VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

DŮVĚRYHODNOST INFORMACÍ NA INTERNETU VE VZTAHU K PREVENCI INTERNETOVÉ TRESTNÉ ČINNOSTI OBYVATELSTVA V ÚSTECKÉM KRAJI, OKRESE DĚČÍN

Autor práce: Pavel Bílek, DiS.

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: kombinovaná

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Právních oborů a bezpečnostních studií

2018

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v této práci.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna v souladu s § 47b zákona č. 111/1998 Sb. v platném znění.

.....

Děkuji vedoucímu bakalářské práce RNDr. Růženě Ferebauerové, za cenné rady, připomínky a metodické vedení práce. Dále bych chtěl poděkovat své rodině za trpělivost a podporu v době studia, zejména při zpracování bakalářské práce.

ABSTRAKT

BÍLEK, P. *Důvěryhodnost informací na internetu ve vztahu k prevenci internetové trestné činnosti obyvatelstva v Ústeckém kraji, okrese Děčín : bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, 2018. 72 s. Vedoucí bakalářské práce : RNDr. Růžena Ferebauerová.

Klíčová slova: důvěryhodnost, informace, internet, prevence kriminality, ověřování informací, zákonné normy

Bakalářská práce pojednává o důvěryhodnosti informací na internetu a jejím vztahu k prevenci počítačové kriminality. V první řadě analyzuje pojmy „důvěryhodnost“, „informace“, „internet“ a „prevence kriminality“.

Na základě této analýzy shrnuje poznatky o nedůvěryhodných informacích a uvádí nejznámější z nich. Dále analyzuje zákonné normy a protiprávní jednání, které se vztahuje k dané problematice.

V neposlední řadě shrnuje a analyzuje preventivní činnosti v oblasti počítačové kriminality prováděné na území České republiky, se kterými se může setkat běžný občan ve svém životě.

Ve své poslední části na základě provedeného dotazníkového šetření a řízeného rozhovoru s policistou zabývajícím se prevencí kriminality zkoumá, jak ovlivňují určité aspekty rozhodování o důvěryhodnosti informací získaných z internetu u osob z Ústeckého kraje okresu Děčín. Dále zkoumá realizaci prevence počítačové kriminality na uvedeném území ze strany státních organizací, škol a soukromých organizací.

ABSTRACT

BÍLEK, P. The Credibility of Information on the Internet in Relation to the Prevention of Criminal Internet Crime in the Ústí nad Labem Region, Děčín District : bachelor thesis. České Budějovice : University of European and Regional Studies, 2018. 72 p. Head of Bachelor Thesis: RNDr. Růžena Ferebauerová.

Key words: credibility, information, internet, crime prevention, information verification, legal standards

The bachelor thesis deals with the trustworthiness of information on the Internet and the relation to prevention of cybercrime. Firstly, it analyses the concepts of "credibility", "information", "internet" and "crime prevention".

Based on this analysis, it summarizes the findings of untrustworthy information and lists the best known ones. It further analyses the legal norms and the offenses related to the given issue.

Last but not least, it summarizes and analyses the preventive activities in the area of cybercrime carried out in the Czech Republic, which a common citizen can encounter in his life.

In the last part, based on a questionnaire survey and a controlled interview with a crime prevention policeman, the thesis examines how certain aspects influence the decision-making on the credibility of information obtained from the Internet belonging to people from Ústí nad Labem region, district of Děčín. It also investigates the implementation of cybercrime prevention on the mentioned above territory from the side of state organizations, schools and private organizations.

Obsah

Úvod

Bakalářská práce se zabývá problematikou důvěryhodnosti informací na internetu a jejím vztahem k prevenci kriminality. V době blízké vzniku internetu nebylo třeba tuto problematiku řešit. Bylo propojeno pouze několik počítačů známých univerzit a společností. Rychlý rozvoj technologií a možnost připojit se téměř kdekoli k internetové síti zapříčinili, že se tento problémem - důvěryhodnost informací a jednotlivých serverů – stává stále aktuálnějším.

Hlavním problémem je anonymita osob publikujících a vystupujících na internetu. Ta prospívá latentnosti protiprávních jednání. Sociální prevence kriminality působí na psychickou stránku jedinců. Je založena na zkušenostech osob, jejich schopnosti přijmout informace a využít tyto poznatky ve chvíli střetu s protiprávním jednáním. Tedy je efektivní jen u určitých osob. Oproti tomu je situační prevence spolehlivější, ovšem nedokáže reagovat tak rychle jako pachatelé protiprávních jednání. Dalším problémem je rychlost mizících dat v prostředí internetu. Tím je velmi ztížena možnost zjištění potřebných stop k odhalení počítače, z kterého byla informace zaslána, nemluvě o možnosti zjistit, kdo jí zaslal. V neposlední řadě se na latentnosti počítačové kriminality, tím i na možných preventivních opatřeních, podílí nepružnost zákona, policejního orgánu a justice.

Propojenost mezi důvěryhodností informací a prevencí kriminality je zřejmá. Pokud půjde o zcela důvěryhodnou informaci nelze jejím šířením spáchat žádný protiprávní čin. Problémem je, že žádná zpráva nemůže být zcela důvěryhodná, protože každá osoba má svůj subjektivní pohled na věc a tedy na důvěryhodnost.

O důvěryhodnosti informace nebylo publikováno mnoho a při zadání tohoto slovního spojení v internetovém prohlížeči zjistíme, že je pojem spojen spíše s preventivními videi a články. Oproti tomu se prevencí kriminality, jako takové, zabývá mnoho knih. Tyto jsou zaměřené na jednotlivé cílové skupiny nebo na širokou veřejnost. Prevencí počítačové kriminality se zabývá velmi málo tištěných knih, a proto je práce sepsána převážně z informací získaných z ověřených elektronických zdrojů. Obecnou prevencí se zabývá i interdisciplinární věda, kriminologie. Také je prioritou státních i nadnárodních organizací. V České republice je prevence kriminality zakotvena v zákoně a spadá pod činnost Ministerstva vnitra.

Autor si téma vybral, jelikož se domnívá, že je v současné době velmi aktuální vzhledem k vysokému nárůstu počítačové kriminality. Dále se domnívá, že by se měla zlepšit informovanost obyvatel a prevence v této oblasti. Práce by mohla přispět k pochopení celého problému a poukázat na jednotlivé nedostatky preventivních činností.

1 Cíl a metodika bakalářské práce

Hlavními cíli bakalářské práce je zjistit, zda je možné informace, získané z internetu, označit za důvěryhodné. Dále zkoumá faktory ovlivňující důvěryhodnost těchto informací, jako jsou zdroj, autor, obsah, vzhled pozadí, na kterém je podávána informace, věk, vzdělání osob přijímajících informaci a v neposlední řadě vztah důvěryhodnosti k prevenci kriminality. Vedlejšími cíli je zjištění, zda osoby pracující s informacemi, získanými z internetu, ověřují jejich pravdivost. Dále analyzuje rozsah preventivních aktivit v oblasti trestné činnosti páchané pomocí internetu v Ústeckém kraji na katastrálním území města Děčín. Navrhuje opatření na zlepšení prevence v dané oblasti.

Bakalářská práce se skládá z teoretické a praktické části. V teoretické části dochází k deskripci a charakteristice základní pojmů na základě odborné literatury z oblasti kriminologie, psychologie a informatiky. Konkrétně je teoretická část rozdělena do tří kapitol. V první z nich jsou analyzovány základní pojmy: „Internet“, „Informace“, „Důvěryhodnost“ a „Prevence kriminality“. Druhá kapitola se zabývá analýzou nedůvěryhodných informací na internetu. Bylo zjištěno, že důvěryhodnost je velmi subjektivní pojem a o žádné informaci nelze říci, že by byla důvěryhodná pro všechny osoby na světě. Třetí kapitola se zabývá důvěryhodností informací ve vztahu k bezpečnostně právnímu prostředí včetně prevence kriminality a jejích prostředků užívaných v České republice.

Praktická část byla realizována kvantitativně kvalitativní metodou. Samotný výzkum byl proveden kvantitativní metodou za pomoci anonymního dotazníkového šetření v České republice, Ústeckém kraji, okrese Děčín v katastru statutárního města Děčín a to v období ledna a února 2018. Město Děčín mělo k 1. 1. 2017 celkem 49 521 obyvatel, kdy předpokladem je, že na začátku roku 2018 bude mít podobný počet obyvatel (aktuální data nejsou dostupná). Jako referenční vzorek bude zvoleno 300 obyvatel (přibližně 0,6 %), kteří byly vybráni z žáků 2. stupně základních škol (věk 11 – 15 let), žáků středních škol (věk 15 – 19 let), studentů vysoké školy (věk 19 – 24 let), zaměstnanců větších firem (věk 19 – 65 let) a členů domovů důchodců a zájmových sdružení seniorů (věk nad 65 let). Věková skupina pod 11 let nebyla zastoupena, jelikož rozumová vyspělost těchto osob není dostatečná pro výzkum.

