaru** a **softwaru**, kde hardwarem označujeme všechny jeho fyzické části, z nichž se skládá nebo se kterými spolupracuje (tedy včetně periferií[8]) a softwarem veškerá data a programové vybavení počítače (Nádběla, 2006). Jedno bez druhého nemůže fungovat. Vstupní data do počítače zadává uživatel, přičemž počítač tato data zpracuje pomocí konkrétního software a poskytne uživateli výsledek svojí práce pomocí výstupního zařízení. Počítače a počítačové systémy jsou v dnešní době využívány takřka ve všech oblastech lidské činnosti a jejich prostřednictvím získáváme přístup k síti internet.

Nádběla (2006) ve svém Velkém počítačovém slovníku definuje **internet** na straně 227 také jako *„World Wide Web. WWW. Celosvětová informační a komunikační síť, která vznikla propojením jiných (menších) sítí, jako je Bitnet a Usenet. Její vznik je datován do r. 1993. Tehdy bylo na internetu pouhých 43 webových adres. Dnes se jejich počet pohybuje ve stovkách mil. a každým rokem se stále zvyšuje“*.

Internet v současné době nemá žádného vlastníka, či jinou autoritu nebo instituci, která by jej řídila. V rámci sítě internet má výsostné postavení sdružení ICANN[9], které stanovuje pravidla provozu systému doménových jmen a přiděluje rozsahy IP adres (Kolouch, 2013).

---

8 monitor, klávesnice, myš, tiskárna, skener apod.

9 Internet Corporation for Assigned Names and Numbers.

Neuvěřitelný rozmach internetu znázorňuje následující obrázek dostupný na webové stránce Internetworldstats.com.

| WORLD INTERNET USAGE AND POPULATION STATISTICS June 30, 2012 | | | | | | |
|---|---|---|---|---|---|---|
| World Regions | Population ( 2012 Est.) | Internet Users Dec. 31, 2000 | Internet Users Latest Data | Penetration (% Population) | Growth 2000-2012 | Users % of Table |
| Africa | 1,073,380,925 | 4,514,400 | 167,335,676 | 15.6 % | 3,606.7 % | 7.0 % |
| Asia | 3,922,066,987 | 114,304,000 | 1,076,681,059 | 27.5 % | 841.9 % | 44.8 % |
| Europe | 820,918,446 | 105,096,093 | 518,512,109 | 63.2 % | 393.4 % | 21.5 % |
| Middle East | 223,608,203 | 3,284,800 | 90,000,455 | 40.2 % | 2,639.9 % | 3.7 % |
| North America | 348,280,154 | 108,096,800 | 273,785,413 | 78.6 % | 153.3 % | 11.4 % |
| Latin America / Caribbean | 593,688,638 | 18,068,919 | 254,915,745 | 42.9 % | 1,310.8 % | 10.6 % |
| Oceania / Australia | 35,903,569 | 7,620,480 | 24,287,919 | 67.6 % | 218.7 % | 1.0 % |
| WORLD TOTAL | 7,017,846,922 | 360,985,492 | 2,405,518,376 | 34.3 % | 566.4 % | 100.0 % |

Obrázek 1: Uživatelé internetu v porovnání s celkovou populací lidstva k datu 30. 06. 2012 (Internetworldstats.com, 2014). První sloupec označuje zemi/region, druhý počet populace k roku 2012, třetí uživatele internetu k 31. 12. 2000, čtvrtý sloupec uživatele internetu k datu 30. 06. 2012, pátý sloupec procentuální vyjádření uživatelů internetu k celkové populaci, šestý sloupec procentuální nárůst uživatelů internetu v době 2000-2012 a poslední sloupec znázorňuje procentuální podíl uživatelů internetu z jednotlivých zemí.

## 1.4 Základní pojmy z pedagogiky

Poslední, avšak neméně důležitou oblastí k vymezení pojmů této práce je vědní obor pedagogika, neboť právě tento vědní obor definuje pojmy jako výchova, vzdělání, výchovný cíl a výchovná metoda. Bez těchto pojmů by totiž nebylo možné účinným způsobem bojovat proti majetkové kriminalitě na internetu.

Co je to pedagogika? **Pedagogika** je *„věda o výchově, která zkoumá výchovný proces jako jeden z nejvýznamnějších společenských jevů. Analyzuje výchovný proces v celé jeho šíři, hledá všeobecně platné zákonitosti, pravidla, poučky, které odrážejí vztahy a souvislosti v konkrétní výchovné praxi. Specifika vědního oboru pedagogika spočívají v jeho úzké spojitosti s praktickou činností – s výchovou. Vychází z ní, zpětně se do ní vrací a ovlivňuje ji“* (Kantorová a kol., 2008, s. 12).

Stejný kolektiv autorů pak definuje **výchovu** jako výhradně lidskou činnost, která se projevuje všestranným formováním osobnosti, působí záměrně a cílevědomě s tím, že má adaptační, anticipační a permanentní charakter.

Výsledkem harmonického procesu – výchovy, je dle O. Kádnera (1926) a F. Drtiny (1930) **vzdělání**, jak uvádí Kantorová a kol. (2008).

Hodláme-li někoho vychovávat, je třeba si stanovit **výchovný cíl** našeho působení. Jde o to, čeho chceme dosáhnout u vychovávaného jedince (Průcha, Walterová, Mareš, 2009).

Způsob, jakým dosáhneme výchovného cíle (výchovně vzdělávacího procesu) se nazývá **výchovnou metodou** (Průcha, Walterová, Mareš, 2009).

Z předchozí kapitoly 1.2 víme, že vzdělávání se v ČR uskutečňuje v souladu se školským zákonem.

Samotný pojem **vzdělávání** pak Kantorová a kol. (2008, s. 89) definuje jako „*proces získávání a rozvoje vědomostí, intelektuálních schopností a praktických dovedností, rozvoje rozumové stránky osobnosti, jejího myšlení a paměti.“*

V této kapitole bych ještě doplnil, že konkrétní obsah vzdělávání se nazývá kurikulem.

Průcha, Waltrová a Mareš (2008) v Pedagogickém slovníku na straně 110 uvádějí tři základní **významy kurikula.** Prvním významem je kurikulum považováno za vzdělávací program, projekt, plán. Druhým významem za průběh studia a jeho obsah a konečně třetím významem jako obsah veškeré zkušenosti, jenž žáci získávají ve škole a v činnostech, které se ke škole vztahují, její plánování a hodnocení.

Kapitolu „Vymezení základních pojmů“ záměrně uzavírám definicí kurikula, neboť především v jeho obsahu je třeba hledat odpověď na otázku, jak chránit (nejen) mládež před majetkovou kriminalitou na internetu.

K tomu, abychom mohli na tuto otázku odpovědět, je vhodné vědět, jak vlastně počítačová kriminalita vznikla a jak se postupem času (z historického hlediska poměrně krátkého) vyvíjela a proč je vlastně tak nebezpečná. Tyto skutečnosti lze nalézt v kapitole následující, kterou jsem pojmenoval „Historie počítačové kriminality“.

# 2. HISTORIE POČÍTAČOVÉ KRIMINALITY

V předchozí kapitole byly vymezeny základní pojmy, které jsou s majetkovou kriminalitou na internetu a její prevencí úzce spjaty. Tato kriminalita byla taktéž nazývána kriminalitou počítačovou, v současné době již ICT.

Druhá kapitola zmiňuje několik významných událostí týkajících se historického vývoje počítačové kriminality.

Právě historické události upozorňují na závažnost a rychlost s jakou se tento druh kriminality vyvíjí.

Závažnost počítačové kriminality byla zmiňovaná ještě před komercionalizací internetu v roce 1994, v rámci 8. konference OSN konané v Havaně roku 1990, kde byla označena jednou z nejnebezpečnějších forem kriminality spolu s organizovaným zločinem a distribucí drog (Smejkal, 1995).

I když je práce zaměřena na začlenění prevence majetkové kriminality do systému vzdělávání v rámci naší republiky, považuji za vhodné zmínit také některé události z historie počítačové kriminality ve světě. Tyto události nebezpečnost počítačové kriminality zcela jistě podtrhují.

## 2.1 Historie ve světě

Počátky „počítačové kriminality“ sahají až do roku 1801, když francouzský vynálezce Joseph Marie Jacquard, sestrojil první programovatelný tkalcovský stav, který se programoval pomocí děrných štítků. Tento vynález ohrožoval manufakturu ručních tkalců, pročež byl opakovaně sabotován, což jeho vývoj pozastavilo (Matějka, 2002). O počítačové kriminalitě v této době lze však hovořit pouze v uvozovkách.

Michal Matějka (2002) rozděluje počítačovou kriminalitu do tří časových období. První z nich nazývá počítačovým pravěkem, který datuje od vynálezu telefonu až do roku 1981, kdy byl uveden na trh první osobní počítač.

Období od roku 1981 do roku 1994 pak označuje počítačovým středověkem, kdy ještě neexistovalo komerční síťové propojení jednotlivých uživatelů počítačů a jako zlomový případ oddělující počítačový středověk od novověku uvádí kauzu CITIBANK, jejímž hlavním představitelem byl Vladimir Levin, který se svými kolegy připravil americkou banku Citibank o 10,7 milionů USD.

Počítačovým novověkem Matějka považuje období od roku 1994.

Ingrid Matoušková (2013) se o historii počítačové kriminality zmiňuje až se vznikem internetu, což mělo počátky v roce 1969, kdy byla grantovou agenturou ministerstva obrany USA spuštěna počítačová síť Advanced Research Projects Agency Network (ARPANET).

Na tuto síť bylo v roce 1972 připojeno asi 50 převážně armádních počítačů. V této době prakticky počítačová kriminalita neexistovala, avšak tím, jak se začínala síť rozšiřovat také na akademická pracoviště, netrvalo dlouho a dne 27. října 1980 byl virem vyřazen celý ARPANET z provozu.

Prvním člověkem potrestaným za počítačovou kriminalitu byl Ian Murény, který v roce 1981 pronikl do sítě firmy AT&T, kde pozměnil čas jejich vnitřního systému, což mělo za následek účtování hovorů s denní sazbou v noci a naopak (Matoušková, 2013).

Prvního internetového červa[10] vypustil do počítačové sítě dne 2. listopadu 1988 Robert Tappan Morris, čímž nakazil z tehdy připojených 60.000 počítačů více než 6.000 počítačů.

Následovaly závažnější případy, když v roce 1990 Kevin Poulsen pronikl do telefonní sítě rozhlasové stanice KIIS-FM v Los Angeles, kde si zajistil 102 pozici volajícího, který vyhrál automobil zn. Porsche 944 S2, a v roce 1994 již zmiňovaný případ CITIBANK (Matoušková, 2013).

Světovou historii počítačové kriminality ukončím případem jednoho z největších hackerů[11], Kevina Mitnicka. Ten zřejmě jako první využíval nejslabšího článku počítačové bezpečnosti – člověka, čímž se stal prvním sociálním inženýrem. V roce 1995 byl zatčen a následně také odsouzen pro způsobení škody ve výši 300.000.000 USD, avšak nikdy mu nebylo prokázáno, že by nějaký majetkový prospěch získal (Mitnick, 2003).

## 2.2 Historie u nás

Prvním případem počítačové kriminality na našem území byla sabotáž z roku 1974. Tehdy zaměstnanec Úřadu důchodového zabezpečení, úmyslně a opakovaně poškozoval na tu dobu vysoce výkonný počítač LEO 360 s magnetopáskovou periferní pamětí, čímž došlo ke

[10] Počítačový červ nebo také anglicky worm je počítačový program, který je schopen vlastní reprodukce s tím,že je šířen emailem nebo prostřednictvím webových stránek (Nádběla, 2006, s. 489).

[11] Hacker a hacking pochází z USA z 50. let 20. století a označoval technicky nadanou osobu (a její činnost) schopnou nalézat nová, mnohdy neortodoxní řešení problému. Hacking je dnes veřejností vnímán jako jakákoliv činnost osoby směřující k získání nelegálního přístupu k cizímu systému či osobnímu počítači (Kolouch, 2013, s. 50).

skluzu ve výplatách asi 40.000 důchodů v řádu pěti týdnů, čímž byla způsobena škoda 1.100.000 Kčs (Suchánek a kol., 1997).

Ze stejného období lze zmínit také případ pracovnice zásilkové služby MAGNET, která si nechala zboží zasílat na adresu své matky, přičemž do odběratelské databáze zaznamenávala, že zboží bylo zaplaceno, i když tomu tak nebylo (Matějka, 2002).

Následovaly další případy, které byly známy převáženě na pracovištích mzdových účtáren, nebo tam, kde docházelo k peněžním manipulacím. V osmdesátých letech bylo 14 deliktů tohoto charakteru právně kvalifikováno podle ust. § 132 tehdejšího Zákona č. 140/1961 Sb., trestní zákon, jako „Rozkrádání majetku v socialistickém vlastnictví“ (Matějka, 2002).

Významným datem počítačové kriminality u nás je jistě 13. únor 1992, kdy bylo do České a Slovenské Federativní republiky zavedeno internetové připojení. Tehdy bylo jako první připojeno ČVÚT v Pražských Dejvicích.

Od tohoto období docházelo na našem území k nárůstu trestných činů směřujících proti porušování autorských práv, jako je nelegální kopírování softwaru, hudby a filmů.

Tím, jak se dostupnost výpočetní techniky na našem území rozšiřovala, přibývalo dalších společensky nežádoucích jednání. Následkem tohoto jevu docházelo k postupným legislativním úpravám našeho právního systému, konkrétně Zákona č. 140/1961 Sb., trestní zákon, účinný do 31. prosince 2009 (TrZ). Došlo k zavedení nových trestných činů, jako např. v roce 1991 „Poškození a zneužití záznamu na nosiči informací“ (TrZ § 257a) nebo v roce 1993 „Neoprávněné nakládání s osobními údaji“ (TrZ § 178).

Zde bych zmínil první průnik do počítačového systému, za který je považován případ z roku 1995, jehož pachatel pozměnil software počítače tak, aby výhra ve vysoce sledované televizní show BINGO, připadla konkrétním osobám. Pachatel byl tehdy odsouzen právě pro trestný čin Poškození a zneužití záznamu na nosiči informací (TrZ § 257a).

S rozmachem internetu bylo jednání pachatelů stále důmyslnější a sofistikovanější.