Tato metoda byla zvolena, jelikož je nejméně náročná na čas a je vstřícnější k respondentům, kdy jim poskytne dostatek času na rozmyšlení a anonymitu.

Nevýhodou je ovšem možnost přeskočení otázky, či její zodpovězení jiným člověkem nebo rodinným týmem. Hlavním problémem je špatná návratnost dotazníků. Tento byl řešen distribucí do prostorově koncentrované společnosti. Samotný dotazník (viz. Příloha I) obsahuje 12 otázek, které lze rozdělit do 3 skupin. V první skupině jsou zjišťovány informace o respondentovi, v druhé faktory ovlivňující důvěryhodnost informace a v třetí preventivní činnost na uvedeném území.

Kvantitativní metoda byla doplněna kvalitativní a to řízeným rozhovorem s policistkou zabývající se preventivní činností v rámci Policie ČR, Krajského ředitelství policie Ústeckého kraje, Územního odboru Děčín, Oddělení tisku a prevence, který byl zaměřen na zodpovězení obsahově stejných otázek jako distribuovaný dotazník.

Výzkum měl potvrdit či vyvrátit tyto předpoklady:

- Hypotéza I: Pro většinu osob je důvěryhodnost informace zaručena jejich autorem.
- Hypotéza II: Pro většinu osob je důvěryhodnost informace zaručena jejím obsahem.
- Hypotéza III: Méně jak 50 % osob získávajících informace z internetu nepovažuje za důležitý zdroj informace.
- Hypotéza IV: Pro více jak 50% osob není důležitý vzhled stránky při určování důvěryhodnosti podávané informace.
- Hypotéza V: Osoby mladší 15 let a starší 40 let více důvěřují informacím na internetu bez jejich ověření než ostatní.
- Hypotéza VI: Více jak 70% osob neověřuje pravdivost informací získaných z internetu.
- Hypotéza VII: Situační prevence je latentního charakteru a není většině osob známa.
- Hypotéza VIII: Preventivní činnost zaměřená na internetovou kriminalitu související s důvěryhodností informací není na katastrálním území města Děčín prováděna.

- Hypotéza IX: Nejznámějším protiprávním jednáním na internetu je SPAM.

- Hypotéza X: Méně jak 50% osob se stalo obětí protiprávního jednání na internetu. (Vyloučen SPAM, jelikož je zachytáván spamovými filtry, tedy osoby se stávají jeho oběťmi bez možnosti si to uvědomit)

- Hypotéza XI: Většina respondentů nezná pojem Netiketa.

Po získání údajů byla provedena jejich analýza a komparace (reálných hodnot a absolutních poměrů) společně s vyhodnocením pravdivosti předpokladů uvedených výše. Některé výsledky byly doplněny grafickým znázorněním pro jejich větší přehlednost.

2 Základní pojmy

Pro analýzu daného problému bylo třeba definovat a pochopit pojmy *internet, informace, důvěryhodnost a prevence kriminality*.

2.1 Internet

Co je to internet? Internet má mnoho definic, asi nejvýstižnější je definice z publikace „*Slovník počítačových pojmů a zkratek"*, z níž byly vybrány pouze části důležité pro tuto práci. Pro účely bakalářské práce došlo k jejich drobné úpravě:

„Internet je celosvětová počítačová síť, která sdružuje počítačové sítě. Jednotlivé sítě jsou na sobě nezávislé, ale používají společný soubor protokolů TCP/IP (Transmission Control Protocol/Internet Protocol). Provoz neřídí žádná organizace ani společnost. O dalším vývoji rozhoduje Internetová společnost (Internet Society, ISOC), která jmenuje Koordinační radu Internetu (Internet Advisory Board, IAB). Ta schvaluje standardy a způsob přidělování adres, doporučení publikuje jako RFC (Requests for Comments). Využívání služeb internetu je možné prostřednictvím různých programů.

Internet umožňuje obrovskému počtu lidí přístup k ohromnému množství informací, ať již uložených v rozsáhlých databázích nebo poskytovaných ochotnými uživateli zdarma prostřednictvím konferencí a stránek WWW. Bezpečnost přenášených dat si však musí zajistit uživatel sám.

Šéfredaktor Softwarových novin v roce 1995 výstižně napsal: „Internet je španělská hospoda velikosti zeměkoule: najdete v něm jen to, co tam jeho účastníci přinesou. Fakta i domněnky, pocitově míněné argumenty i demagogii, hledání souhlasu i indoktrinaci."[1]

Pokud pomineme technické záležitosti, pak lze definovat internet jako „nový svět", ve kterém kdokoli může být kýmkoli, sdílet, publikovat a získávat informace, které jsou pravdivé i nepravdivé a v neposlední řadě zde může prožít i „celý" svůj život.

[1]VORÁČEK, R. *Slovník počítačových pojmů a zkratek.* Praha: nakladatelství Fortuna, 1998. str. 66.

Ve většině publikací, které pojednávají o vzniku internetu a to byť i jen okrajově se dozvíme, že počátky internetu přicházejí s organizací ARPA (Advanced Research Projects Agency). V té době se jednalo o tzv. ARPAnet. Ovšem pokud se na problematiku podíváme hlouběji a v souvislostech doby, můžeme o prapočátku internetu hovořit již se vznikem dálnopisů a telegrafů, které tvořili prapůvodce sítí. Je pravdou, že neefektivní, pomalou, nákladnou síť s lidským prvkem, ale přenášející přesné informace v podobě blízké binárnímu kódu. S vynálezem počítače došlo k revoluci v přenosu a zpracování dat, postupně byly čárky a tečky Morseovy abecedy nahrazeny symboly 0 a 1. Na počátku došlo k pokusům o vývoj sítí a jejich prvků nejen ze strany USA (United States of America), ale i SSSR (Svaz sovětských socialistických republik), dále pilotních projektů vědeckých akademií a vysokých škol. Tyto nebyly z různých důvodů realizovány. USA ovšem vynaložilo největší náklady na výzkum a vývoj v této oblasti a uspělo.

Podnětem k vzniku samotné organizace ARPA byl start sovětského Sputniku 1, který proběhl dne 4. října 1957, tedy v době tzv. „studené války“ mezi USA a SSSR. USA tedy zahájilo „protiútok“ mobilizací všech dostupných sil vědy a byla založena organizace ARPA, která dostala za úkol dohlížet nad všemi americkými vesmírnými programy a strategickými raketovými výzkumnými projekty. Vesmírné projekty byly v té době výhradně vojenské povahy.

V tuto chvíli „také došlo k poznatku, že nadregionální výměna informací by mohla mít význam nejen pro zvýšení schopnosti obrany, ale že nabízí i možnost spojit vzájemně počítače ve vědeckých zařízeních celé země, aby bylo možné využívat existující zdroje bez jakýchkoliv hranic.“[2]

V duchu tohoto poznatku začala organizace ARPA vyhledávat nápady a technologie na univerzitách a výzkumných institutech. Roku 1958 vešel v platnost zákon o založení NASA (National Aeronautics nad Space Administration), který hlavní úkoly týkající se vesmírných a raketových projektů přisoudil právě NASA. Společnost ARPA se tedy začala zabývat základním výzkumem a spolupracovat s univerzitami a výzkumnými zařízeními, kdy se nakonec stala elitním zařízením v Scientific Community. Roku 1962 byla v ARPA vyvinuta koncepce „intergalaktické počítačové sítě“, kdy její architektura byla blízká současnému internetu. Roku 1965 se podařilo

[2]NAUMANN, F. *Dějiny informatiky, Od abaku k internetu*. Praha: nakladatelství Academia, 2009, str. 348.