Dne 23. listopadu 2001 byla v Budapešti otevřena k podpisu Úmluva o počítačové kriminalitě, kterou Česká republika podepsala dne 9. února 2005.

*„Cílem úmluvy je vytvořit mezinárodní právní rámec pro účinné potírání počítačové kriminality prostřednictvím harmonizace prvků skutkových podstat v oblasti počítačové kriminality za účelem zajištění adekvátního postihu pachatelů, stanovení nezbytných vnitrostátních vyšetřovacích pravomocí pro zajišťování důkazů v elektronické formě a vyšetřování počítačové kriminality, jakož i zavedení pohotového a efektivního režimu*

*mezinárodní spolupráce ve vztahu k trestným činům souvisejícím s informačními technologiemi"* (Conventions.coe.int., 2014).

Na základě zmiňované úmluvy byly do právního systému ČR implementovány s účinností TZ od 1. ledna 2010 nové trestné činy, jako „Neoprávněný přístup k počítačovému systému a nosiči informací" (TZ § 230), Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat" (TZ § 231), „Výroba a jiné nakládání s dětskou pornografií" – spácháno prostřednictvím počítačového systému (TZ § 192), „Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi" – spácháno v komerčním měřítku a prostřednictvím počítačového systému (TZ § 270).

Česká republika Úmluvu ratifikovala dne 1. prosince 2013 a dne 23. prosince 2013 vyšla ve Sbírce mezinárodních smluv.

Tímto se tedy dostáváme až k současnému legislativnímu stavu naší právní soustavy ve smyslu počítačové (ICT) kriminality, přičemž o trestně právní rovině majetkové kriminality na internetu bude pojednávat kapitola následující.

# 3. TRESTNĚ PRÁVNÍ ROVINA MAJETKOVÉ KRIMINALITY NA INTERNETU

Z první kapitoly vyplývá, že majetková kriminalita na internetu je kriminalitou ICT, přičemž se jedná o sociálně patologický jev, jehož pachatelé zneužívají internetu za účelem způsobení majetkové škody.

Jelikož vycházíme z legálního pojetí tohoto druhu kriminality, je na místě uvést, že trestné činy proti majetku jsou konkrétně uvedeny v páté hlavě zvláštní části trestního zákoníku a to od § 205 TZ (Krádež) po § 232 TZ (Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti).

Nutno však podotknout, že majetkový charakter mají také další trestné činy, které je možno páchat s využitím (zneužitím) internetu. Jako příklad z hlavy druhé zvláštní části trestního zákoníku uvádím § 175 TZ (Vydírání) či § 182 odst. 2 TZ (Porušování tajemství dopravovaných zpráv). Z hlavy šesté § 234 TZ (Neoprávněné opatření, padělání a pozměňování platebního prostředku) nebo § 270 TZ (Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi).

Jistě by bylo možné dohledat i jiné, v této práci výslovně nezmiňované paragrafy, jejichž předmětem je způsobení majetkové škody s využitím internetu, avšak stanovený rozsah bakalářské práce by k jejich podrobnějšímu popisu nestačil.

Podrobněji bude v následujícím textu popsán trestný čin Podvod dle ust. § 209 TZ, neboť ten je na internetu páchán nejčastěji, jak dokládají statistické údaje Policejního prezidia České republiky (PP) obsaženy v příloze č. 2. Taktéž jeho aktéry bývají, ať už v postavení oběti nebo pachatele, osoby mladistvé.

## 3.1 Podvod jako nejčastěji páchaný trestný čin na internetu

K naplnění základní skutkové podstaty trestného činu Podvod dle ust. § 209 TZ je třeba uvedení někoho v omyl, využití něčího omylu nebo zamlčení podstatné skutečnosti a zároveň způsobení škody ve výši nikoli nepatrné, což činí min. 5.000 Kč (TZ § 138/1). Je zde třeba úmyslného zavinění. Postihy za spáchání tohoto trestného činu se pohybují od propadnutím věci nebo jiné majetkové hodnoty až po trest odnětí osobní svobody až na deset let (úplné aktuální znění § 209 TZ – viz. příloha č. 3).

Skutková podstata trestného činu podvodu nezmiňuje ve svém obsahu podmínku, aby byl k jejímu spáchání použit počítač.

Osobně bych se však přikláněl alespoň k používání vyšších trestních sazeb v případě, kdy je k podvodu použit počítač, resp. internet a možná by stálo za zvážení také rozšíření skutkové podstaty tohoto trestného činu s ohledem na tento modus operandi[12].

Co se týče trestných činů majetkového charakteru páchaných na internetu, tak podvod patří jistě k těm nejrozšířenějším i v souvislosti s internetovým obchodováním. Co si však představit pod pojmem internetového nebo elektronického obchodu?

### 3.1.1 Elektronické obchody

Podle definice používané OECD[13] elektronický obchod zahrnuje jakékoli obchodní transakce prováděné fyzickými i právnickými osobami s tím, že tyto transakce jsou založeny na elektronickém zpracování a přenosu dat (Businessinfo.cz, 2014).

Definice WTO[14] upřesňuje, že takový obchod mimo výrobků prodávaných a placených přes internet a doručovaných v hmotné podobě, zahrnuje také produkty doručované přes internet v digitální podobě (Businessinfo.cz, 2014).

Smejkal (2001) vymezuje vzájemné vztahy v e-obchodu do tří skupin. První označuje zkratkou B2B (Business to business), kdy je prodávajícím i kupujícím podnikatel. Druhou skupinu označuje zkratkou B2C (Business to consummer), kdy je prodávajícím podnikatel a kupujícím spotřebitel (koncový zákazník). Poslední skupinu označuje zkratkou C2C (Consummer to consummer), kde je prodávajícím i kupujícím občan.

Prostřednictvím internetového obchodu lze zakoupit téměř vše co v klasické kamenné prodejně, ať už se jedná o věci nebo o služby.

Občanský zákoník (OZ) umožňuje spotřebiteli v případě uzavření smlouvy výhradně prostředkem komunikace na dálku (tedy i internetem), odstoupit od této smlouvy ve lhůtě 14 dnů od uzavření smlouvy a v některých případech i později (OZ § 1846).

Této zákonné lhůty využívá také nová on-line platební metoda, která se v České republice objevila teprve nedávno. Metoda se nazývá „zaplať po vyzkoušení“ a její princip spočívá v tom, že spotřebitel si v e-shopu „zakoupí“ zboží v hodnotě do 3.000 Kč, které však neplatí a má možnost si jej ve 14 denní lhůtě zdarma vyzkoušet. Platbu provede až v případě,

---

12 Způsob provedení.

13 Organisation for Economic Co-operation and Development (Organizace pro hospodářskou spolupráci a rozvoj).

14 World Trade Organization (Světová obchodní organizace).

že mu zboží vyhovuje a nebude jej tedy e-shopu vracet. Tuto službu zajišťuje projekt Twisto.cz, který za spotřebitele e-shopu zboží zaplatí a nespokojený zákazník tak nemusí na vrácení kupní ceny čekat až 30 dnů, jak je tomu ve standardních případech. Pakliže je spotřebitel se zbožím spokojen, uhradí jej investičním firmám Miton a Enern, které se na projektu Twisto.cz podílejí (Novinky.cz; A, 2013).

Mezi další výhody internetového obchodování patří jistě anonymita, nízké ceny, dostupnost z pohodlí domova a prakticky neomezené hranice obchodování. Nutno podotknout, že obdobné výhody má také potencionální pachatel, který jich mnohdy bezezbytku využívá, například založením podvodného e-shopu.

### 3.1.2 Podvodné e-shopy

Cílem podvodného e-shopu je logicky maximální finanční zisk. Provozovatelé takových e-shopů nabízejí fiktivní zboží nebo služby za velice výhodné až nereálně nízké ceny, přičemž požadují jejich platbu předem na bankovní účet. Zboží nebo službu dle učiněné objednávky následně nedodají a získané finanční prostředky použijí pro vlastní potřebu. Registrace domény podvodného e-shopu, kterou je možné ověřit na webových stránkách www.nic.cz, bývá často provedena v poměrně krátké době před samotným nákupem ze strany klienta. Podvodné e-shopy převážně nemají možnost doručení zboží na dobírku, nebo je tato možnost cenově znevýhodněna a schází jim věrohodné kontaktní údaje, u kterých absentuje např. telefonní číslo pevné linky apod. (Hruška, 2014).

Další podvodné způsoby internetového obchodování lze zaznamenat na inzertních portálech, které jsou k tomuto účelu často zneužívány.

### 3.1.3 Vybrané inzertní portály zneužívané k páchání podvodů

Jako nejznámější inzertní portály zneužívány k páchání podvodného internetového obchodování uvádím: sBazar.cz, Bazos.cz a Hyperinzerce.cz.


Obrázek 2: Loga vybraných inzertních portálů zneužívaných k páchání podvodů (Sbazar.cz, 2014; Bazos.cz, 2014; Hyperinzerce.cz, 2014).

Důvodem obliby těchto portálů ze strany pachatelů je poměrně vysoká míra anonymity. Potencionální oběť si zde nemůže předem ověřit např. kolik druhá strana (potencionální pachatel) obchodů realizovala a s jakou úspěšností, jak je tomu třeba u aukčního portálu Aukro.cz – viz. další kapitola.

Problémy vzniklé nejen s tímto internetovým obchodováním mohou být následující (Smejkal, 2001, s. 237):

- *„ověření totožnosti obou stran,*
- *skutečné provedení úhrady,*
- *doručení úhrady skutečnému prodávajícímu,*
- *dodání zboží (služby) skutečnému kupujícímu.“*

Inzertní portál Sbazar.cz na svých stránkách upozorňuje uživatele na nebezpečí tzv. nigerijských dopisů (Sbazr.cz, 2014). Zasílání nigerijských dopisů je považováno za jeden z nejstarších podvodných způsobů na internetu, a jeho počátky se datují až do 80. let minulého století (Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online, 2013).

V podstatě jde o fingované dopisy v rámci internetu rozesílané elektronickou poštou s lákavými nabídkami na výdělek vysokých částek. Odesílatelé zde vystupují např. jako bohatí podnikatelé a žádají adresáty o poskytnutí pomoci při převodu finančních částek ze zemí, ve kterých žijí. Pakliže na tyto inzertní nabídky adresát odpoví je odesílatelem vyzýván k tomu, aby uhradil postupně v malých či větších částkách krytí bankovního převodu cílové částky. Odesílatelé nigerijských dopisů pak převod fiktivní cílové částky neuskuteční a adresáta tím připraví o zaslané krytí převodů (Kolouch, 2013).

Dalšími portály zneužívanými k páchání podvodů jsou portály aukční.

### 3.1.4 Vybrané aukční portály zneužívané k páchání podvodů

Mezi nejznámější a nejrozšířenější weby zabývajícími se nákupem a prodejem nejen použitých věcí u nás jsou jistě Aukro.cz, iKup.cz nebo Odklepnuto.cz. Ze zahraničních webů nutno zmínit také eBay.com.


Obrázek 3: Vybraná loga aukčních portálů zneužívaných k páchání podvodů (Aukro.cz, 2014; iKup.cz, 2014; Odklepnuto.cz, 2014; ebay.com, 2014).

Podrobněji popíši, alespoň činnost portálu Aukro.cz, neboť patří v České republice k těm nejznámějším.

Server Aukro.cz provozuje od roku 2003 polská skupina Allegro. Z historie tohoto webu jsou zmíněny následující události:

V roce 2008 byla spuštěna služba „Program na ochranu kupujících“ a byla stanovena pravidla definující podmínky, za kterých mohou kupující žádat provozovatele o peněžitou částku za účelem zmírnění utrpěných škod v případě, kdy prostřednictvím systému Aukro uzavřeli kupní smlouvu na určité zboží, ale prodávající dodal zboží v rozporu s kupní smlouvou nebo jej nedodal vůbec (Pravidla programu ochrany kupujících, §1).

V roce 2009 na Aukru obchodovalo více než milion registrovaných Čechů.

V roce 2011 došlo k podpisům smluv s nejlepšími prodejci Aukro+ a kupujícím tak byly garantovány jejich profesionální služby. Dále byla zavedena možnost platit platební kartou nebo rychlým on-line převodem. Nákup bylo od této doby možné uskutečnit i bez registrace.

V roce 2012 se na Aukru zaregistroval 2,5 miliontý Čech a zboží je od této doby možné vyzvednout také v kamenné pobočce AukroPointu.

V současné době se jedná o relativně bezpečný způsob nakupování. Provozovatel serveru dokonce uvádí, že celých 99,98% nákupů proběhne bez problémů.

Jeho bezpečnost je dána především tím, že každý jeho prodejce se musí nejprve řádně zaregistrovat, což zahrnuje také ověření doručovací adresy. Na tuto je uživateli zasílán dopis s aktivačním kódem. Registrace je dokončena až jeho zadáním do systému.

Historie prodejů, každého uživatele a jeho hodnocení ostatními je pak dalším potencionálním kupcům, ale i prodejcům známá. U uživatelského jména má totiž každý registrovaný uživatel v závorce uveden počet úspěšných obchodů, přičemž za každý pozitivní komentář získává jeden bod a za každý negativní jeden bod ztrácí. Pro lepší přehled je u každého uživatele, který má více jak 5 pozitivních hodnocení znázorněna hvězdička, která má podle počtu pozitivních komentářů několik barvených obměn.

Prostřednictvím serveru Aukro je nabízeno zboží použité, avšak i zcela nové. Své nabídky zde mají vystaveny různé e-shopy a jiné podnikající fyzické či právnické osoby.

Na Aukru není nutné veškeré nabízené zboží dražit od prodávajícím stanovené částky po určitou dobu, ale toto je od roku 2009 možné v mnoha případech zakoupit za pevnou cenu pomocí nabídky „Kup teď“. Nejedná se tedy pouze o aukční portál (Aukro.cz, 2014).

Ke způsobům, jakými lze podvodně vylákat od obětí citlivé informace, vztahující se například k bankovním účtům, se blíže vyjádřím v následující kapitole.

## 3.2 Vybrané způsoby páchání podvodu na internetu

Mezi nejzávažnější způsoby páchaní podvodů na internetu patří sociální inženýrství, phishing a pharming.