poprvé spojit dva počítače na větší vzdálenost, univerzitní a vojenský, kdy nebyly ještě přenášeny soubory, ale jen zprávy. Tím vznikl tzv. „ARPAnet“, prazáklad internetu. Roku 1969 byla v rámci ARPAnet propojena nejdůležitější centra vojenského výzkumu v USA, tedy University of California v Los Angeles, Stanford Research Institute v Menlo Park, University of California v Santa Barbara a University of Utah v Salt Lake City. Toto propojení využívalo již blízkou strukturu i způsob přenosu informací nynějšímu internetu. Tedy počítače určené jako uzlové (tzv. „servery“), přenos rozdělených dat tzv. „paketů“ po více než jedné cestě apod. Nicméně v této době ještě neexistovalo vlastní vedení pro komunikaci počítačů, ale byly využívány již existující telefonní linky. Od zahájení oficiálního provozu ARPAnet v dubnu roku 1970 došlo k jeho rozšíření na důležitá centra po celé USA. V této době byly na ARPAnetu dostupné pouze dvě služby a to TELNET (TELetype NETwork - možnost ovládání jiného počítače po síti) a FTP (File Transfer Protokol – přenos dat jakéhokoliv druhu). Postupem času vznikl komunikační protokol, pro nějž se vžilo označení TCP/IP a stejně se vžil i pojem „internet“ pro sadu sítí. ARPAnet byl ovšem určen pro vojenský výzkum a nebyl volně přístupný veřejnosti a proto se v roce 1979, sedm velkých univerzit rozhodlo založit vlastní síť, CSnet (Computer Science Network). Do této měli možnost přístupu i jiní uživatelé. V této době byly zaznamenány první případy tzv. „Hackingu“ zejména vojenských informací. Proto se v roce 1983 z ARPAnet vyčlenila čistě vojenská síť tzv. „MILNet“ (Military Network). Po vzoru ARPAnet byly vytvářeny i v jiných zemích sítě sloužící ke komunikaci s předpokladem mezinárodního spojení. Postupem času a s rozvojem technologií došlo k propojení těchto sítí do dnešní podoby internetu. Ironií je, že roku 1990 byla síť ARPAnet pozastavena a její služby byly přebrány ostatními. Dále probíhal vývoj mnoha služeb poskytovaných na internetu, kdy nejdůležitější pro tuto práci je služba WWW (World Wide Web) a také služba electronic mailing. Electronic mailing zajišťuje přímou komunikaci uživatelů a zasílání e-mailů. Oproti tomu WWW je službou, která je schopna navádět uživatelský počítač od jednoho dokumentu k druhému bez zvláštních příkazových struktur, kdy tyto dokumenty byť i ze vzdálených serverů jsou čitelné v počítači uživatele za pomoci programu tzv. „browseru“ neboli prohlížeče. Od roku 1992 je WWW, včetně zdrojového kódu, dostupné široké veřejnosti a dochází k rychlému rozvoji, kdy od roku 1995 je hlavní a nejdůležitější službou internetu.[3]

[3]NAUMANN, F. *Dějiny informatiky, Od abaku k internetu.* Praha: nakladatelství Academia, 2009 str. 345 – 365 – podkapitola 2.1.2 volně parafrázována.

Jak bylo uvedeno výše, internet je plný informací ať již pravdivých či nepravdivých, které vkládají uživatelé s různými úmysly. Z tohoto hlediska se dá internet rozdělit na část internetu, kterou zná každá osoba a je běžně dostupná. A dále na část, která je dostupná obtížnějším způsobem (speciální prohlížeč apod.). Tyto informace se nedají označit za legální a ve spoustě případů ani za důvěryhodné, jelikož je nelze ověřit dostupnými prostředky. Navíc zde existuje i tzv. „černý trh“, jehož důvěryhodnost se liší uživatel od uživatele a nemáte možnost následné reklamace či jiného opravného prostředku. Tato část se nazývá „Darknet“. Vzhledem k omezeným možnostem přístupu uživatele se práce dále zabývá jen běžně přístupnou částí internetu.[4]

2.2 Informace

Co je to informace? Co si představit pod slovem *informace*? V dostupné literatuře je mnoho definic z různých hledisek, ovšem nejvhodnější je definice týkající se informačních technologií. S touto jsou úzce spjaty pojmy *data* a *znalost*, jejichž obsah je třeba pochopit a odlišovat je od sebe navzájem.

„Data jsou vyjádření skutečností formálním způsobem tak, aby je bylo možné přenášet nebo zpracovat.“[5]

„Informací nazýváme abstraktní veličinu, která může být přechovávána v určitých objektech, předávána určitými objekty, zpracovávána v určitých objektech a použita k řízení určitých objektů. Jako objekt přitom chápeme živé organismy, technická zařízení nebo soustavy těchto prvků.“[6]

„Informace je jev a proces, který vzniká nezávisle na nás a který zachycujeme nevědomě i vědomě. […] Informace nemá hodnotu, je hodnotově neutrální. Hodnotu jí přisuzuje teprve člověk v procesu poznání. […] Zpracování informace je proces porovnávání informací s osobnostním fondem (endoceptem), který jsme si dosud v průběhu života vytvořili, tj. s našimi dosavadními znalostmi, zkušenostmi, příběhy,

[4]CHIP: Magazín o digitálních technologiích. Německá spolková republika: CHIP Holding, G.m.b.H. vydavatelství Burda Praha, spol. s r.o., 2016, 11/2016, str. 61-64.
[5]FARANA, R. *Teorie informace – podklady pro výuku* [online], [cit. 2017-11-11]. Dostupné z WWW: <www1.osu.cz/~farana1/KodovaniKomprese/01TeorieInformace.ppt>.
[6]FARANA, R. *Teorie informace – podklady pro výuku* [online], [cit. 2017-11-11]. Dostupné z WWW: <www1.osu.cz/~farana1/KodovaniKomprese/01TeorieInformace.ppt>.

které se vryly do naší paměti, a prožitky. Výsledkem zpracování informace je znalost, která může zase ovlivnit náš osobnostní fond (endocept), restrukturalizovat či obohatit ho apod.“[7]

Znalosti „představují zobecněné poznání reality. Na rozdíl od dat, která zobrazují realitu na úrovni detailů a rychle se mění – tak, jak se mění detaily stavů objektů a procesů kolem nás, jsou znalosti relativně stálejší, protože představují vyšší stupeň abstrakce, zobecnění procesů a stavů objektů v realitě. Znalosti souvisejí s vymezováním pojmů, s kategorizací, s definováním, s odvozováním závěrů z dostupných faktů na základě abstraktních schémat a s vymezováním mechanismů odvozování závěrů.“[8]

„Vzájemnou souvislost a podmíněnost dat, informací a znalostí dobře vyjádřili Checkland a Scholes: Technologie pracují s daty, lidé je interpretují jako informace nesoucí význam, které se stávají podnětem pro další jednání. Proces interpretace je kognitivní záležitost, ve které stěžejní roli hrají znalosti.“[9]

2.2.1 Jak ověřit informace?

V dnešní době jsme díky volnému přístupu k sociálním sítím obklopeni množstvím informací, které jsme schopni okamžitě šířit dál. Dokumenty na internetu rychle vznikají a zanikají, proto se také může jednoduše stát, že narazíme na informace, které nejsou pravdivé. Ne vždy se jedná o záměrné šíření lží, ale může dojít jen ke špatné interpretaci události. Setkáváme se rovněž s cíleným šířením dezinformací či tzv. hoaxů, které mohou mít různou podobu (video, psaný text, fotografie, apod.). Ať už je záměr autora pro jejich šíření jakýkoliv, nesmíme věřit všemu, co čteme na sociálních sítích a pravdivost informací si musíme ověřovat. Zvláště pokud chceme předcházet negativním důsledkům, které může mít šíření poplašných zpráv či manipulace s veřejným míněním.

Poté co získáme informaci, je třeba při ověřování její pravdivosti odpovědět zejména na tyto otázky:

---

[7]CEJPEK, J. *Informace, komunikace a myšlení.* Praha: Univerzita Karlova v Praze, nakladatelství Karolinum, 2005, str. 23.
[8]INFORMATIKA UČEBNÍ TEXT PDF. *Představujeme Vám pohodlné a bezplatné nástroje pro publikování a sdílení informací.* [online]. Copyright © DocPlayer.cz [cit. 2018-01-11]. Dostupné z WWW: <http://docplayer.cz/848837-Informatika-ucebni-texty-2006.html>.
[9]SKLENÁK, V. *Data, informace, znalosti a internet*. Praha: C. H. Beck, 2001, str. 124.

I. Co je obsahem tvrzení?

Zde je potřeba zapojit zdravý rozum a kritické myšlení. Je třeba zhodnotit obsah, a pokud nejsme schopni vlastními znalostmi potvrdit pravdivost či jí vyvrátit, pak je možné pomocí klíčových slov vyhledávat informace, které nám pomohou v rozhodování. Neplatí ovšem, že na čím více místech obsah nalezneme, tím je pravdivější. Spousty serverů informace jen přebírá a neověřuje. Dále lze obsah ověřit na serverech zabývajících se šířením nepravdivých informací např.: www.Hoax.cz, www.manipulatori.cz a další.

II. Kdo sdílel tvrzení?

Je nám sdílející osoba či server známý? Získáváme od něj informace poprvé? Víme, že informace ověřuje nebo je jen přebírá? Pokud jsme již jednou přišli na to, že osoba sdílející tvrzení jen kopíruje, pak bychom neměli slepě věřit tomu, co sdílí.

III. Kdo je zdrojem tvrzení?

Ve své podstatě zde platí stejné věci jako u bodu II. Za pravdivé zdroje lze považovat vládní stránky s dokumenty či stránky univerzit, vědeckých ústavů apod. Zde je předpoklad, že šíření nepravdivých informací těmito institucemi by byly nežádoucí. Policie ČR (Policie České republiky) jako spolehlivé zdroje využívá centrální databáze (osob, vozidel apod.). Pro běžného občana lze za důvěryhodný zdroj považovat například Katastr nemovitostí a další. Servery, které podávají pravdivé informace, obvykle uvádějí jejich autora. Je tedy možno přímo tohoto autora kontaktovat a vznést na něj dotaz ohledně skutečností uvedených v tvrzení.

IV. Kde byl obsah vytvořen?

„Pokud autor přiložil k danému tvrzení fotografie nebo video za účelem podpory tvrzení, je žádoucí všímat si detailů, které by mohly prozradit, kde byl tento materiál pořízen a následně i to, zda je relevantní. Takovým znakem může být název ulice, policejní sirény, dialekt, nápisy kolem, apod. Všechny tyto detaily pomáhají dohledat místo pořízení dat. Youtube a některé video přehrávače umožňují zpomalit záběr, aby bylo možné zachytit tyto detaily. K ověření lokace slouží aplikace Wikimap (online

mapa), satelitní snímky na Google Earth a Panoramio (přístupné i z Google Earth), jež by se měly shodovat.“[10]

V. Kdy byl obsah vytvořen?

Při ověřování lze zjistit, že obsah byl pravdivý, ale nyní již není relevantní, jelikož se změnili zákony či jiné věci. Je třeba sledovat, kdy byl článek vytvořen a tedy jestli je ještě aktuální. Nebo je možné z dat, které jsou v článku uváděny zjistit, že tvrzení se nezakládá na pravdě. Dle data lze určit například přes server www.wolframalpha.com počasí v daném místě nebo jiné skutečnosti. Tedy další informace, které mohou potvrdit či vyvrátit pravdivost tvrzení.

VI. Za jakým účelem určité tvrzení vzniklo a je šířeno?

Je tvrzení šířeno za účelem rozšíření nějakého faktu nebo se jedná o už od začátku smyšlenou věc např.: sci-fi povídku? Tyto informace mohou být zjištěny z obsahu, zapsány na konci či začátku tvrzení nebo je v neposlední řadě můžeme získat přímo od autora či šiřitele. Pokud ani jedna z těchto možností není, pak se můžeme obracet na již výše uvedené servery týkající se hoaxů, dezinformací apod.

2.3 Důvěryhodnost

Co si představit pod pojmem důvěryhodnost? Důvěryhodnost je abstraktní věc, tedy jí nelze popsat žádnými hmatatelnými vlastnostmi, žádnými daty. Je subjektivní, kdy každý z nás může za důvěryhodné považovat něco jiného, vzhledem ke svým zkušenostem a vlastnostem. Z hlediska jazykovědného se jedná o vlastnost, ať již osoby, věci či informace. Slovo „důvěryhodnost“ je odvozeno od slova „důvěryhodný“, tedy hodný důvěry. Slovník uvádí význam slova „hodný“ (v tomto kontextu) jako „takový, který si něco zasluhuje“ a slova „důvěra“ jako „ochota věřit něčemu“[11]. Tedy po spojení těchto významů lze důvěryhodnost definovat jako vlastnost objektu, která mu přisuzuje zásluhu v něj věřit. Například u informace v její pravdivost.

[10]KREJČÍ, M. *Odborný podklad think-tanku Evropské hodnoty, Fact checking manuál* [online], 22. 10. 2016, [cit. 2018-01-12]. Dostupné z WWW: <http://www.evropskehodnoty.cz/vyzkum/fact-checking-manual/> - je i zdrojem pro oddíl 2.2.1.
[11]LINGEA s r.o. nechybujte.cz, správně česky. Pojem důvěra, hodný, [online], [cit. 2017-12-27]. Dostupné z WWW: <http://www.nechybujte.cz/slovnik-soucasne-cestiny>.

2.3.1 Rozhodování o tom co je důvěryhodné.

Důvěryhodnost je subjektivní vlastnost, jak tedy můžeme určit co je obecně důvěryhodné a co ne? Každý z nás je jiný, někteří lidé slepě důvěřují všemu, jiní zase nedůvěřují ničemu a je mnoho těch, kteří váhají. Rozhodnutí čemu chceme věřit a čemu ne je na každém z nás. Stejně tak je to s důvěryhodností. Při rozhodování bychom neměli zapomínat na zdravý rozum, kritické myšlení a vlastní zkušenosti. Tento rozhodovací proces by měl být blízký procesu ověřování informací. Můžeme důvěřovat tomu co nám okolí tvrdí, ale měli bychom se držet známého rčení „Důvěřuj, ale prověřuj.“. Konečné rozhodnutí čemu nebo komu dáme nálepku „důvěryhodný“ je ovšem na každém z nás.

Z nemalé míry dochází k posuzování důvěryhodnosti stránek na internetu podle jejich vzhledu. Platí zde „ustálené pravidlo“, že čím lépe je stránka graficky zpracována, tím je důvěryhodnější pro veřejnost. Vzhled stránky by neměl být kritériem při hodnocení důvěryhodnosti. Mnoho stránek je vytvořeno graficky na vysoké úrovni, ovšem jejich obsah je zcela nesmyslný.

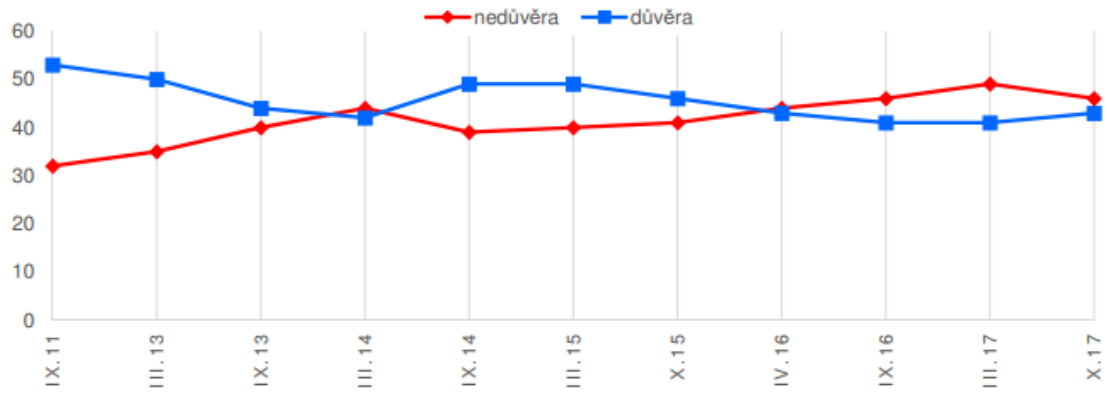
Lidé častokrát považují za důvěryhodné jakékoli informace, které uvede známá osobnost či osoba odborníka. I tyto informace je třeba podrobit kritickému myšlení, jelikož nikdo nezaručí pravdivost informace. Většina lidí za tento akt dostane zaplaceno nebo se jím chce pouze zviditelnit. Vysloví tedy předložený text a o daný problém se nezajímají. Na tomto principu je založeno mnoho reklam, které tvrdí, že výrobek jedné značky je lepší než jiný a podobně.

K tomuto se vztahuje i tvrzení, že „zvyšuje-li se množství podnětů z vnějšího světa v podobě informací, neznamená to vždy automaticky, že jsme znalejší, vzdělanější, že náš osobnostní fond je bohatší. Pro takovéto obohacení našeho osobnostního fondu není rozhodující množství informací, které máme k dispozici, ale jejich osvojení, tj. zpracování informací na poznatky a znalosti.“[12] Toto potvrzuje, že každá osoba má individuální zkušenosti a znalosti i když žije ve stejném prostředí. Na základě nich posuzuje důvěryhodnost a pravdivost informace.

Následující graf ukazuje důvěru a nedůvěru lidí v internet. Je vidět, že v roce 2011, internetu důvěřovalo přes 50 % dotazovaných. Od této doby došlo k poklesu důvěry pod hranici 50 % a má klesající tendenci, kdežto nedůvěra v internet spíše roste.