### 3.2.1 Sociální inženýrství

Sociální inženýr nebo též sociotechnik využívá k dosažení svého cíle slabin lidského vnímání, využívá manipulace a přesvědčování svých obětí (Jirovský, 2007). Útočí pod smyšlenou identitou na konkrétní oběť, což jeho úspěšnost zvyšuje. Snaží se získat maximum informací o své oběti, získat její důvěru. Ve správný čas pokládá vhodné otázky k získání potřebných informací, kterých následně využívá ve svůj prospěch. Sociotechnik musí pohotově reagovat na položené otázky, předvídat obsah zamýšlené i probíhající konverzace, improvizovat. Editorka Linda McCarthy v knize Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online (2013, s. 57) definuje sociální inženýrství jako *"používání obecné znalosti lidského chování k přesvědčení uživatelů, aby porušili svá vlastní bezpečnostní pravidla"*. Konverzace může probíhat telefonicky, elektronickou poštou, chatováním, ale také písemně nebo osobně. Cílem útočníka mohou být hesla k různým aplikacím, bezpečnostní kódy nebo získání dálkového přístupu do počítače oběti např. formou zaslání phishingové zprávy. Sociálního inženýra však nemusí hnát pouze touha po penězích, ale např. po zdolávání překážek, testování svých možností, získávání nových vědomostí (Mitnick, 2003).

### 3.2.2 Phishing

Phishing, česky též „rybaření“ je technika, kterou lze získat prostřednictvím internetu citlivá data (např. přihlašovací údaje k internetovému bankovnictví nebo čísla platebních karet) od nic netušících uživatelů, a s jejich pomocí následně provést neoprávněné výběry nebo převody finančních prostředků z jejich bankovních účtů.

Úspěšnost této techniky je založena na nedodržování bezpečnostních pravidel uživatelů při komunikaci s finančními institucemi.

Pachatel phishingu odesílá potencionálním obětem emailové zprávy, které se tváří, jako by je odesílala jejich banka, přičemž často upozorňují na hrozící bezpečnostní riziko a nutí tím uživatele k tomu, aby si např. změnil heslo, či PIN kód svojí platební karty a to na falešných stránkách přístupných uživateli odkazem obsaženým v emailové zprávě. Stránky

otevřené po kliknutí na tento odkaz věrně napodobují oficiální stránky předmětného peněžního ústavu (Jirovský, 2007).

Podle statistik bezpečnostního týmu CSIRT.CZ, který provozuje CZ.NIC, správce české národní domény, a to na základě memoranda uzavřeného v roce 2012 s Národním bezpečnostním úřadem, bylo v období od 1. dubna 2008 do 14. května 2014 prověřováno 1070 phishingových útoků na našem území (Csirt.cz, 2014).

V poslední době se pachatelé používající phishingovou techniku snaží pomocí trojských koňů[15] dostat také do operačních systémů chytrých telefonů, aby tak získali přístup k autorizačním SMS zprávám banky (Novinky.cz; B, 2014).

### 3.2.3 Pharming

Sofistikovanější a o to nebezpečnější formou phishingu je **pharming**[16]. Útoky tímto způsobem mají dvě podoby.

Jednou z nich je pro útočníka extrémně složitý, avšak velice účinný útok na server DNS. Zde dochází k přeložení doménového jména na adresu IP[17] (např. www.seznam.cz = 194.108.114.194). Útok se spouští v okamžiku, ve kterém se uživatel připojí ze svého internetového prohlížeče na stránky peněžního ústavu. DNS serverem však není spojen s IP adresou jeho peněžního ústavu, nýbrž na adresu falešnou, která originální stránky opět věrně napodobuje. Tímto způsobem útočník opět získá citlivá data (v tomto případě bez přičinění uživatele), která následně zneužívá k vlastnímu obohacení.

Druhou podobou pharmingu je upravení hosts souboru v systému Windows, který funguje obdobně, jako DNS server. Zde se však jedná o lokální pharming u koncového počítače uživatele, kde lze předpokládat nižší míru zabezpečení, např. absence antivirového programu. Útočník se pak k upravení tohoto souboru dostává pomocí trojského koně, který si uživatel do počítače sám nevědomky nainstaluje (např. z neověřeného zdroje) a poté jej může útočník ovládat k vlastnímu využití (Lupa.cz, 2014).

---

15 Trojský kůň (trojan) je program tvářící se, jakoby vykonával určitou činnost, ale ve skutečnosti vykonává funkci, se kterou uživatel nesouhlasí (Nádběla, 2006).

16 Česky také jako pharmaření.

17 IP (Internet Protocol) adresa slouží k jedinečné identifikaci zařízení v rámci sítě a může být dynamická tzn. při každém připojení jiná nebo statická tzn. neustále stejná (Nádběla, 2013, s. 230).

Některá podvodná jednání lze postihovat také dle ust. § 230 odst. 2 TZ (Neoprávněný přístup k počítačovému systému a nosiči informací)[18], avšak tato právní kvalifikace není u phishingu, pharmingu aj. možná, neboť útočník nezíská přístup k počítačovému systému nebo nosiči informací (Kolouch, 2013).

V kapitole 3.1 je uvedeno, že pachatel trestného činu Podvod (TZ § 209) musí svým jednáním naplnit také materiální stránku skutkové podstaty tohoto trestného činu a tedy způsobit škodu alespoň ve výši 5.000 Kč. Je tedy zřejmé, že vylákáním přístupových kódů a hesel pachatelovo jednání nekončí. *„Vytvoření repliky webové stránky a získání přihlašovacích jmen a vstupních hesel by pak bylo možné kvalifikovat jako přípravu či pokus trestného činu § 209 tr. zákoníku“* (Kolouch, 2013, s. 38). V praxi je však takové jednání právně kvalifikováno i jako Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (TZ § 231) – úplné aktuální znění viz. příloha č. 4.

Skutková podstata trestného činu Podvod (TZ § 209) je tedy dokonána až obohacením pachatele.

Pachatelé si často bývají této podmínky trestnosti jejich jednání vědomi, a proto se v některých případech snaží od obětí podvodně vylákat částky do 5.000 Kč. V takových případech je pak na místě ověřit také všechny okolnosti alternativní možnosti jejich postihu.

## 3.3 Alternativní možnost postihu dle zákona o přestupcích

Mohlo by se zdát, že zákon o přestupcích (PZ) s majetkovou kriminalitou dle jejího legálního pojetí přímo nesouvisí, avšak opak je pravdou.

O přestupcích hovoříme ve společensky méně škodlivých případech**,** přičemž přestupkem je *„zaviněné jednání, které porušuje nebo ohrožuje zájem společnosti a je za přestupek výslovně označeno v tomto nebo jiném zákoně, nejde-li o jiný správní delikt postižitelný podle zvláštních právních předpisů anebo o trestný čin“* (PZ § 2/1).

Pakliže hrozící majetková újma nedosahuje výše požadované k naplnění skutkové podstaty trestného činu podvodu (5.000 Kč), je na místě jednání pachatele právně kvalifikovat, jako přestupek proti majetku dle ust. § 50 PZ. Ustanovení toto paragrafu zní:

*(1) „Přestupku se dopustí ten, kdo*

[18] Podvodu lze dosáhnout daty nejen zamlčenými, ale i neoprávněně vloženými (Kolouch, 2013, s. 91).

*a) úmyslně způsobí škodu na cizím majetku krádeží, zpronevěrou, podvodem nebo zničením či poškozením věci z takového majetku, nebo se o takové jednání pokusí,*

*b) úmyslně neoprávněně užívá cizí majetek nebo si přisvojí cizí věc nálezem nebo jinak bez přivolení oprávněné osoby,*

*c) úmyslně ukryje nebo na sebe nebo jiného převede věc, která byla získána přestupkem spáchaným jinou osobou, nebo to, co za takovou věc bylo opatřeno.*

*(2) Za přestupek podle odstavce 1 lze uložit pokutu do 15 000 Kč nebo zákaz pobytu".*

Jak již bylo řečeno výše, této materiální hranice rozdělující přestupky od trestných činů jsou si pachatelé v mnoha případech vědomi, a proto úmyslně uvádějí ceny nabízeného zboží na různých inzertních serverech právě do výše 5.000 Kč. Pakliže však svá protiprávní jednání opakují, je možné na tato pohlížet jako na pokračování v trestném činu podle ustanovení § 116 TZ, které zní: „*Pokračováním v trestném činu se rozumí takové jednání, jehož 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".*

Pachatelé trestných činů na internetu využívají i jiných možností, aby se vyhnuli trestnímu postihu za jejich jednání. Využívají k tomu skutečnosti, že na internetu obecně neplatí žádné zvláštní zákony (Smejkal, 2001) a otázka působnosti práva v kyberprostoru je tedy řešena legislativní úpravou konkrétního státu. Blíže o tomto globálním problému v následující kapitole.

## 3.4 Problematika distančního deliktu

Distanční delikty jsou postihovány podle zásady teritoriality (TZ § 4). Zde je ve druhém odstavci uvedeno, že trestný čin se považuje za spáchaný na území České republiky, pakliže se tu pachatel dopustil zcela nebo zčásti jednání, i když porušení nebo ohrožení zájmu chráněného trestním zákonem nastalo nebo mělo nastat zcela nebo zčásti v cizině, nebo zde pachatel poruší nebo ohrozí zájem chráněný trestním zákonem nebo měl-li tu alespoň zčásti takový následek nastat, i když se jednání dopustil v cizině.

Podstatou distančního deliktu je tedy skutečnost, že pachatel může jednat na jednom místě a následek, který svým jednáním způsobí, nastane na místě jiném.

V rámci internetu, který nemá žádné hranice, tak může nastat situace, že pachatel z České republiky on-line vykrade banku v USA a peníze uloží ve Švýcarsku. Právě

teritorialita práva je základním problémem v boji proti počítačové kriminalitě (Matějka, 2002).

Otázka působnosti mezinárodního či národního práva v kyberprostoru je poslední dobou stále častěji řešena. Neznámou však zůstává, jaký právní systém by se na protiprávní jednání páchané na internetu vztahoval a zdali vůbec (Kolouch, 2013).

Matějka (2002) uvádí, že např. USA přijali velmi nebezpečnou zásadu, podle které je dle jejich práva trestně odpovědným autor, který na internet umístí nezákonný obsah, k němuž mají američtí občané přístup. Takovým způsobem by se mohl prakticky každý poskytovatel obsahu na internetu stát subjektem trestního práva ve všech zemích světa.

K samotným aktérům majetkové kriminality na internetu, ať už v postavení oběti nebo pachatele, viz. následující kapitola.

# 4. AKTÉŘI MAJETKOVÉ KRIMINALITY NA INTERNETU

Majetkovou kriminalitu na internetu může páchat nebo se stát její obětí prakticky každý uživatel internetu, ať už se jedná o dítě nebo dospělého (fyzické osoby). Do obou rolí se však mohou dostat i osoby právnické. Oběťmi často bývají velké banky a nadnárodní společnosti, které nemají zájem zveřejňovat, že se stali obětí počítačové kriminality – ztráta důvěry (Smejkal, 1995). Naopak pachateli mohou být např. firmy používající nelegální software apod.

Oproti tradiční kriminalitě, jejíž pachatelé bývají často členy podsvětí a mají vazby na ostatní kriminální živly, je situace u počítačové kriminality odlišná. Její pachatelé bývají nezřídka zcela mimo tradiční zločinecké struktury, jedná se o studenty, počítačové odborníky nebo techniky, u kterých je velmi nepravděpodobné, že by spáchali také jinou trestnou činnost mimo rámec počítačové kriminality (Matějka, 2002).

Do obou rolí se mohou mnohem snadněji dostat právě děti, které se již ve věku kolem jedenácti let dostávají na úroveň dospělých, co se týče technických dovedností při práci s počítačem v on-line prostředí internetu. V tomto věku si však stále nevytvořily přiměřenou intelektuální a emocionální zralost, které je třeba pro správná rozhodnutí, kterým musí čelit na internetu, jak bylo zjištěno průzkumem společnosti AVG Technologies (Krčmářová, 2012).

V oblasti online nakupování (kapitoly 3.1.1 až 3.1.4) se zdá být sice nejpočetnější skupinou uživatelů Generace X, jak ji nazývají demografové, přičemž se jedná o věkové rozmezí od roku narození 1965 do roku 1976, avšak údaje v tomto smyslu nejsou zcela relevantní. Generace X má v online nakupování zastoupení z 80ti% uživatelů, což oproti dětem a mladistvým ve věku do 18 let, činí rozdíl 42%. Tento rozdíl spočívá především v tom, že platební karty k bankovním účtům jsou vydávány převážně dospělým uživatelům, avšak právě pomocí těchto platebních karet nakupují také děti a mladiství, nebo jsou alespoň koncovými příjemci zakoupeného zboží či služeb. Nelze tedy jednoznačně říci, že v této oblasti internetu děti a mladiství nevévodí (Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online, 2013).

Obecně lze k majetkové kriminalitě na internetu říci, že v případě oběti, postačuje zanedbání nebo podcenění bezpečnostních pravidel spojených s užíváním internetu, u dětí pak navíc jejich absence přiměřené intelektuální a emocionální zralosti. V případě pachatelů je to motiv, odpovídající úroveň technických dovedností, informace o oběti, u dětí a mladistvých,

avšak nejen u nich, navíc také neznalost zákona (co je a není protiprávní). Zde mám na mysli především nedávno zavedené trestné činy do naší legislativy jako např. § 230 TZ (Neoprávněný přístup k počítačovému systému a nosiči informací), jehož plné znění je obsaženo v příloze č. 5.

K tomu aby se uživatelé internetu nestávali oběťmi ICT kriminality, nebo dokonce jejími pachateli, je nutná mimo represe také prevence. Právě prevenci v oblasti majetkové kriminality na internetu bude věnována následující, poslední kapitola teoretické části práce.

# 5. PREVENCE MAJETKOVÉ KRIMINALITY NA INTERNETU

Pojem **prevence kriminality** lze chápat v nejobecnějším smyslu jako *„intervenci realizovanou různými subjekty na různých stupních, přičemž v zásadě je hlavním účelem zabránit trestné činnosti ještě předtím, než k ní dojde. Tedy kriminalitě předcházet“*. (Chalupová, 2012, s. 11).

## 5.1 Dělení prevence a její druhy

Nejobecněji se prevence kriminality dělí na primární, sekundární a terciální. Toto dělení bylo převzato ze zdravotnictví Brentinghamem a Faustem již v roce 1976, jak uvádí Chalupová (2012), která dále doplňuje, že **primární prevence kriminality** je zaměřena obecně na předcházení kriminality a snižování příležitostí k jejímu páchání. Je tedy směřována k obecné části populace a na místa dosud nezatížené kriminalitou. Aktivním způsobem podporuje společensky akceptovatelná chování.

**Sekundární prevence kriminality** je zaměřena na osoby nebo místa, která byla vyhodnocena jako kriminálně riziková. Její aktéři jsou již vymezeni konkrétněji, např. podle věku, teritoria apod.).

**Terciální prevence kriminality** je zaměřena již na konkrétní pachatele a oběti kriminality. Dále na místa, kde se tato kriminalita odehrává.

Jelikož hodláme majetkové kriminalitě na internetu předcházet, je tato práce směřována do oblasti prevence primární.

Miovský (2010) uvádí, že primární prevence má mezioborovou povahu (pedagogika, psychologie, sociologie ad.) a je charakteristická mezisektorovostí (preventivní programy a jednotlivé přístupy se rozvíjejí v různých resortech – školství, zdravotnictví, ministerstvo vnitra, dopravy a spravedlnosti).

Stejný autor na straně 23 poukazuje na to, že pojem sociálněpatologické jednání, který se dosud v oblasti primární prevence používal je nově nahrazován pojmem **rizikové chování.** Překonanost termínu sociálněpatologické jednání autor spatřuje v tom, že toto jednání působí stigmaticky, je normativně laděné a klade neobvykle velký důraz na skupinovou/společenskou normu. Rizikové chování vysvětluje jako *„chování, v jehož důsledku dochází k prokazatelnému nárůstu zdravotních, sociálních, výchovných a dalších rizik pro jedince a společnost“*. Pojem rizikového chování se používá především ve školství.

Matějka (2002) rozlišuje v souvislosti s počítačovou kriminalitou také prevenci psychologickou a technologickou.

**Psychologickou prevencí** nazývá *„opatření, která napomáhají vytvářet povědomí o nemorálnosti a společenské nepřijatelnosti právem závazných činů“* (Matějka, 2002, s. 78).

**Technologickou prevencí** pak autor označuje primárně zabezpečení. Na mysli má obecně zabezpečení ICT, proti hackerům a crackerům[19] např. používání a pravidelné aktualizování antivirových programů, instalování zveřejněných záplat atd.

Technologická prevence pak musí působit současně s prevencí psychologickou, jinak nelze nad počítačovou kriminalitou zvítězit (Matějka, 2002).

Jednotlivé druhy prevencí uzavírám prevencí **situační**, která má za cíl minimalizovat příležitosti k páchání trestného činu (Chalupová, 2012), což by mohlo mít také významný vliv na předcházení majetkové kriminality na internetu (např. řádnou registrací a ověřováním reg. údajů osob nabízejících k prodeji zboží na různých inzertních serverech a mnoho dalšího).

Kdo a jak má prevenci zajišťovat bude ve stručnosti popsáno v následujících kapitolách.

### 5.1.1 Preventivní působení v rodině

Ve 4. kapitole této práce je zmínka o tom, že nejsnáze se mohou do role aktérů dostat děti (Krčmářová, 2012).

*„Prvním místem, kde se dítě setkává s výchovným působením je rodina“* (Grecmanová, 2003, s. 13).

Definicí rodiny se podle Opatřila a kol. (1985) zpravidla rozumí *„společenství lidí, svazek dvou rovnoprávných partnerů, malá sociální skupina či buňka, společenská jednotka, která vzniká na základě manželského a pokrevního svazku a představuje komplex specifických vztahů mezi mužem a ženou, mezi rodiči a dětmi, rodinou a společností“* (Grecmanová, 2003, s. 7).

Právě rodiče by si měli uvědomit, jakou roli v životě jejich dětí hraje technologie, aby je vychovávali ke správnému užívání internetu (Krčmářová, 2012).

Ideální výchovné prostředí se odehrává ve zdravé rodině, kde se dítě chová bezprostředně a rodiče se tak k němu mohou snadněji přiblížit, což je důležité pro pochopení

[19] Cracking – prolamování nebo obcházení ochranných prvků počítačového systému, programu nebo aplikací s cílem jejich následného neoprávněného užití (Kolouch, 2013, s. 52).

skutečných rysů a projevů dítěte. Nalezení správného vztahu k dítěti není snadné a to především v době dospívání (Grecmanová, 2003).

Důsledky, jaké může mít nesprávná výchova dětí ve vztahu k ICT a majetku lze volně převzít od Krčmářové (2012), která mezi ně řadí: zavirování počítače (spamy[20] a hoaxy[21]), phishing, sociální inženýrství, hackery (crackery).

Stejná autorka na straně 59 uvádí několik bezpečnostních pravidel pro děti při užívání internetu. Z těchto pravidel vybírám některá související s majetkovou kriminalitou na internetu a doplňuji možná nebezpečí:

1. Bez souhlasu rodiče nikdy nesdělovat osobní informace (adresu, telefony, zvyky) osobě, kterou známe pouze přes internet (sociální inženýrství – nebezpečí podvodu, nebo např. krádeže – vloupání do bytu v době dovolené apod.).
2. Bez porady s rodiči nikomu neposílat své fotografie, čísla kreditních karet, údaje o bankovním účtu (nebezpečí sociálního inženýrství – následovat může podvod, neoprávněné opatření, padělání a pozměnění platebního prostředku[22] apod.).
3. Nikdy nikomu neprozrazovat svoje heslo nebo přihlašovací údaje na internetové stránky nebo do počítače, a to ani svému nejlepšímu příteli (sociální inženýrství – nebezpečí následného podvodu, kdy se pachatel vydává jménem oběti a podvodným způsobem tak vyláká od jeho přátel finanční půjčky).
4. Bez vědomí rodičů si nikdy nedomlouvat schůzku s osobou, kterou známe pouze přes internet a v případě jejich souhlasu nejít sám (nebezpečí zbavení svobody a následné vydírání rodičů).
5. Nikdy neotvírat soubory přiložené k elektronickým zprávám, pakliže byly doručeny od neznámých odesílatelů (nebezpečí phishingu s možností následného podvodu a neoprávněného opatření, padělání a pozměnění platebního prostředku). Zde bych ještě doplnil, že taková příloha může být zaslána i od přítele, který nezná její původ (sám ji nevytvořil) a doporučil bych neotvírat žádné přílohy neznámého původu.

---

20 Spam – nevyžádaný e-mail (Nádběla, 2006, s. 420).

21 Hoax – elektronické šíření poplašné (nepravdivé) zprávy (Nádběla, 2006).

22 Platebním prostředkem jsou míněny i elektronické peníze (Kolouch, 2013, s. 91).

6. Pamatovat si pravidlo, že lákavé nabídky na internetu nemusí být vždy pravdivé - většinou nejsou (hrozí např. nebezpečí podvodu - falešné e-shopy, inzertní a aukční portály).
7. V případě zjištění nelegálního obsahu na internetu informovat rodiče (nebezpečí porušení autorského práva, práv souvisejících s právem autorským a práv k databázi).
8. Na počítači a s internetem pracovat pouze po předchozí domluvě s rodiči ve stanovenou dobu (nebezpečí netolismu[23], s čímž může být spojená např. nepozornost, či neohroženost ve všech výše uvedených bodech).

Jak je z výše uvedeného patrno, úloha rodičů je ve výchově velice důležitá a nelze ji podceňovat. O prevenci v rodinné výchově lze hovořit na úrovni primární i sekundární. Další neméně důležitou institucí ve výchově a vzdělávání je samozřejmě školství.

### 5.1.2 Preventivní působení ve školství

Jak bylo již uvedeno v kapitole 1.2, vzdělávání v České republice je realizováno v souladu se školským zákonem. Systém vzdělávání je pak tímto zákonem řešen ve třech rovinách, a to jako Národní program vzdělávání, Rámcové vzdělávací programy a Školní vzdělávací programy. Preventivní působení v těchto kurikulárních dokumentech je zmiňováno spíše obecně, např. v **Národním programu rozvoje vzdělání,** který je znám také jako Bílá kniha a vypracován byl v roce 2001 ze strany MŠMT, je potřeba prevence obecně zmiňována ve společných otázkách pod druhým bodem nazvaným *„Zvyšování kvality vzdělávání“,* kde je uvedeno, že se *„zvyšuje počet dětí ohrožených ve vývoji znevýhodňujícím socioekonomickým prostředím, žáků s problémy v učení, osobnostním vývoji či sociální adaptaci, žáků zneužívajících návykové látky, šikanujících i šikanovaných a* ***s prekriminálním[24] až kriminálním jednáním.*** *Objevují se i nové požadavky související s měnící se rolí školy. Vedle již tradičního poskytování odborné pomoci pro podporu vzdělávání, profesní orientaci a volbu vzdělávací dráhy* ***půjde i o posílení prevence sociální patologie,*** *o podporu a vytváření podmínek pro rozvoj osobnosti žáků a harmonizaci vztahu rodiny a školy, o podporu integrace dětí se zdravotním postižením do běžných typů škol a o tvorbu inkluzivního prostředí[25]“* (Bílá kniha, 2001, s. 40).

---

23 Závislost na internetu ve všech formách.

24 Disociální chování ještě nedosahující všech znaků kriminality.

25 Přizpůsobeno pro dítě se speciálními vzdělávacími potřebami.

Z výše uvedené citace je patrno, že majetková kriminalita na internetu a obecně problematika ICT nemá ve stávající Bílé knize výsadnějšího postavení v oblasti prevence. Tento trend se však mění dokumentem *„Hlavní směry strategie vzdělávací politiky do roku 2020“*.

Vize MŠMT v těchto hlavních směrech strategie na straně 6 poukazuje na nepřehlédnutelný vliv rozvoje komunikačních technologií a klade důraz na změnu představ o školním vzdělávání a nárocích na něj právě v návaznosti na internet, televizi apod. (Strategie vzdělávání 2020: Hlavní směry vzdělávací politiky do roku 2020, 2014).

Co se týče primární prevence rizikového chování u dětí, žáků a studentů ve školách a školských zařízeních, tak konkrétně k této problematice vydalo MŠMT Metodické doporučení s účinností od 1. listopadu 2010 pod číslem jednacím 21291/2010-28.

Toto Metodické doporučení (MD) již obsahuje konkrétnější informace k primární prevenci rizikového chování u žáků v působnosti MŠMT a dokonce se prioritně zaměřuje na předcházení rozvoje rizik, které směřují mimo jiné také k rizikovým formám komunikace prostřednictvím multimédií, což může mít přímou spojitost s majetkovou kriminalitou páchanou na internetu.

Z obsahu MD je také patrna struktura organizace a řízení primární prevence rizikového chování u žáků. Je zde zmiňována činnost MŠMT, Krajských úřadů, Krajského školského koordinátora prevence, Metodika prevence v pedagogicko-psychologické poradně, dále Ředitele školy a školského zařízení, Školního metodika prevence a konečně činnost Třídního učitele.

MD definuje Minimální preventivní program, který zpracovává školní metodik prevence na jeden školní rok. Tento program podléhá kontrole České školní inspekci, je průběžně vyhodnocován a na konci školního roku probíhá jeho evaluace (Ministerstvo školství, mládeže a tělovýchovy: Metodické pokyny, 2014).

Pakliže tedy není primární prevence konkrétní problematiky obsažena v jiných kurikulárních dokumentech (např. RVP), je koordinace tvorby a kontroly realizace preventivního programu školy v náplni činnosti školního metodika prevence. Ten může při této činnosti spolupracovat s orgány státní správy a samosprávy, které mají v kompetenci problematiku prevence sociálně patologických jevů, avšak také s dalšími zařízeními, působícími v této oblasti, kterými mohou být různá sdružení či projekty, o kterých se blíže zmíním v následující kapitole.

### 5.1.3 Preventivní působení vybraných sdružení a projektů

V rámci primární prevence majetkové kriminality na internetu působí na území České republiky mimo OČTŘ[26] celá řada neziskových organizací, zájmových sdružení občanů, právnických a fyzických osob, také církve či nerepresivní orgány veřejné správy.

Jelikož práce pojednává o majetkové kriminalitě na internetu, uvedu pouze ve zkratce činnost několika vybraných sdružení a projektů působících právě na internetu.

V kapitole 3.1.6 je zmiňováno sdružení CSIRT. Toto sdružení působí na celém území České republiky a svou činností zde ovlivňuje všechny uživatele a veškeré sítě. Konkrétně udržuje zahraniční vztahy se světovými týmy a organizacemi CERT/CSIRT podporující tuto komunitu. Dále spolupracuje v rámci ČR se subjekty, jako jsou ISP[27], banky, bezpečnostní složky, akademický sektor, úřady státní správy atd. Zabývá se školící a osvětovou činností a své služby poskytuje také v oblasti bezpečnosti. Řeší bezpečnostní incidenty a koordinuje je. V poslední době se zaměřuje na prevenci stále častějších DNS útoků[28] (Csirt.cz, 2014).

Webové stránky Policie České republiky odkazují v části prevence – preventivní informace – informační kriminalita na projekt Bezpečný internet.cz (Policie.cz; A, 2014), který byl založen společnostmi Česká spořitelna, Microsoft a Seznam.cz.

Tento projekt vznikl s cílem poukázat na mnohá rizika spojená s používáním internetu, avšak také na to, jak se těmto rizikům úspěšně bránit. Při své činnosti využívá zásadu názornosti, kterou ve výchově aplikoval již J. Á. Komenský a pomocí této zásady nutí různé cílové skupiny vytvářet si správné bezpečnostní návyky při práci s internetem. Své rady, návody a zkušenosti poskytuje zcela zdarma a není vázán na produkty jiných společností. Drží se hesla *„čím více budou uživatelé internetu vědět o rizicích, která jsou s jeho užíváním spojená, tím lépe budou schopni správně reagovat na podvodné nabídky, sociální inženýrství, nebo na útočené viry“* (Bezpecnyinternet.cz, 2014).

---

[26] Orgány činné v trestním řízení (Policie, Státní zastupitelství, Soudy, Vězeňství)

[27] Internete Service Provider – poskytoval internetových služeb.

[28] útočník posílá na DNS servery malé DNS dotazy a oběti jsou na její IP adresu zasílány několikanásobně větší odpovědi, čímž může dojít k vyřazení zařízení z provozu (Csirt,cz, 2014)


Obrázek 4: Screenshot webové stránky bezpecnyinternet.cz (Bezpecnyinternet.cz, 2014).