[12] CEJPEK, J. *Informace, komunikace a myšlení.* Praha: Univerzita Karlova v Praze, nakladatelství Karolinum, 2005, str. 20.

Graf 1: Důvěra/nedůvěra v internet (časové srovnání v procentech)[13]



Názorem autora je, že je internet v této době již přesycen informacemi, které jsou pochybného původu. Lidé získaná data nechtějí ověřovat, a proto je raději považují za nedůvěryhodné. Také často dochází k situacím, kdy sledujete několik zdrojů vypovídajících o jedné události (internet, televize, noviny apod.) a každý z nich situaci popisuje jinak. Člověk si často nemá možnost ověřit podávanou informaci, tedy dojde k závěru, že ani jeden ze zdrojů není důvěryhodným.

2.3.2 Záruka důvěryhodnosti?

Je mnoho lidí, kteří věří v Boha, je jedno v kterého. Pro většinu věřících je garantem informací které dostávají ohledně víry, způsobu, jakým by měli žít a podobně. Právě Bůh, promlouvající prostřednictvím proroků nebo psaných pramenů (Bible, Korán). Poté jsou lidé, kteří věří v Boha, ale nevěří v proroky a psané prameny. Také nalezneme osoby nevěřící. Pro každou z těchto skupin je důvěryhodnost informací o Bohu jiná. Jedni jej mají za garanta důvěryhodnosti všech informací, druzí jen části a pro další není Bůh vůbec garantem. Ze zde uvedeného příkladu je vidět, že zaručit důvěryhodnost informací pro všechny lidi nelze. I přes skutečnost, že budete podávat informaci pravdivou, která je mnohokráte ověřena a nelze jí vyvrátit, najde se na světě člověk, který jí nebude věřit a bude jí popírat, tedy pro něj bude nedůvěryhodná. Důvěryhodnost je tedy zcela relativním pojmem.

Existují takové informace a zdroje, které jsou všeobecně považovány za důvěryhodné. Takovými informacemi jsou například osobní fotografie, otisky prstů.

[13] TUČEK, M., CENTRUM PRO VÝZKUM VEŘEJNÉHO MÍNĚNÍ, Sociologický ústav AV CR, v.v.i. Důvěra k vybraným institucím veřejného života – říjen 2017, [online], Naše společnost 27. 11. 2017, [cit. 2018-03-01]. Dostupné z WWW: <https://cvvm.soc.cas.cz/cz/tiskove-zpravy/politicke/politicke-ostatni/4464-duvera-k-vybranym-institucim-verejneho-zivota-rijen-2017>.

U zdrojů lze například hovořit o databázích osob, vozidel, katastru nemovitostí. Tyto informace nejsou vždy jednoznačné. U fotografií osoby lze mít dvě stejné fotografie různých lidí, dvojčat. U otisků lze najít ve velmi výjimečných případech dva stejné otisky prstů různých lidí. Databáze plní daty lidé, kteří nejsou neomylní, tedy dochází k neúmyslnému předání mylných informací.

2.4 Prevence kriminality

Při zkoumání tohoto pojmu vynaložil, autor knihy „Prevence kriminality“, docent Svatoš nemalé úsilí ke sběru všech definic dostupných v běžné literatuře. Z těchto byla vybrána pro autora nejvýstižnější definice, která tvrdí, že „prevence kriminality, neboli také kriminální profylaxe, představuje pokus eliminovat trestnou činnost ještě před jejím započetím nebo před jejím pokračováním. Do prevence kriminality tak náležejí – v našem pojetí – veškeré aktivity směřující k předcházení páchání trestných činů, k snižování jejich výskytu cestou zamezená páchání neboli k neutralizaci příčin a podmínek vzniku trestných činů (kriminogenních faktorů). Patří sem opatření, jejichž cílem je zmenšování rozsahu a závažnosti kriminality, ať již prostřednictvím omezení kriminogenních příležitostí nebo působením na potenciální pachatele a oběti trestných činů.“[14]

Zapletal, Novotný a kol.[15] uvádí dělení prevence kriminality v obecnější formě než Svatoš[16], kdy se shodují v obsahu i v jednotlivém dělení. Tohoto členění užívá i ministerstvo vnitra.

Kriminální prevence se tedy člení

- podle obsahového zaměření na:
    - sociální prevenci - zaměřenou na sociální faktory kriminality, které jsou významné také pro náležitou socializaci člověka. Hlavně aktivity ovlivňující proces socializace a sociální integrace. Dále aktivity zaměřené na změnu nepříznivých společenských a ekonomických podmínek. Je součástí sociální politiky státu

[14] SVATOŠ, R., *Prevence kriminality*, VŠERS o.p.s., 2014, s. 14.
[15] NOVOTNÝ, O., ZAPLETAL, J., a kol. *Kriminologie*, Praha: ASPI Publishing, 2004 s. 173-191.
[16] SVATOŠ, R., *Prevence kriminality*, VŠERS o.p.s., 2014, s. 16 – 17.

- situační prevenci - zaměřenou na kriminogenní situace, tj. hlavně na zmenšování příležitostí k páchání trestných činů. Je založena na zkušenosti, že určité druhy kriminality se objevují v určité době na určitých místech a za určitých okolností. Dle slov docenta Svatoše je úspěšnost vysoká, ovšem vyžaduje adekvátní volbu opatření, finanční a personální prostředky. Odpovědnost za situační prevenci nesou hlavně občané a obce, dále v rámci vymezených kompetencí Ministerstvo Vnitra respektive Policie České republiky.

- prevenci viktimnosti a pomoc obětem trestných činů – je založena na konceptech bezpečného chování, diferencovaného s ohledem na různé kriminální situace a na psychickou připravenost ohrožených osob. V praxi se jedná o skupinové i individuální zdravotní, psychologické a právní poradenství, trénink v obranných strategiích a propagaci technických možností ochrany před trestnou činností

- podle adresátů preventivních aktivit na:

  - primární prevenci - adresátem je celá společnost či veškeré obyvatelstvo některého města či místa nebo některá demograficky vymezená skupina lidí např. mládež, ženy apod., zahrnuje především výchovné, vzdělávací, volnočasové, osvětové a poradenské aktivity. Hlavními institucemi v této oblasti jsou rodina, škola a lokální společenství.

  - sekundární prevenci - orientovanou na rizikové skupiny potencionálních pachatelů nebo potencionálních obětí a na kriminogenní situace

  - terciární prevenci – orientovanou na resocializaci osob a prevenci recidivy, tj. pracovní uplatnění vč. rekvalifikace, sociální a rodinné poradenství, pomoc při získání bydlení apod.

3 Nedůvěryhodné informace na internetu

Důvěryhodnost tedy neznamená pravdivost informace a je subjektivním pojmem. Proto se tato kapitola zabývá informacemi, které by člověk za důvěryhodné neměl považovat nikdy. Jedná se o informace, které mohou být vytvořeny již úmyslně jako nepravdivé nebo být změněny v průběhu přenosu k příjemci.

3.1 Informace nepravdivé již od svého zdroje

Tyto informace jsou vytvořeny s různými úmysly autora. Některé pro zábavu, jiné pro zmatení lidí, další jako podvodné jednání. Ovšem jsou zde i informace, které autor převzal z nepravdivého zdroje a poté je interpretuje jako pravdivé, bez jakéhokoli záměru. Nejčastějšími případy jsou:

HOAX

„Anglické slovo HOAX [:houks:] v překladu znamená: falešnou zprávu, mystifikaci, novinářskou kachnu, podvod, poplašnou zprávu, výmysl, žert, kanadský žertík. V počítačovém světě slovem HOAX nejčastěji označujeme poplašnou zprávu, která varuje před neexistujícím nebezpečným virem.

Jak HOAX poznáme? Typický text poplašné zprávy obsahuje většinou tyto body:

I. Popis nebezpečí (viru)

Smyšlené nebezpečí (vir) bývá stručně popsané, v případě viru bývá uváděný i způsob šíření.

II. Ničivé účinky viru

Zde záleží převážně na autorově fantazii. Ničivé účinky mohou být celkem obyčejné, třeba zformátování disku nebo už míň důvěryhodné - zběsilý útěk myši do ledničky, roztočení HDD opačným směrem, výbuch počítače. Autoři hororů zde mohou hledat inspiraci.

III. Důvěryhodné zdroje varují

Ve většině případů se pisatel poplašné zprávy snaží přesvědčit, že varování přišlo od důvěryhodných zdrojů ("IBM a FBI varují" nebo "Microsoft upozorňuje" atd.)