Praktická část práce je mimo jiné zaměřena na ověření existence preventivních programů zaměřených na problematiku majetkové kriminality na internetu v rámci území města Olomouce, proto považuji za vhodné zmínit také činnost celorepublikového projektu E-Bezpečí, který je realizován Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci, která na něm spolupracuje s dalšími organizacemi.

Projekt je zaměřen obecně na nebezpečné jevy vyskytující se na internetu jako je kyberšikana a sexting[29], kybergrooming[30], kyberstalking[31], hoax, spam a v oblasti majetkové kriminality se specializuje např. na internetové podvody.

29 kybernetické útoky v různých formách na děti a dospělé – vydírání, vyhrožování atd. (E-bezpeci.cz, 2014).

30 komunikace vedoucí k osobním schůzkám (E-bezpeci.cz, 2014).

31 nebezpečné pronásledování (E-bezpeci.cz, 2014).

Do cílové skupiny tohoto projektu spadají žáci od 1. stupně ZŠ, studenti, vychovatelé učitelé, metodici prevence, policisté, pracovníci OSPOD[32] a v neposlední řadě také rodiče.

Mimo vzdělávacích akcí projekt E-Bezpečí realizuje také pravidelná výzkumná šetření celorepublikového charakteru, která se zaměřují na rizikovou komunikaci v online prostředí. Provozuje online poradnu, vydává poutavé tiskoviny pro žáky a učitele a vykonává mnoho dalších aktivit (E-bezpeci.cz, 2014).


Obrázek 5: Screenshot webové stránky e-bezpeci.cz (E-bezpeci.cz, 2014).

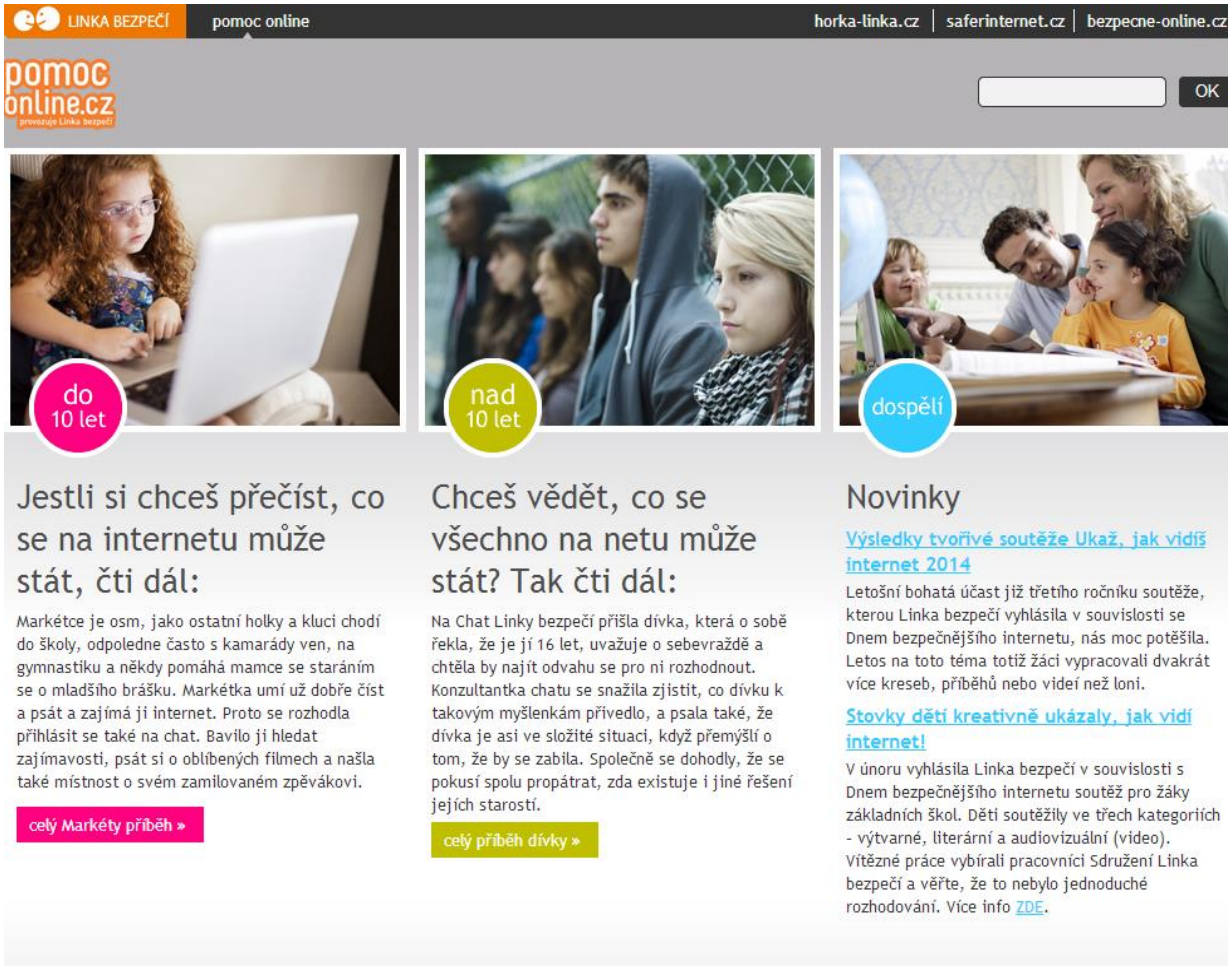
Nelze opomenout ani sdružení Linka bezpečí, která poskytuje své služby dětem a studentům do 25 let. Na Linku bezpečí je možné telefonovat v kteroukoliv dobu, má nepřetržitý provoz. Mimo telefonního čísla 116 111 lze využít také online komunikaci přes chat nebo e-mail.

32 Orgán sociálně-právní ochrany dětí.

Mezi zásady Linky bezpečí patří především anonymita, délka a četnost kontaktu podle potřeby, rovnost přístupu a dobrovolnost.

Sdružení Linka bezpečí provozuje také Rodičovskou linku, která je sice zpoplatněna, avšak rodiče zde mohou žádat o radu v různých obtížných situacích, které se svými dětmi z nějakého důvodu nedokáží sami vyřešit. Komunikace s Linkou bezpečí je v těchto případech možná také emailem.

Linka bezpečí se mimo jiného zabývá také nebezpečnými situacemi na internetu. Majetkové kriminality na internetu se v těchto případech týkají např. pasáže *„Co mám dělat, když mi nefunguje mé heslo, nemohu se dostat do emailové schránky nebo na svůj účet v icq?“,* nebo *„Přišel mi email z banky nebo úřadu, kde mě žádají o rodné číslo a číslo účtu. Prý se jedná o běžnou kontrolu. Mám odepsat?“* (Linkabezpeci.cz, 2014).




Obrázek 6: Screenshot webové stránky www.pomoc-online.cz provozované sdružením Linka bezpečí (Linkabezpeci.cz, 2014).

Přehled dalších institucí zabývajících se prevencí kriminality v České republice je stručně uveden v následující kapitole.

### 5.1.4 Prevence kriminality v České republice

Poslední kapitola teoretické části práce popisuje stručně činnost institucionálních orgánů zabývajících se obecně prevencí kriminality na území České republiky. V tomto případě lze hovořit o všech úrovních prevence a tedy primární, sekundární i terciální.

Chalupová (2012) uvádí, že v roce 1993 byl při Ministerstvu vnitra zřízen usnesením vlády **Republikový výbor pro prevenci kriminality.** Jedná se o stálý orgán zabývající se v České republice problematikou prevence kriminality a jde o meziresortní iniciační, koordinační a metodický orgán.

Činností tohoto výboru je vytváření koncepce preventivní politiky vlády České republiky právě na meziresortní úrovni a její konkretizace na úrovni místní. K hlavním úkolům republikového výboru pro prevenci kriminality patří metodické vedení a podpora rozvoje preventivních činností a aktivit na místní úrovni.

Struktura prevence kriminality v České republice je rozdělena do tří hlavních okruhů. Jedná se o prevenci sociální [33], prevenci situační a prevenci viktimnosti[34] a pomoc obětem trestných činů. Prevence se realizuje na všech základních stupních (primární, sekundární a terciální) a na třech úrovních (meziresortní, rezortní a místní).

Autorka dále uvádí, že od roku 1996 funguje v rámci Ministerstva vnitra České republiky také **Odbor prevence kriminality (OPK),** mezi jehož základní činnosti patří mimo jiné partnersky se podílet na projektu Kyberšikana – projekt E-Synergie, což je mladší sourozenec výše představeného projektu E-Bezpečí, do jehož působnosti spadá mimo jiné i primární prevence majetkové kriminality na internetu.

Dále se má OPK podílet na přípravě nové Strategie prevence kriminality na léta 2012-2015, která má v rámci prioritních témat uvedenou mimo jiné trestnou činnost páchanou prostřednictvím elektronických médií.

Prevence kriminality spadá také do náplně práce Policie České republiky (PČR), která je podřízena Ministerstvu vnitra ČR.

Předcházet trestné činnosti je dáno především § 2 Zákona o Policii České republiky.

Preventivní činnost na úrovni Policejního prezidia ČR řídí **republikový koordinátor prevence kriminality.** Tento zodpovídá také za preventivní činnost celé PČR.

---

[33] Aktivity ovlivňující proces socializace a sociální integrace a aktivity zaměřené na změnu nepříznivých společenských a ekonomických podmínek, jež jsou považovaných za klíčové příčiny páchaní trestné činnosti (Chalupová, 2012, s. 38).

[34] Disponovanost člověka stát se obětí (Zoubková, 2011).

Preventivní činnost na úrovni útvarů s celostátní působností řídí koordinátor prevence kriminality těchto útvarů.

Na úrovni krajských ředitelství policie ČR řídí tuto činnost **krajský koordinátor prevence kriminality.** Tento řídí také práci koordinátorů jednotlivých územních odborů PČR, kteří vykonávají preventivní činnost na této úrovni.

V rámci Krajského ředitelství policie Olomouckého kraje (KROK) byla z preventivní činnosti Oddělení tisku a prevence KROK v nedávné době zveřejněna na webových stránkách Policie České republiky „Beseda na téma nebezpečí internetové komunikace dětí pro rodiče a pedagogy“, která se uskutečnila na základní škole v obci Ptení na Prostějovsku. Beseda nebyla sice zaměřena přímo na problematiku majetkové kriminality na internetu, avšak zasahovala do ní alespoň okrajově desaterem bezpečného internetu (Policie.cz; B, 2014).

Z výše uvedeného přehledu je zřejmé, že prevencí majetkové kriminality na internetu se zabývá celá řada subjektů.

Otázkou však zůstává, jak je tato prevence účinná a efektivní.

Statistické údaje PP obsažené v příloze č. 2 efektivnosti prevence v této oblasti dosud příliš nenasvědčují, ba naopak je zřejmé, že majetkové trestné činy na internetu, potažmo podvody, stále narůstají.

Právě z tohoto důvodu je nutné všechna preventivní opatření řádně evaluovat a dle výsledku této evaluace[35] rozhodnout o jejich dalším osudu - úprava, či zrušení (Chalupová, 2013).

Otázkou, zdali existují preventivní programy zabývající se problematikou majetkové kriminality na internetu na středních školách a gymnáziích v okrese Olomouc, jsem se zabýval v praktické části práce.

[35] Proces hodnocení preventivní intervence (Chalupová, 2013).

# II. PRAKTICKÁ ČÁST

V praktické části práce se mi nabízely tři možnosti výzkumu (průzkumu). První možností bylo provedení případových studií vybraných trestných činů majetkové kriminality páchané na internetu osobami mladistvými a nezletilci.

Druhou možností byla obsahová analýza dokumentů RVP se zaměřením na výskyt prevence ve vztahu k majetkové kriminalitě na internetu a poslední třetí možností bylo dotazníkovou metodou ověřit od školních metodiků prevence existenci preventivních programů zaměřených na problematiku majetkové kriminality na internetu v rámci středních škol a gymnázií v okrese Olomouc.

Jelikož teoretická část práce přesahuje spíše do oblasti kriminality, rozhodl jsem se praktickou část práce zpracovat naopak v oblasti pedagogické.

Z tohoto důvodu jsem si zvolil třetí možnost a tedy dotazníkovou metodou ověřit od školních metodiků prevence existenci preventivních programů zaměřených na problematiku majetkové kriminality na internetu v rámci středních škol a gymnázií v okrese Olomouc.

Cíle praktické části práce jsem zvolil následující.

# 6. STANOVENÍ CÍLE PRÁCE

Hlavním cílem praktické části práce je ověřit **existenci preventivních programů zaměřených na problematiku majetkové kriminality na internetu v rámci středních škol a gymnázií v okrese Olomouc,** a pakliže existují, tak zdali byly evaluovány.

Tento cíl práce jsem zvolil proto, abych zjistil současný stav primární prevence v dané problematice na úrovni středních škol a gymnázií v okrese Olomouc, což byla první úroveň průzkumu.

K tomu abych ověřil, zdali nemohou mít studenti středních škol a gymnázií v okrese Olomouc potřebnou vybavenost v dané problematice ze základních škol, jsem provedl tentýž průzkum na stejném počtu náhodně vybraných základní škol v okrese Olomouc, což byla druhá úroveň průzkumu.

Otázku evaluace těchto preventivních programů jsem zařadil proto, abych ověřil, zdali se tyto programy, pakliže existují, zpětně vyhodnocují, což je nesmírně důležité pro jejich efektivnost (Chalupová, 2013).

Výsledek této evaluace již nebyl z důvodu omezeného rozsahu bakalářské práce ověřován a otázka účinnosti těchto preventivních programů tak zůstává otevřenou k dalšímu zkoumání.

# 7. VÝZKUMNÁ METODA

Jako výzkumnou metodu jsem zvolil metodu explorativní. Výzkumnou technikou byl v rámci metody explorativní zvolen dotazník a to z důvodu rychlého shromáždění dat od vícera subjektů.

Tato technika je postavena na dotazech a je příbuzná po metodologické stránce bezprostřednímu ústnímu rozhovoru – interview (Švec, 2009). Dotazy jsou však písemné. V našem případě byly položeny elektronickou formou – emailem a posléze také telefonicky.

Samotné rozesílání dotazníků cílovým osobám se nazývá administrování dotazníku a cílové osoby se označují jako respondenti (Švec, 2009). V našem případě jsou pod označením respondenti myšleni primárně školní metodici prevence nebo osoby vykonávající jejich činnost, nejsou-li tato místa na konkrétních školách obsazena.