IV. Výzva k dalšímu rozeslání

Tento bod HOAX vždy obsahuje! Mnoho nezkušených uživatelů se nechá zprávou napálit a bez přemýšlení výzvu uposlechnou. Právě proto se tyto nesmysly lavinovitě šíří.

Jako hoax můžeme také označit šířenou zprávu, která obsahuje nepřesné, zkreslující informace, účelově upravené polopravdy nebo směsku polopravd a lží.

V praxi můžeme použít následující pravidlo:

Jestliže zpráva obsahuje výzvu k hromadnému rozeslání na další adresy, je to podezřelé a s největší pravděpodobností HOAX. Občas to také může být původně opravdová prosba o pomoc, ale i ty svého největšího šíření dosáhnou v době, kdy jsou již neaktuální.“[17]

Dezinformace

Je definována jako „Záměrně nepravdivá (falešná, lživá, nesprávná, zkreslená) informace sdělovaná s cílem uvést v omyl a ovlivnit příjemce tím, že ji bude považovat za pravdivou a důvěryhodnou. Rozlišují se dezinformace pasivní (zatajení, zadržení, zpoždění informace) a aktivní (tvorba nepravdivé informace, modifikace původní informace či jejího kontextu).“[18] V poslední době se objevují v souvislosti s ruskou propagandou a vlnou uprchlíků přicházejících do států Evropské unie.

Podvodná jednání

„S rozvojem internetových a elektronických služeb vymýšlejí podvodníci stále nové triky, jak vylákat z neopatrných uživatelů peníze. Někdy jsou to falešné nabídky neexistujícího zboží v internetových aukcích, podvodné inzeráty na prodej levného automobilu nebo pronájem bytů. Podvodníci se neštítí zneužívat různá neštěstí nebo přírodní katastrofy k nachytání dalších obětí.

Některé podvody bývají v principu jednoduše provedeny, ale velmi často bývají propracovány i do drobných detailů, jako jsou profesionálně vytvořeny webové stránky

[17]DŽUBÁK, Josef & HOAX.cz. Co je to hoax, Co je to phishing, Co je to SCAM-419, Co jsou to podvodné loterie [online], ©2000-2017, [cit. 2018-01-16]. Dostupné z WWW: <http://hoax.cz/cze/>.
[18]KUČEROVÁ, H. *Dezinformace.* In: KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV) [online]. Praha : Národní knihovna ČR, 2003- [cit. 2018-01-17]. Dostupné z WWW: <http://aleph.nkp.cz/F/?func=direct&doc_number =000000095&local_base=KTD>.

neexistujících společností a bankovních institucí. Obětem bývají zasílány i podvržené falešné dokumenty a certifikáty.“[19]

Nejznámějšími podvodnými praktikami jsou Phishing, podvodné loterie a SCAM419, tyto budou popsány v podkapitole 4.2.

Cílená manipulace

„Manipulace je pokusem ovládnout, zavázat, zneužívat nebo využívat jiné lidi pomocí nečestných prostředků. Nejistí lidé ji používají k tomu, aby lépe vypadali v očích druhých. Lidé pyšní a takoví, kteří trpí pocitem, že se jim stále něco nedaří, ji používají k tomu, aby ovládali druhé nebo aby dosáhli svého, zatímco moci chtiví se jí chápou, aby se vyšvihli nahoru. Nedočkaví používají často manipulace, protože si myslí, že výsledky jsou důležitější než lidé, které nechají podél cesty. Manipulace může být zjevná nebo skrytá - taková, která používá nenápadně utroušených poznámek, předem promyšlených výrazů obličeje a pečlivého plánování. Pro někoho je to zakořeněný podvědomý zvyk, zatímco jiní se k ní uchylují jen v tísni.“[20]

Při cílené manipulaci dochází k šíření nepravdivých či upravených informací s cílem působit na myšlení a uvažování skupiny osob nebo jednotlivce, tak aby byl naplněn sledovaný účel.

3.2 Informace změněné v průběhu přenosu

Informace, které poskytujeme ostatním osobám, mohou být z jejich i našeho hlediska důvěryhodné, ale to ještě neznamená, že cílová osoba dostane důvěryhodnou informaci, kterou požadovala. Tyto informace z naší strany odejdou v pořádku, ovšem díky prostředí internetu se může stát, že v průběhu přenosu budou neoprávněně změněny či zaměněny za jiné.

Z technického hlediska se internet skládá z jednotlivých počítačů navzájem propojených v celosvětovou počítačovou síť. Tato má několik úrovní a dá se rozdělit do jednotlivých segmentů. Nejmenšími segmenty jsou sítě LAN (Local Area Network, lokální sítě např. firemní), které jsou dále spojovány do sítí WAN (Wide Area Network,

[19]DŽUBÁK, Josef & HOAX.cz. Co je to hoax, Co je to phishing, Co je to SCAM-419, Co jsou to podvodné loterie [online], ©2000-2017, [cit. 2018-01-16]. Dostupné z WWW: <http://hoax.cz/cze/>.
[20]MCCLUNG Jr, F. *Otče, sjednoť nás.* Praha: LOGOS, 1991, str. 103.

rozsáhlé na nějakém území např. České republiky) a tyto jsou propojeny v internet. Informace v takovéto síti jsou z koncového počítače předány specializovanému serveru, který dotazem zjistí cestu k cílovému počítači a poté informaci přepošle přes další servery a směrovače. Při vyhledávání informací je postup obdobný. Pro náš účel je ovšem podstatné, že přenos informace je realizován mezi jednotlivými počítači kabelovým, optickým či bezdrátovým vedením (tzv. „pasivní síťové prvky“). Každé z nich má své výhody i nevýhody. Dále je podstatné, že na internetu existují servery a směrovače (tzv. „aktivní síťové prvky“), které přijímají a předávají informaci ke koncovému počítači.

3.2.1 Možnosti ovlivnění přenosu informací

Ovlivnění přenosu tedy může nastat v dvou různých místech a to ve směrovacím prvku (server, směrovač) nebo přímo napadením vedení.

Internetové servery se dají napadnout fyzicky či softwarově. Fyzickému napadení je bráněno polohou serverů na hlídaných místech. Softwarová obrana serveru je zajišťována u malých serverů jen specializovanými programy či hardwarem, například firewally, antivirovými programy apod. Ale servery velkých společností či vládních institucí mají k ochraně dat a zjištění prolomení ochrany serveru speciální programy a mnohdy i tým osob, který se zabývá jen bezpečností serveru. Jednodušší je napadnout směrovač, tedy zařízení pro vytvoření podsítě (router, access point apod.), tyto mají většinou koncový uživatelé či společnosti poskytující internetové připojení. Většinou nejsou ani nijak zabezpečené z hlediska polohy (například společné prostory domu) a mají základní softwarovou ochranu.

Vedení je napadáno fyzicky, jelikož nemá žádné programové vybavení. Osoba, která chce informace v samotném vedení změnit, musí vedení buď přerušit a nahradit novým, vlastním či narušit jeho ochranu a připojit zde své zařízení, které je schopné informace zachytit, pozměnit a poté vyslat ve změněné podobě. Toto neplatí o bezdrátovém vysílání, kde musí dojít k napadení zdroje vysílání.

- Kabel
  - Výhodou je nízká cena a ohebnost materiálu.
  - Nevýhodou je relativně snadný odposlech, relativně snadné přerušení, nižší přenosová rychlost, menší propustnost dat, jeden kabel vede jen na jedno určité místo.

- Optický kabel
  - Výhodou je nemožnost odposlechu bez přerušení vedení, vysoká přenosová rychlost, vysoká propustnost dat.
  - Nevýhodou je vysoká cena kabeláže, horší ohebnost materiálu, jeden kabel vede jen na jedno určité místo.
- Bezdrátové spojení
  - Výhodou je možnost připojení více zařízení jedním prvkem, přenosovým prostředím je vzduch.
  - Nevýhodou je možnost odchycení signálu z každého místa dosahu prvku, snadný odposlech, přerušením signálu dojde k odpojení všech koncových počítačů, omezený dosah, který je zkracován předměty v prostředí a ovlivnitelnost jiným vysíláním.[21]

3.2.2 Zabezpečení přenosu informací

Ze všech způsobů zabezpečení přenosu informací byly vybrány základní, nejznámější a nejpoužívanější, tedy protokol TCP/IP, šifrování dat, elektronický podpis a využití certifikační autority.

Tyto prostředky neslouží k zjištění důvěryhodnosti informací, nicméně pokud již se rozhodneme, že zdroj a informace, které podává, budeme považovat za důvěryhodné, pak uvedené věci napomohou k tomu, aby informace i po přenosu přes internet zůstaly důvěryhodnými nebo aby bylo možné zjistit, že byly kompromitovány.