Jednotlivé otázky v dotazníku jsou označeny jako položky. Náš dotazník obsahoval pouze tři položky, které byly tvořeny uzavřenými, dichotomickými otázkami, což znamená, že na ně existovaly pouze dvě vzájemně se vylučující odpovědi ANO/NE (Chráska, 2007). Položky v dotazníku měly následující znění:

**Položka č. 1**
Objevil se na Vaší škole případ majetkové kriminality na internetu, kde v roli oběti nebo pachatele byl Váš žák/student?
**Položka č. 2**
Existuje na Vaší škole preventivní program zaměřený přímo na problematiku majetkové kriminality na internetu?
**Položka č. 3** (pouze v případě, že odpověď na položku č. 2 byla ANO)
Proběhla evaluace Vašeho preventivního programu zaměřeného na problematiku majetkové kriminality na internetu?

I přesto, že byly otázky jednotlivých položek uzavřené, měli respondenti možnost, ke každé připojit vlastní poznámku.

Mimo položek č. 1-3, obsahoval dotazník také úvod, instrukce k jeho vyplnění, způsob jeho odeslání a nakonec také poděkování respondentům za jejich spolupráci. Konkrétní znění dotazníku je obsaženo v příloze č. 6.

# 8. CHARAKTERISTIKA SOUBORU ŠETŘENÍ

Základní soubor průzkumu tvoří všechny subjekty, o kterých chce výzkumník získat informace (Švec, 2009). V našem případě tvořily základní soubor na první úrovni průzkumu všechny střední školy a gymnázia v okrese Olomouc, kterých je dle dostupných informací na internetu, celkem 35 (Stredniskoly.cz, 2014).

Na druhé úrovni průzkumu tvořily základní soubor všechny základní školy v okrese Olomouc, kterých je dle dostupných informací na internetu, celkem 105 (Zakladniskoly.cz, 2014).

Abych vyrovnal poměr mezi počtem středních škola a gymnázií v okrese Olomouc s počtem základních škol v okrese Olomouc, provedl jsem ze základního souboru druhé úrovně průzkumu náhodný výběr 35 subjektů. Náhodný výběr proto, že je považován za nejlepší způsob, jak určit výběrový soubor (Švec, 2009).

# 9. ČASOVÁ ORGANIZACE

Po vypracování dotazníku a stanovení základního a výběrového souboru průzkumu jsem provedl předvýzkum, abych si ověřil funkčnost zvolené výzkumné metody, srozumitelnost položených otázek, časovou náročnost apod. (Švec, 2009).

Tento předvýzkum jsem realizoval na náhodně vybraných šesti školách, přičemž z každé úrovně průzkumu byly elektronickou poštou osloveny tři školy (jejich metodici prevence).

Následně získané odpovědi jsem vyhodnotil a provedl konečnou úpravu dotazníku. Oslovené respondenty jsem zařadil zpět do průzkumu.

Finální verzi dotazníku jsem současně rozeslal elektronickou poštou základnímu i výběrovému souboru průzkumu, což činilo celkem 70 subjektů.

Dotazníky jsem se snažil adresovat přímo školním metodikům prevence, byla-li jejich emailová adresa známa. V opačném případě, byly dotazníky zasílány na hlavní emailové adresy oslovených škol.

Výsledek tohoto elektronického způsobu dotazování byl však pro učinění relevantních závěrů zcela nedostatečný.

Na první úrovni se průzkumu prováděného elektronickou formou účastnilo pouze 5 respondentů, což je 14,3 % dotázaných, z tohoto počtu mělo 40 % preventivní program zaměřený na problematiku majetkové kriminality na internetu a evaluace proběhla v 20 % z nich.

Na druhé úrovni průzkumu elektronicky odpovědělo 10 respondentů, což je 28,6 % dotázaných, z toho 30 % mělo preventivní program zaměřený na problematiku majetkové kriminality na internetu, a u 10 % z nich proběhla evaluace.

Chráska (2007) uvádí, že se údaje o průměrné návratnosti dotazníků rozesílaných poštou v literatuře rozcházejí, avšak pohybují se v rozmezí od 30 % do 60 %. Průzkum realizovaný elektronickou formou v našem případě nedosáhl ani 30 %.

Vzhledem k výše uvedenému bylo nutné změnit způsob komunikace, a proto bylo přistoupeno k dotazování telefonickému.

Respondenti byli tímto způsobem oslovování podle pořadí, ve kterém byli zařazeni při dotazování elektronickou poštou. Pakliže nebyl některý z respondentů v daném pořadí zastižen, byl přesunut na konec pořadí a poté opětovně osloven.

Tímto způsobem se podařilo získat odpovědi od dostatečného počtu respondentů, aby mohly být presentovány výsledky šetření.

# 10. VÝSLEDEKY ŠETŘENÍ

Získané odpovědi na položené otázky v položkách č. 1-3 jsem průběžně zaznamenával do předem připravených tabulek, čímž bylo prakticky zamezeno vzniku možných nepřesností v jejich interpretaci.

Tabulka číslo 1 obsahuje výsledky první úrovně průzkumu, a tedy zaznamenané odpovědi respondentů na středních školách a gymnáziích v okrese Olomouc.

Ve sloupci *poznámka k položce* je vyjádřeno číslo položky (položek), u kterých respondenti připojili svoji poznámku.

Položky dotazníku byly tedy následující:

**Položka č. 1 -** Objevil se na Vaší škole případ majetkové kriminality na internetu, kde v roli oběti nebo pachatele byl Váš žák/student?

**Položka č. 2 - Existuje na Vaší škole preventivní program zaměřený přímo na problematiku majetkové kriminality na internetu?**

**Položka č. 3** (pouze v případě, že odpověď na položku č. 2 byla ANO)

Proběhla evaluace Vašeho preventivního programu zaměřeného na problematiku majetkové kriminality na internetu?

Tabulka 1: Zaznamenané odpovědi respondentů na první úrovni průzkumu.

| Přiřazené číslo školy | Odpověď na položku č. 1 | **Odpověď na položku č. 2** | Odpověď na položku č. 3 | Poznámka k položce |
|---|---|---|---|---|
| 1. | ANO | **NE** | NE | |
| 2. | NE | **NE** | NE | |
| 3. | NE | **NE** | NE | |
| 4. | NE | **ANO** | ANO | 3 |
| 5. | NE | **NE** | NE | |
| 6. | NE | **NE** | NE | |
| 7. | NE | **NE** | NE | 2 |
| 8. | NE | **NE** | NE | 2 |
| 9. | x | x | x | x |
| 10. | NE | **NE** | NE | |
| 11. | NE | **NE** | NE | |
| 12. | NE | **NE** | NE | 2 |

| | | | | |
|---|---|---|---|---|
| 13. | NE | **NE** | NE | |
| 14. | NE | **NE** | NE | 2 |
| 15. | NE | **NE** | NE | |
| 16. | NE | **NE** | NE | |
| 17. | NE | **ANO** | NE | 1, 2, 3 |
| 18. | NE | **NE** | NE | 1 |
| 19. | NE | **NE** | NE | - |
| 20. | NE | **NE** | NE | |
| 21. | NE | **NE** | NE | |
| 22. | NE | **NE** | NE | 2 |
| 23. | NE | **NE** | NE | |
| 24. | NE | **NE** | NE | 2 |
| 25. | x | x | x | x |
| 26. | NE | **NE** | NE | |
| 27. | x | x | x | x |
| 28. | NE | **NE** | NE | |
| 29. | x | x | x | x |
| 30. | x | x | x | x |
| 31. | NE | **NE** | NE | |
| 32. | NE | **NE** | NE | |
| 33. | NE | **NE** | NE | 2 |
| 34. | NE | **NE** | NE | 2 |
| 35. | x | x | x | x |

Z dat obsažených v předchozí tabulce je zřejmé, že preventivní program zaměřený přímo na problematiku majetkové kriminality na internetu má jen 6,9 % středních škol a gymnázií v okrese Olomouc. Z toho počtu byl pouze jeden takový program evaluován. S případem majetkové kriminality na internetu, kde v roli oběti nebo pachatele byl žák/student oslovené školy se setkalo 3,4 % dotázaných.

Tabulka číslo 2 obsahuje odpovědi respondentů druhé úrovně průzkumu, kdy se jedná o nahodile vybrané základní školy v okrese Olomouc.

Tabulka 2: Zaznamenané odpovědi respondentů na druhé úrovni průzkumu.

| Přiřazené číslo školy | Odpověď na položku č. 1 | **Odpověď na položku č. 2** | Odpověď na položku č. 3 | Poznámka k položce |
|---|---|---|---|---|
| 1. | NE | **NE** | NE | |
| 2. | NE | **NE** | NE | |
| 3. | NE | **NE** | NE | |
| 4. | NE | **NE** | NE | |
| 5. | NE | **NE** | NE | |
| 6. | NE | **NE** | NE | |
| 7. | x | x | x | x |
| 8. | x | x | x | x |
| 9. | NE | **NE** | NE | |
| 10. | NE | **ANO** | NE | |
| 11. | NE | **NE** | NE | |
| 12. | NE | **NE** | NE | 1 |
| 13. | NE | **NE** | NE | |
| 14. | NE | **NE** | NE | |
| 15. | NE | **NE** | NE | |
| 16. | NE | **NE** | NE | |
| 17. | ANO | **ANO** | ANO | 2 |
| 18. | NE | **NE** | NE | |
| 19. | NE | **NE** | NE | |
| 20. | NE | **NE** | NE | |
| 21. | x | x | x | x |
| 22. | x | x | x | x |
| 23. | NE | **NE** | NE | |
| 24. | NE | **NE** | NE | |
| 25. | ANO | **ANO** | ANO | |
| 26. | NE | **NE** | NE | |
| 27. | NE | **ANO** | NE | |
| 28. | NE | **NE** | NE | 2 |
| 29. | NE | **NE** | NE | |

| | | | | |
|---|---|---|---|---|
| 30. | x | x | x | x |
| 31. | NE | **NE** | NE | |
| 32. | NE | **NE** | NE | |
| 33. | NE | **NE** | NE | |
| 34. | NE | **NE** | NE | |
| 35. | NE | **NE** | NE | |

Z dat obsažených v předchozí tabulce je zřejmé, že preventivní program zaměřený přímo na problematiku majetkové kriminality na internetu má pouze 13,3 % náhodně vybraných základních škol v okrese Olomouc. Z tohoto počtu byla evaluována pouze polovina těchto programů, a s případem majetkové kriminality na internetu, kde v roli oběti nebo pachatele byl žák/student oslovené školy se setkalo 6,7 % dotázaných respondentů.

# 11. INTERPRETACE A DISKUSE VÝSLEDKŮ

Hlavním cílem praktické části práce bylo v první úrovni ověřit existenci preventivních programů zaměřených na problematiku majetkové kriminality na internetu v rámci středních škol a gymnázií v okrese Olomouc (položka č. 2)[36], a pakliže existují, tak zdali byly evaluovány (položka č. 3)[37]. Doplňující otázka (položka č. 1)[38] měla zjistit, zdali se objevil na oslovených školách případ majetkové kriminality na internetu, kde v roli oběti nebo pachatele byl jejich žák/student.

Stejný průzkum byl pro srovnání proveden také na náhodně vybraném souboru základních škol v okrese Olomouc.

## 11.1 Výsledky první úrovně průzkumu

Provedeným průzkumem na první úrovni bylo zjištěno, že **na převážné většině středních škol a gymnázií v okrese Olomouc neexistují preventivní programy zaměřené přímo na problematiku majetkové kriminality na internetu. Jejich existence byla potvrzena pouze ve dvou případech a z toho pouze v jednom případě, byl tento preventivní program evaluován.**

Souhrnné výsledky k této hlavní výzkumné otázce jsou uvedeny v následující tabulce.

Tabulka 3: Souhrnné výsledky prováděného průzkumu na první úrovni.

| | | |
|---|---|---|
| Počet středních škol a gymnázií v okrese Olomouc: | 35 | |
| Počet oslovených respondentů na těchto školách: | 35 | |
| Počet oslovených respondentů, kteří se průzkumu účastnili: | 29 | |
| Existenci preventivního programu zaměřeného přímo na problematiku majetkové kriminality na internetu | potvrdilo: | 2 |
| | vyvrátilo: | 27 |

Doplňující otázkou (položka č. 1)[39] ověřující výskyt kriminality tohoto druhu na oslovených školách bylo zjištěno, že takový případ se vyskytl pouze v jednom případě. Shodou okolností právě na škole, která nemá preventivní program zaměřený na problematiku majetkové kriminality na internetu.

[36] Dotazník je obsažen v příloze č. 6

[37] taktéž

[38] taktéž

[39] taktéž

## 11.2 Výsledky druhé úrovně průzkumu

Informovanost studentů středních škola a gymnázií v dané problematice zřejmě neproběhla ani na předchozí, absolvované úrovni vzdělávání a tedy na základních školách.

Průzkum druhé úrovně sice proběhl pouze na výběrovém souboru základních škol v okrese Olomouc, avšak i přesto byla existence preventivního programu zaměřeného přímo na majetkovou kriminalitu na internetu potvrzena pouze u tří oslovených základních škol. Evaluace (položka č. 3)[40] pak proběhla pouze ve dvou případech.

Souhrnné výsledky k vedlejší výzkumné otázce (položka č. 2)[41] jsou obsaženy v následující tabulce.

Tabulka 4: Souhrnné výsledky prováděného průzkumu na druhé úrovni.

| | | |
|---|---|---|
| Počet náhodně vybraných základních škol v okrese Olomouc: | 35 | |
| Počet oslovených respondentů na těchto školách: | 35 | |
| Počet oslovených respondentů, kteří se průzkumu účastnili: | 30 | |
| Existenci preventivního programu zaměřeného přímo na problematiku majetkové kriminality na internetu | potvrdilo: | 3 |
| | vyvrátilo: | 27 |

Doplňující otázkou (položka č. 1)[42] ověřující výskyt kriminality tohoto druhu na oslovených základních školách bylo zjištěno, že takový případ se vyskytl dvakrát, přičemž v obou případech již na dotčených školách existuje preventivní program zaměřený na tuto problematiku.

Absenci preventivních programů zaměřených přímo na majetkovou kriminalitu na internetu někteří telefonicky oslovení respondenti přisuzovali tomu, že na jejich škole se dosud podobný případ nevyskytl, nebo o něm alespoň nebyl pedagogický sbor ze strany žáků/studentů informován. Tento argument však z pohledu primární prevence, která je zaměřena obecně na předcházení kriminality, neobstojí.