3.2.2.1. Protokol TCP/IP

„Jedná se o celosvětově nejpoužívanější komunikační protokol (či spíše soubor protokolů). Je univerzální (nezávisí na operačním systému) a je „routovatelný“.“[22]

Není jediným protokolem pro přenos informací, ale v obecné rovině platí, že: „Správný přenos dat internetem zajišťují komunikační protokoly. Hlavním komunikačním protokolem internetu je protokol TCP/IP, přičemž protokol IP se stará o vlastní přenos dat včetně adresování. Protokol TCP se pak stará o správný přenos dat -

[21]Zdroj oddílů 3.2.1. a 3.2.2.: HORÁK, J., KERŠLÁGER, M., *Počítačové sítě pro začínající správce*. Praha: Computer Press, a.s., 2003, str. 13 – 57.
[22]KVÍTEK, L., KATEDRA FYZIKÁLNÍ CHEMIE, PŘÍRODOVĚDECKÁ FAKULTA, UNIVERZITA PALACKÉHO, *Internet a zdroje*, [online], Olomouc 2005, [cit. 2018-01-18]. Dostupné z WWW: <http://fch.upol.cz/skripta/intz/1-NEW/INTZ.pdf>.

poskytuje protokolu IP kontrolní mechanismy. Data se přenášejí v balíčcích definované velikosti - paketech, které začínají hlavičkou, obsahující informace nezbytné pro přenos dat.“[23]

Dále se dozvíme, že „protokol TCP vytvářející při zahájení komunikace spolehlivý, bezchybný, plně duplexní kanál mezi dvěma počítači. TCP přidává mechanismy zabezpečení proti ztrátě či dublování dat při přenosu protokolem IP. Navíc protokol TCP zabezpečuje správné složení jednotlivých datagramů IP, na straně příjemce, za obnovení původní formy informace odeslané ze zdrojového počítače.“

Protokol TCP/IP je tedy prostředkem pro přenos informací poskytujícím základní ochranu.

3.2.2.2. Šifrování dat (kryptografie)

„Kryptografie se zabývá kódováním dat do podoby, nečitelné neoprávněnou osobou. Kódování se provádí pomocí šifrovacího algoritmu (matematická operace). Mimo kódování dat pro zajištění jejich důvěrnosti je třeba při provozu na internetu zajistit i autentizaci těchto dat, tedy zabezpečit správnou totožnost uživatele nebo procesu (serveru), s nímž je komunikace vedena.“[24]

Existují dva základní typy šifrovacích metod - symetrické (konvenční) a asymetrické šifrování (neboli šifrování veřejným klíčem).

- **Symetrické**

„Při symetrickém šifrování používají odesílatel a příjemce dat stejný šifrovací klíč. Důvěrnost je zajištěna tím, že je tento klíč tajný, proto se symetrickému šifrování také říká šifrování s tajným klíčem. Vlastní metody šifrování lze rozdělit do dvou skupin. Při blokovém šifrování se zašifruje blok dat o pevné délce jako celek. Při proudovém šifrování se data šifrují bit po bitu.

Jako bezpečný pro běžný provoz na internetu je pokládán algoritmus DES (Data Encryption Standard), který je zástupcem blokového šifrování, dalším zástupcem je

[23]KVÍTEK, L. KATEDRA FYZIKÁLNÍ CHEMIE, PŘÍRODOVĚDECKÁ FAKULTA, UNIVERZITA PALACKÉHO, Internet a zdroje, [online], Olomouc 2005, [cit. 2018-01-18]. Dostupné z WWW: <http://fch.upol.cz/skripta/intz/1-NEW/INTZ.pdf>.
[24]KVÍTEK, L. KATEDRA FYZIKÁLNÍ CHEMIE, PŘÍRODOVĚDECKÁ FAKULTA, UNIVERZITA PALACKÉHO, Internet a zdroje, [online], Olomouc 2005, [cit. 2018-01-18]. Dostupné z WWW: <http://fch.upol.cz/skripta/intz/1-NEW/INTZ.pdf>.

bezpečnější Triple-DES, tento je obdobou DES, kdy šifrování je provedeno třikrát za sebou, různými klíči.

Zástupcem proudového šifrování je algoritmus IDEA (International Data Encryption Algorithm). Tento je evropským standardem a ve srovnání s algoritmem DES nezaostává v rychlosti a mírně jej převyšuje v bezpečnosti.“[25]

- **Asymetrické**

„V algoritmech asymetrického šifrování se na rozdíl od symetrického používají dva různé klíče. První klíč je privátní a zná jej pouze vlastník klíče. Druhý klíč dává vlastník privátního klíče veřejně k dispozici všem, s nimiž šifrovaně komunikuje - veřejný klíč. Funkce obou klíčů je dvojí - data zašifrovaná privátním klíčem lze dešifrovat pouze příslušným veřejným klíčem a data zašifrovaná veřejným klíčem (např. odpověď příjemce odesílateli) pouze příslušným privátním klíčem. Tato vlastnost asymetrického šifrování se využívá rovněž při realizaci digitálních podpisů.

Příkladem je algoritmus RSA (zkratka jmen tvůrců -Rivest, Shamir, Adieman), který je užíván bankami ke komunikaci. „Principem realizace klíčů pro asymetrické šifrování algoritmu RSA je předpoklad, že lze jen obtížně rozložit dostatečně velké číslo na součin dvou prvočísel, na nichž je založena každá dvojice klíčů. Z daného veřejného klíče se dá tedy jen poměrně dosti obtížně zjistit odpovídající privátní klíč.“[26]

3.2.2.3. Elektronický podpis

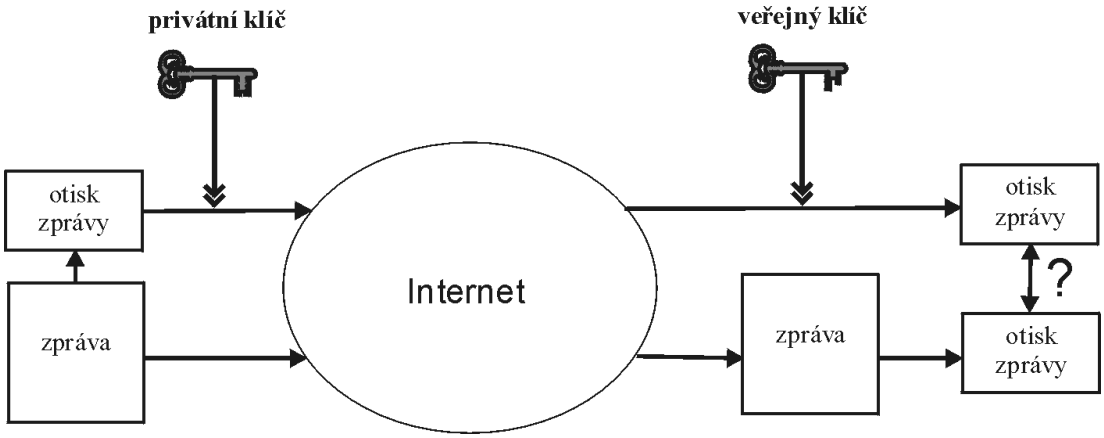
Dle zákona o elektronickém podpisu se jedná o „údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.“.[27]

„Digitální podpis umožňuje ověření obsahu zprávy a totožnosti jejího odesílatele. Pro realizaci digitálního podpisu se využívají technologie asymetrického šifrování a otisku zprávy. Základní princip vytvoření digitálního podpisu je poměrně jednoduchý. Odesílatel vytvoří otisk odesílané zprávy a zašifruje jej svým privátním

[25]KVÍTEK, L. KATEDRA FYZIKÁLNÍ CHEMIE, PŘÍRODOVĚDECKÁ FAKULTA, UNIVERZITA PALACKÉHO, Internet a zdroje, [online], Olomouc 2005, [cit. 2018-01-18]. Dostupné z WWW: <http://fch.upol.cz/skripta/intz/1-NEW/INTZ.pdf>.
[26]KVÍTEK, L. KATEDRA FYZIKÁLNÍ CHEMIE, PŘÍRODOVĚDECKÁ FAKULTA, UNIVERZITA PALACKÉHO, Internet a zdroje, [online], Olomouc 2005, [cit. 2018-01-18]. Dostupné z WWW: <http://fch.upol.cz/skripta/intz/1-NEW/INTZ.pdf>.
[27]ČESKO. *Zákon č. 227/2000 Sb. o elektronickém podpisu* In: *Sbírka zákonů,* Česká republika. 2000, částka 68. s. 3290 – 3297. §2 písm. a).

klíčem. Tento zašifrovaný otisk odešle společně se zprávou příjemci. Příjemce si vytvoří svůj otisk zprávy a porovná jej s dešifrovaným otiskem zprávy od odesílatele.