40 Dotazník je obsažen v příloze č. 6

41 taktéž

42 taktéž

## 11.3 Komparace výsledků průzkumu

Komparací průzkumů na první a druhé úrovni bylo zjištěno, že nepatrně větší zkušenosti mají s problematikou majetkové kriminality páchané na internetu v okrese Olomouc, školní metodici prevence na základních školách.

Průzkum také naznačuje, že základní školy by mohly být i pružnější v reakcích na výskyt tohoto rizikového chování, neboť v obou případech, kde byl tento druh kriminality registrován, existují preventivní programy zaměřené přímo na tuto problematiku.

Je však otázkou, zdali preventivní programy zaměřené přímo na problematiku majetkové kriminality na internetu byly na předmětných základních školách vytvořeny až po zjištění tohoto rizikového chování, nebo ještě před ním.

Stejně tak nebylo průzkumem zjištěno, kdy přesně se zatím s jediným případem majetkové kriminality na internetu setkali na jedné z oslovených středních škol a gymnázií, neboť zde existuje možnost, že na toto rizikové chování jednoduše nebyl dostatečný časový prostor zareagovat.

Ze statistického hlediska jsou však rozdíly na první a druhé úrovni průzkumu zcela zanedbatelné a lze vyslovit závěr, že **převážná většina oslovených škol v okrese Olomouc nemá preventivní program, který by byl přímo zaměřený na problematiku majetkové kriminality na internetu.**

## 11.4 Vyhodnocení poznámek k jednotlivým položkám

Z poznámek k jednotlivým položkám, které jsou obsaženy v příloze č. 7 a 8, lze ověřit, že na primární prevenci majetkové kriminality na internetu a obecně bezpečnosti v kyberprostoru se v rámci okresu Olomouc podílí mimo již zmiňovaného projektu e-Bezpečí, také Oddělení informační kriminality KROK a v neposlední řadě také Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci.

Je tedy zřejmé, že primární prevence v oblasti majetkové kriminality na internetu v okrese Olomouc probíhá a postupně proniká jak do středních škol a gymnázií, tak také do škol základních, kde je realizována převážně formou besed s Policií České republiky.

# 12. ZÁVĚR

Bakalářská práce pojednává obecně o jinak široce obsáhlém tématu majetkové kriminality na internetu. Popisuje tuto kriminalitu jako společensky velice nebezpečnou a to hlavně z důvodu její anonymity a absence hranic k jejímu páchání, ať už ve vztahu k věku aktérů nebo místu jednání, které může být prakticky kdekoliv na světě (je-li z tohoto místa přístup k internetu).

Teoretická část práce popisuje tuto kriminalitu v pojmovém aparátu, poskytuje krátký exkurz do její historie ve světě i na našem území. Podrobněji popisuje a zaměřuje se na její nejčastější výskyt v podobě podvodného jednání a v neposlední řadě poskytuje také přehled subjektů působících na různých úrovních prevence, ať už v oblasti primární, sekundární, či terciární.

Praktická část práce je pak zaměřena především na primární prevenci v rámci středních škol a gymnázií v okrese Olomouc. Na první úrovni dotazníkového průzkumu zjišťuje primárně existenci preventivních programů zaměřených na problematiku majetkové kriminality na internetu. Doplňující otázky jsou pak zaměřeny na ověření zpětného hodnocení – evaluaci takových preventivních programů (pakliže existují) a dále na to, zdali se na oslovených školách vůbec vyskytl případ majetkové kriminality na internetu. Jako respondenti byli oslovováni hlavně školní metodici prevence.

Pro srovnání byl proveden na druhé úrovni stejný průzkum také na nahodile vybraných základních školách v okrese Olomouc.

Zjištěné výsledky průzkumu však ukázaly, že na převážné většině (93.1 %) středních škol a gymnáziích v okrese Olomouc neexistují preventivní programy zaměřené přímo na problematiku majetkové kriminality na internetu.

Obdobný výsledek byl zaznamenán také průzkumem na vybraných základních školách v okrese Olomouc, kde bylo zjištěno, že preventivní program zaměřený přímo na majetkovou kriminalitu na internetu nemají na 86.7 % oslovených škol.

Prevencí v oblasti majetkové kriminality na internetu se věnuje celá řada subjektů zmiňovaných v této práci, otázkou k dalšímu výzkumu by mohla být například evaluace tohoto preventivního působení, neboť dle statistik PP obsažených v příloze č. 2 je zřejmé, že tento druh kriminality stále narůstá a to celkem znepokojujícím tempem.

Primární prevenci je nutné zaměřovat také na potencionální pachatele této kriminality, nejen na její oběti.

Preventivně by měli působit v první řadě rodiče, kteří by měli mít kontrolu nad činností svých dětí v kyberprostoru, a proto by bylo vhodné šířit osvětu také do jejich řad.

Na úrovni školství lze hovořit v souvislosti s primární prevencí o šíření právního vědomí žáků a studentů v dané problematice a tedy o tom, co je a není na internetu protiprávní – trestné.

Nemalou měrou by mohla ke snížení majetkové kriminality na internetu přispět také prevence situační, například ověřování registračních údajů na různých inzertních webech, nebo používání antivirových programů a podobného software na počítačových systémech atd..

Věřím, že bakalářská práce na téma „majetková kriminalita na internetu“ bude přínosem nejen pro pedagogické pracovníky, ale také pro každého, kdo se touto problematikou blíže zabývá.

# Seznam použitých zkratek

| | |
|---|---|
| ICT | Information and Communication Technology (informační a komunikační technologie) |
| KROK | Krajské ředitelství policie Olomouckého kraje |
| MD | Metodické doporučení k primární prevenci rizikového chování u dětí, žáků a studentů ve školách a školských zařízeních č.j. 21291/2010-28 |
| MŠMT | Ministerstvo školství, mládeže a tělovýchovy |
| NPV | Národní program vzdělávání |
| OZ | Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů |
| PP | Policejní prezídium České republiky |
| PZ | Zákon č. 200/1990 Sb., o přestupcích, ve znění pozdějších předpisů |
| RVP | Rámcový vzdělávací program |
| ŠZ | Zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), ve znění pozdějších předpisů |
| ŠVP | Školní vzdělávací program |
| TrZ | Zákon č. 140/1961 Sb., trestní zákon, účinný do 31. 12. 2009 |
| TŘ | Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád) ve znění pozdějších předpisů |
| TZ | Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů |
| ZP | známý pachatel |
| ZSVM | Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže) |

# Seznam literatury a zdrojů


*Aukro.cz* [online]. [cit. 2014-06-02]. Dostupné z: http://info.aukro.cz/about/

*Bazos.cz* [online]. [cit. 2014-06-02]. Dostupné z: http://www.bazos.cz/

*Bezpecnyinternet.cz* [online]. [cit. 2014-05-21]. Dostupné z:http://www.bezpecnyinternet.cz

*Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online.* Editor Linda McCarthy, Denise Weldon-Siviy. Praha: CZ.NIC, 2013, ISBN 978-90-904248-6-9.

*Businessinfo.cz.* [online]. [cit. 2014-05-21]. Dostupné z: http://www.businessinfo.cz/cs/clanky/elektronicky-obchod-opu-13390.html#b1

*Conventions.coe.int.* [online]. [cit. 2014-05-21]. Dostupné z: http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm

*Csirt.cz.* [online]. [cit. 2014-05-21]. Dostupné z: http://www.csirt.cz/files/csirt/statistics/stats.html

Česká republika. Občanský zákoník. In: *89/2012*. 2012.

Česká republika. Trestní zákoník. In: *40/2009*. 2009.

Česká republika. Zákon o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů: Zákon o soudnictví ve věcech mládeže. In: *218/2003*. 2003.

Česká republika. Zákon o předškolním, základním, středním, vyšším odborném a jiném vzdělávání: Školský zákon. In: *561/2004*. 2004.

Česká republika. Zákon o přestupcích. In: *200/1990*. 1990.

*Ebay.com* [online]. [cit. 2014-06-02]. Dostupné z: http://www.ebay.com/

*E-bezpeci.cz* [online]. [cit. 2014-05-21]. Dostupné z:http://www.e-bezpeci.cz

GRECMANOVÁ, Helena. Obecná pedagogika II. Olomouc: Hanex, 2003, ISBN 80-85783-24-X.

HRUŠKA, Vlastimil. Mezinárodní vědecká konference - Olomouc, 6. května 2014: Rizika internetu v pohledu Policie ČR. [online]. [cit. 2014-06-02]. Dostupné z: http://konference.e-bezpeci.cz./?akce=prezentace

*Hyperinzerce.cz* [online]. [cit. 2014-06-02]. Dostupné z: http://hyperinzerce.cz/

CHALUPOVÁ, Kateřina. *Základy prevence kriminality pro pedagogické pracovníky: sborník studií.* Editor Michaela Štefunková, Jaroslav Šejvl. Praha: Klinika adiktologie, 1. lékařská fakulta Univerzity Karlovy v Praze a Všeobecná fakulta nemocnice v Praze ve vydavatelství Togga, 2012, ISBN 9788087258-97-5.

CHRÁSKA, Miroslav. *Metody pedagogického výzkumu: základy kvantitativního výzkumu.* Praha: Grada Publishing, 2007, ISBN 978-80-247-1369-4.

*IKup.cz* [online]. [cit. 2014-06-02]. Dostupné z: http://ikup.cz/

*Internetworldstats.com* [online]. [cit. 2014-05-22]. Dostupné z: http://internetworldstats.com/

JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007, ISBN 978-80-247-1561-2.

KANTOROVÁ, Jana. *Vybrané kapitoly z obecné pedagogiky I.* Olomouc: Hanex, 2008, ISBN 978-807-4090-240.

KOLOUCH, Jan, VOLECKÝ, Petr. *Trestněprávní ochrana před kybernetickou kriminalitou*. Praha: Policejní akademie, 2013, ISBN 978-80-7251-402-1

KRČMÁŘOVÁ, Barbora. *Děti a online rizika: sborník studií.* Sdružení Linka bezpečí, 2012, ISBN 978-809-0492-028.

KUCHTA, Josef. *Kurs trestního práva. Trestní právo hmotné. Zvláštní část.* Praha, C. H. Beck, 2009.

*Linkabezpeci.cz* [online]. [cit. 2014-06-02]. Dostupné z: http://www.linkabezpeci.cz/

*Lupa.cz* [online]. [cit. 2014-05-21]. Dostupné z: http://www.lupa.cz/clanky/pharming-je-zpet-a-silnejsi/

MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, ISBN 80-722-6419-2.

MATOUŠKOVÁ, Ingrid. *Aplikovaná forenzní psychologie*. Praha: Grada, 2013, Psyché (Grada). ISBN 978-80-247-4580-0.

Ministerstvo školství, mládeže a tělovýchovy: Metodické pokyny. [online]. [cit. 2014-06-02]. Dostupné z: http://www.msmt.cz/file/20274

MIOVSKÝ, Michal a kol. *Primární prevence rizikového chování ve školství.* Praha: Centrum adiktologie, 2010, ISBN978-80-87258-47-7.

MITNICK, Kevin a Roman RAK. *Umění klamu: (vybrané problémové okruhy výzkumu).* Gliwice: Helion, 2003, ISBN 8373612106.

MUSIL, Stanislav. *Počítačová kriminalita: nástin problematiky: kompendium názorů specialistů*. Praha: Institut pro kriminologii a sociální prevenci, 2000, ISBN 80-86008-80-0.

NÁDBĚLA, Josef. *Velký počítačový slovník.* Kralice na Hané: Computer Media, 2006, ISBN 80-86686-56-6.

*Národní program rozvoje vzdělávání v České republice: Bílá kniha.* Praha: Ústav pro informace ve vzdělávání, 2001, ISBN 80-211-0372-8

*Novinky.cz; A* [online]. [cit. 2014-05-21]. Dostupné z: http://www.novinky.cz/finance/316331-nova-metoda-platby-za-zbozi-z-e-shopu-bude-mozne-zaplatit-az-po-vyzkouseni.html

*Novinky.cz; B* [online]. [cit. 2014-05-21]. Dostupné z: http://www.novinky.cz/internet-a-pc/325792-nebezpecny-virus-cili-na-bankovni-ucty-v-cesku.html

*Odklepnuto.cz* [online]. [cit. 2014-06-02]. Dostupné z: http://www.odklepnuto.cz/

*Policie.cz; A* [online]. [cit. 2014-05-22]. Dostupné z: http://www.policie.cz/clanek/rady-policie-cr-a-informace-o-prevenci-143872.aspx

*Policie.cz; B* [online]. [cit. 2014-06-10]. Dostupné z: http://www.policie.cz/clanek/rizikovy-kyberprostor.aspx

PRŮCHA, Jan, WALTEROVÁ, Eliška, MAREŠ, Jiří. *Pedagogický slovník.* Praha: Portál, 2008, ISBN 978-80-7367-416-8.

PRŮCHA, Jan, WALTEROVÁ, Eliška, MAREŠ, Jiří. *Pedagogický slovník.* Praha: Portál, 2009, ISBN 978-807-3676-476.

*Sbazar.cz* [online]. [cit. 2014-06-02]. Dostupné z: http://napoveda.seznam.cz/cz/sbazar/podvodne-jednani/nigerijske-dopisy/

SMEJKAL, Vladimír. *Internet a §§§*. Praha: Grada, 2001, ISBN 80-247-0058-1.

SMEJKAL, Vladimír. *Počítačové právo*. Praha: C. H. Beck, 1995, ISBN 80-7179-009-5.

Strategie vzdělávání 2020: Hlavní směry vzdělávací politiky do roku 2020. [online]. [cit. 2014-06-02]. Dostupné z: http://www.vzdelavani2020.cz/images_obsah/dokumenty/hlavni-smery-strategie-vzdelavaci-politiky-cr-2020.pdf

*Stredniskoly.cz* [online]. [cit. 2014-06-09]. Dostupné z: http://www.stredniskoly.cz/seznam-skol/olomoucky-kraj/olomouc/

ŠVEC, Štefan. *Metodologie věd o výchově: kvantitativně-scientické a kvalitativně-humanitní přístupy v edukačním výzkumu.* Překlad Jana Cacková. Brno: Paido, 2009, ISBN 978-807-3151-928.

*Zakladniskoly.cz* [online]. [cit. 2014-06-09]. Dostupné z: http://www.zakladniskoly.cz/seznam-skol/olomoucky-kraj/olomouc/

ZOUBKOVÁ, Ivana. *Kriminologický slovník*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2011, ISBN 978-807-3803-124.

# Seznam obrázků



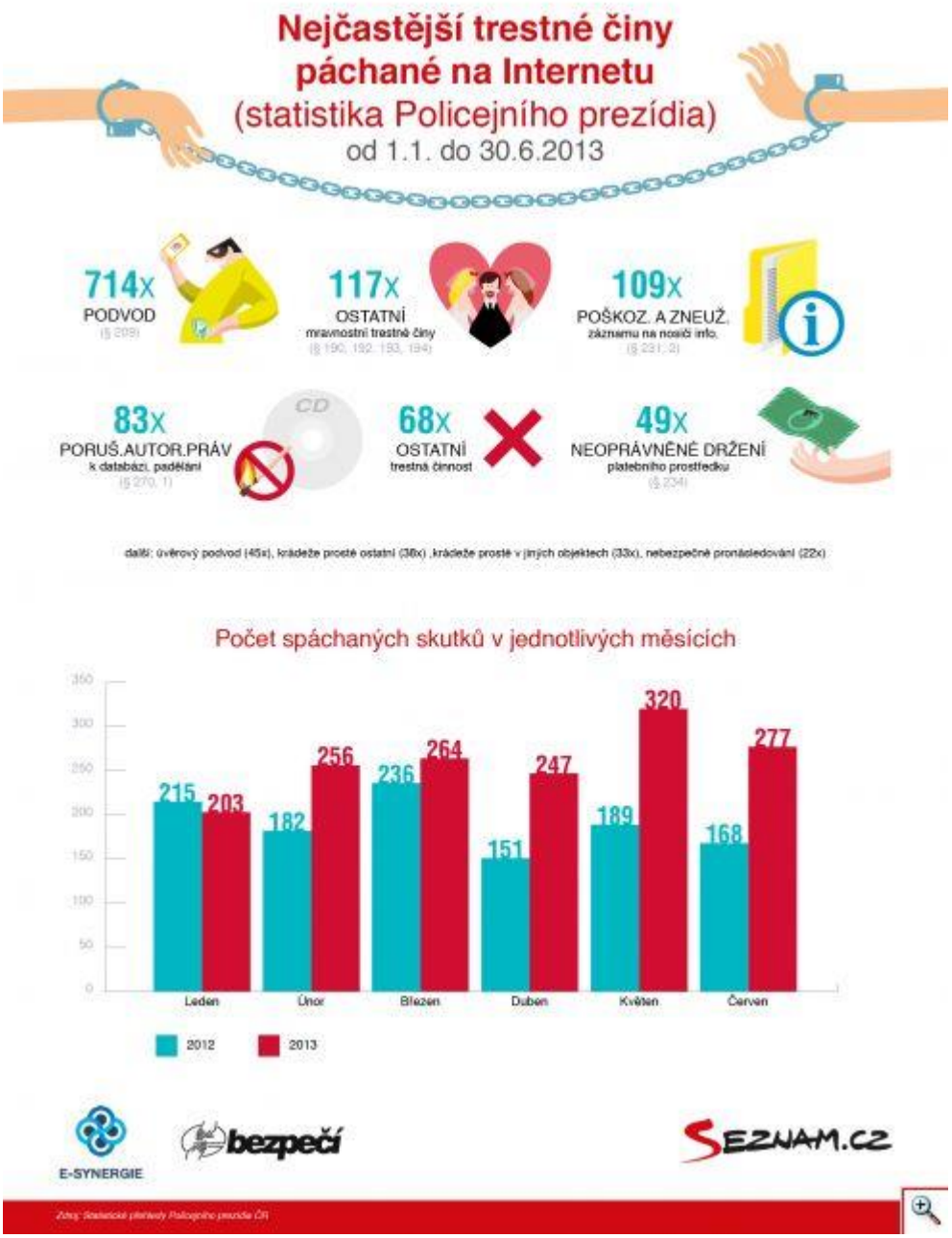
# Seznam tabulek



# Seznam příloh

# Přílohy

## Příloha č. 1 – Nejčastější trestné činy páchané na internetu.



**Příloha č. 2 – Statistiky PP k ICT kriminalitě včetně vybrané skupiny ZP 0-18 let.**

| Statistické údaje ICT kriminality v rámci České republiky za roky 2011-03/2014. | | | | |
|---|---|---|---|---|
| **Česká republika** | **2011** | **2012** | **2013** | **2014/1.-3. měsíc** |
| **ICT celkem** | 1540 | 2285 | 3278 | 1059 |
| 0-15 let | 6 | 4 | 8 | 0 |
| 15-18 let | 17 | 26 | 26 | 4 |
| **ICT majetková** | 1328 | 2015 | 2834 | 947 |
| 0-15 let | 5 | 4 | 6 | 0 |
| 15-18 let | 17 | 21 | 21 | 2 |
| **ICT V. hlava TZ** | 1041 | 1509 | 2382 | 786 |
| 0-15 let | 3 | 2 | 4 | 0 |
| 15-18 let | 13 | 17 | 17 | 2 |
| **Podvody §209 TZ** | **899** | **1282** | **1853** | **537** |
| 0-15 let | 1 | 1 | 1 | 0 |
| 15-18 let | **11** | **16** | **13** | **2** |

| Statistické údaje ICT kriminality v rámci Krajského ředitelství policie Olomouckého kraje (KROK) za roky 2011-03/2014. | | | | |
|---|---|---|---|---|
| **KROK** | **2011** | **2012** | **2013** | **2014/1.-3. měsíc** |
| **ICT celkem** | 143 | 176 | 178 | 89 |
| 0-15 let | 0 | 0 | 0 | 0 |
| 15-18 let | 0 | 2 | 3 | 0 |
| **ICT majetková** | 128 | 164 | 155 | 86 |
| 0-15 let | 0 | 0 | 0 | 0 |
| 15-18 let | 0 | 2 | 3 | 0 |
| **ICT V. hlava TZ** | 120 | 90 | 117 | 50 |
| 0-15 let | 0 | 0 | 0 | 0 |
| 15-18 let | 0 | 0 | 3 | 0 |
| **Podvody §209 TZ** | **117** | **80** | **90** | **30** |
| 0-15 let | 0 | 0 | 0 | 0 |
| 15-18 let | 0 | 0 | 2 | 0 |

**Příloha č. 3 – Úplné, aktuální znění skutkové podstaty trestného činu Podvod dle ust. § 209 Zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.**

*§ 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 nebo jiné majetkové hodnoty.*

*(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 trestného činu vlastizrady (§ 309), teroristického útoku (§ 311) nebo teroru (§ 312).*

*(6) Příprava je trestná.*

**Příloha č. 4 – Úplné, aktuální znění skutkové podstaty trestného činu Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle ust. § 231 Zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.**

*§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat*

*(1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává*

*a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo*

*b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,*

*bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo jiné majetkové hodnoty nebo zákazem činnosti.*

*(2) Odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán,*

*a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo*

*b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch.*

*(3) Odnětím svobody na šest měsíců až pět let bude pachatel potrestán, získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu.*

**Příloha č. 5 – Úplné, aktuální znění skutkové podstaty trestného činu Neoprávněný přístup k počítačovému systému a nosiči informací dle ust. § 230 Zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.**

*§ 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 jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.*

*(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 dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.*

*(3) Odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty 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.*

**Příloha č. 6 – Dotazník**

Dobrý den,

jmenuji se Martin Vyhlídal a jsem studentem Univerzity Palackého v Olomouci, Pedagogická fakulta, obor Učitelství praktického vyučování a odborného výcviku. Tento obor studuji kombinovanou formou.

Jelikož pracuji u Policie České republiky, kde jsem v poslední době registroval nárůst majetkové kriminality páchané na internetu, rozhodl jsem se bakalářskou práci zaměřit právě na tuto oblast.

Dovoluji si Vás tedy oslovit s žádostí o vyplnění níže obsaženého dotazníku, který je zcela anonymní a zabere Vám jen malou chvíli. Navíc údaje získané tímto dotazníkem jsou pro moji práci nezbytné.

Otázky v dotazníku jsou sice uzavřené, avšak Vaše názory a připomínky můžete vyjádřit v kolonce „poznámka“ u každé položky.

Velice Vám děkuji za spolupráci, vyplnění dotazníku a jeho brzké odeslání zpět formou odpovědi na tento email.

S pozdravem a přáním hezkého dne

Martin Vyhlídal

**DOTAZNÍK**

**Položka č. 1**

Objevil se na Vaší škole případ majetkové kriminality na internetu, kde v roli oběti nebo pachatele byl Váš žák/student? ANO/NE*

Vaše poznámka:

**Položka č. 2**

Existuje na Vaší škole preventivní program zaměřený přímo na problematiku majetkové kriminality na internetu? ANO/NE*

Vaše poznámka:

**Položka č. 3** (pouze v případě, že odpověď na položku č. 2 byla ANO)

Proběhla evaluace Vašeho preventivního programu zaměřeného na problematiku majetkové kriminality na internetu? ANO/NE*

Vaše poznámka:

*nehodící se vymažte

**Příloha č. 7 – Zaznamenané poznámky k dotazníku první úrovně průzkumu**

| Přiřazené číslo školy | Číslo dotazníkové položky | Zaznamenané poznámky |
|---|---|---|
| 17 | 1 | Má informovanost pochopitelně není 100%. Nicméně se žáky o těchto rizicích hovořím. |
| 17 | 2 | Bude mít ve škole přednášku a besedu k této tematice kpt. Bc. Pavel Schweiner (KROK), jinak průběžně po dobu celého školního roku informace a rozhovory. |
| 17 | 3 | Jako samostatnou kapitolu jsem ji zařadila v tomto školním roce. Jinak byla součástí bloku rizika kyberprostoru. |
| 4 | 3 | autorská práva a internet (beseda pro žáky 2. ročníku) |
| 18 | 1 | spíše by se hodila odpověď NEVÍM, žáci a studenti se nesvěřují ve škole se svými problémy na internetu. |
| 7 | 2 | Jednou ročně probíhá beseda s PČR, která je spíše obecná a účastní se jí studenti 2. ročníku |
| 8 | 2 | Program přímo nemáme, využíváme však náhodné nabídky jiných subjektů v dané problematice |
| 14 | 2 | Žáci 1. ročníku nižšího stupně gymnázia a studenti 1. ročníku vyššího stupně gymnázia se účastní besedy s UPOL. Prvořadá je pro nás bezpečnost dětí na internetu. |
| 22 | 2 | Máme preventivní programy, ale ty jsou zaměřeny pouze proti rasismu a drogám. |
| 24 | 2 | Program sice nemáme, ale danou problematiku řešíme okrajově v rámci finanční gramotnosti. |
| 33 | 2 | Danou problematiku řešíme okrajově v rámci předmětu ICT, kde probíráme bezpečný internet a také kyberšikanu. |
| 34 | 2 | Program nemáme, ale v případě potřeby bychom se obrátili na projekt e-Bezpečí. |

**Příloha č. 8 – Zaznamenané poznámky k dotazníku druhé úrovně průzkumu**

| Přiřazené číslo školy | Číslo dotazníkové položky | Zaznamenané poznámky |
|---|---|---|
| 12 | 1 | Setkali jsme se s kyberšikanou! |
| 35 | 2 | Minimální preventivní program máme zpracovaný, problematika majetkové kriminality na internetu tam však zapracovaná není. Zřejmě doplním. |
| 17 | 2 | Okrajově probírají danou problematiku v občanské nauce, minimální preventivní program mají zaměřený převážně na kyberšikanu. |

# Anotace

| | |
|---|---|
| **Jméno a příjmení:** | Martin Vyhlídal |
| **Katedra:** | Ústav pedagogiky a sociálních studií Pdf UP Olomouc |
| **Vedoucí práce:** | PhDr. René Szotkowski, Ph.D. |
| **Rok obhajoby:** | 2014 |
| **Název práce:** | MAJETKOVÁ KRIMINALITA NA INTERNETU |
| **Název v angličtině:** | THE PROPERTY CRIME ON THE INTERNET |
| **Anotace práce:** | Bakalářská práce pojednává obecně o problematice majetkové kriminality na internetu. Zdůrazňuje její nebezpečnost pro společnost v historických souvislostech a jejím hlavním cílem v teoretické části práce je popsat její trestně právní rovinu s důrazem na nejčastěji páchaný trestný čin, kterým je Podvod. Práce je zaměřena na primární prevenci této kriminality především na úrovni středoškolského vzdělávání a tedy na osoby mladistvé. Dílčím cílem praktické části práce je ověřit existenci preventivních programů zaměřených přímo na problematiku majetkové kriminality na internetu. |
| **Klíčová slova:** | Majetková kriminalita, Počítačová kriminalita, Informační a komunikační technologie, Internet, Mladiství, Prevence. |
| **Anotace v angličtině:** | Bachelor thesis deals generally about issues of property crime on the Internet. It emphasizes the danger to society in a historical context and its main objective in the theoretical part is to describe the criminal plane, with an emphasis on the most commonly perpetrated crime, which is a scam. The work is aimed at the primary prevention of this crime especially at the level of secondary education and thus to juveniles. A partial aim of the practical part of the work is to verify the existence of prevention programs focused directly on the issue of property crime on the Internet. |
| **Klíčová slova v angličtině:** | The property crime, Cyber crime, Information and communication technology, Internet, Juveniles, Prevention. |
| **Přílohy vázané v práci:** | • Nejčastější trestné činy páchané na internetu.<br>• Statistiky PP k ICT kriminalitě včetně vybrané skupiny ZP 0-18 let.<br>• Úplné, aktuální znění skutkové podstaty trestného činu Podvod dle ust. § 209 Zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.<br>• Úplné, aktuální znění skutkové podstaty trestného činu |

| | |
|---|---|
| | Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle ust. § 231 Zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.<br>• Úplné, aktuální znění skutkové podstaty trestného činu Neoprávněný přístup k počítačovému systému a nosiči informací dle ust. § 230 Zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.<br>• Dotazník<br>• Zaznamenané poznámky k dotazníku první úrovně průzkumu<br>• Zaznamenané poznámky k dotazníku druhé úrovně průzkumu |
| **Rozsah práce:** | 64 s. |
| **Jazyk práce:** | český |