Obr. 1: Princip digitálního podpisu využívajícího asymetrické šifrování otisku zprávy[28]



Pokud oba otisky souhlasí, je zaslaná zpráva originální (neupravená během své cesty internetem). Současně je potvrzena totožnost odesílatele, protože dekódování je provedeno jeho veřejným klíčem.“[29]

Otisk (tzv. „hash“) zprávy je vytvořen tak, že z každé zprávy je vybrán vhodným algoritmem proměnný počet bitů, z níž se vytvoří řetězec o pevné délce, jedinečný pro tuto zprávu.

3.2.2.4. Certifikační autority

Dalším prostředkem jak zabezpečit přenos informací na internetu je používání tzv. „certifikátů“. Dle zákona o elektronickém podpisu se jedná o: „datovou zprávu, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu“[30]

[28] KVÍTEK, L. KATEDRA FYZIKÁLNÍ CHEMIE, PŘÍRODOVĚDECKÁ FAKULTA, UNIVERZITA PALACKÉHO, Internet a zdroje, [online], Olomouc 2005, [cit. 2018-01-18]. Dostupné z WWW: <http://fch.upol.cz/skripta/intz/1-NEW/INTZ.pdf>.
[29] KVÍTEK, L. KATEDRA FYZIKÁLNÍ CHEMIE, PŘÍRODOVĚDECKÁ FAKULTA, UNIVERZITA PALACKÉHO, Internet a zdroje, [online], Olomouc 2005, [cit. 2018-01-18]. Dostupné z WWW: <http://fch.upol.cz/skripta/intz/1-NEW/INTZ.pdf>.
[30] ČESKO. *Zákon č. 227/2000 Sb. o elektronickém podpisu* In: *Sbírka zákonů,* Česká republika. 2000, částka 68. s. 3290 – 3297.

V České republice akredituje poskytovatele certifikačních služeb Ministerstvo vnitra. V současné době poskytují certifikační služby pouze tři subjekty a existují dva typy certifikátů:

- **Komerční certifikáty**

Tyto slouží pro bezpečné přihlašování do aplikací např. datové schránky a zašifrování komunikace. Dále se dělí na osobní, který je určen pro konkrétní osoby a systémový určený pro technická zařízení (aplikace na serverech). Není automaticky uznáván úřady státní správy, strany se o jeho přijetí musí dohodnout.

- **Kvalifikované certifikáty**

Slouží k vytvoření zaručeného elektronického podpisu, který je uznáván všemi orgány veřejné moci v ČR. Dále k elektronické archivaci dokumentů, elektronickému podání daňového přiznání, odesílání datových zpráv, pokud má společnost více jednatelů, komunikaci s Českou správou sociálního zabezpečení, využívání elektronických formulářů a e-podatelen, práci s e-tržišti.[31]

Dalším možným zabezpečením přenosu spojeným s certifikačními autoritami je zabezpečení důvěryhodnosti serveru za pomoci certifikátu SSL (Secure Socket Layer). Důvěryhodnost v tomto směru není brána jako důvěryhodnost informací, které server obsahuje, ale jako zabezpečení dat na internetu při přenosu mezi prohlížečem a serverem. Tedy certifikát při přenosu zabezpečuje, že komunikace nebyla pozměněna a nebyla přesměrována na jinou stránku, než bylo požadováno. V prohlížeči poznáme zabezpečení tímto certifikátem dle adresního řádku, jelikož se v něm objeví řetězec znaků „https://adresa stránky“. SSL certifikáty jsou vydávány firmami ze soukromého sektoru. Za nejdůvěryhodnější certifikační autority na světě jsou považovány velké společnosti, například firma Symantec.[32]

[31]ČESKÁ POŠTA. *Kvalifikované certifikáty, Komerční certifikáty*, [online], © 2010 Česká pošta, [cit. 2018-01-18]. Dostupné z WWW: <http://www.postsignum.cz>.
[32]SSL MARKET od Zoner software. SSL certifikáty, [online], © ZONER software, a.s., [cit. 2018-01-18]. Dostupné z WWW: <https://www.sslmarket.cz/ssl/certifikaty#proc-ssl-market>.

4 Důvěryhodnost informací ve vztahu k bezpečnostně právnímu prostředí

Cílem kapitoly není popsat počítačovou kriminalitu, ale analyzovat, jak důvěryhodnost informací zasahuje do bezpečnostně právního oboru a jak souvisí s prevencí kriminality. Nejprve jsou uvedeny zákonné normy vztahující se k informacím na internetu a dále je nastíněno, k čemu může dojít, pokud osoba považuje za důvěryhodné takové informace, které nejsou pravdivé. V neposlední řadě došlo k analýze preventivní činnosti v oblasti počítačové kriminality v České republice.

4.1 Zákonné normy vztahující se k informacím na internetu

Celosvětově nejsou právní předpisy týkající se informací na internetu sjednocené. Pokud bychom zde chtěli uvést zákonné normy všech zemí světa, jednalo by se o zcela samostatnou práci. "Předpisy a směrnice evropské unie, které bezprostředně souvisí s informatikou a telekomunikacemi, jsou spíše předmětem jednoúčelových doporučení nebo naopak koncepčních materiálů velmi širokého záběru."[33]. Na jejich základě vznikají či jsou upravovány zákonné normy států evropské unie. Dále s přibývajícím množstvím informací a rozšířením internetu mezi lidmi dochází stále častěji k podvodným jednáním, dezinformacím a kybernetickým teroristickým útokům, proto jsou v mnoha vyspělých zemích zakládány instituce, které tyto informace odhalují, monitorují a analyzují. V České republice vznikla takováto instituce ke dni 1. 1. 2017, pod záštitou Ministerstva vnitra České republiky, jedná se o Centrum proti terorismu a hybridním hrozbám.

4.1.1 Zákonné normy

Pro práci jsou důležité jen zákonné normy České republiky, které se vztahují k problematice informací a důvěryhodnosti. Byly vybrány jen ty nejdůležitější a bylo stručně charakterizováno, čím přispívají k prevenci kriminality či k zajištění důvěryhodnosti šířených informací, popřípadě trestněprávními účinky.

[33]JIROVSKÝ, V. *Kybernetická kriminalita nejen o hacking, cracking, virech a trojských koních bez tajemství*. Praha: Grada Publishing, a. s., 2007, str. 90.

- Občanský zákoník, zákon č. 89/2012 Sb. ve znění pozdějších předpisů, který jednoznačně definuje vlastnické právo, dále pojmy právnická a fyzická osoba.
- Zákon o elektronických komunikacích, zákon č. 127/2005 Sb. ve znění pozdějších předpisů, který pokrývá širokou škálu působení telekomunikačních a podobných společností na internetu. Řeší telekomunikační tajemství a zákaz používání automatického systému volání bez lidské účasti pro účely přímého marketingu.
- Autorský zákon, zákon č. 121/2000 Sb. ve znění pozdějších předpisů, který je rozebírán dále.
- Zákon o ochraně osobních údajů, zákon č. 101/2000 Sb. ve znění pozdějších předpisů, související úzce s telekomunikačním tajemstvím a uchováním dat v databázích.
- Trestní zákoník, zákon č. 40/2009 Sb. ve znění pozdějších předpisů, sloužící společně se zákonem o přestupcích, zákon č. 251/2016 Sb. jako represivní nástroj.
- Zákon o některých službách informační společnosti, zákon č. 480/2004 Sb. ve znění pozdějších předpisů, který upravuje odpovědnost poskytovatelů služeb a šíření obchodního sdělení. Měl být vhodným nástrojem pro boj proti spamu, ale jeho dopad je téměř nulový.
- Zákon o regulaci reklamy, zákon č. 40/1995 Sb. ve znění pozdějších předpisů, který reguluje elektronické nešvary jako je spam.
- Zákon o službách vytvářejících důvěru pro elektronické transakce, zákon č. 297/2016 Sb. ve znění pozdějších předpisů, který nahradil zákon č. 227/2000 Sb. o elektronickém podpisu.
- Zákon o svobodném přístupu k informacím, zákon č. 106/1999 Sb. ve znění pozdějších předpisů a Zákon o informačních systémech veřejné správy zákon č. 365/2000 Sb. ve znění pozdějších předpisů.[34]

[34]JIROVSKÝ, V. *Kybernetická kriminalita nejen o hacking, cracking, virech a trojských koních bez tajemství*. Praha: Grada Publishing, a. s., 2007, str. 89 – 90.

- Zákon o kybernetické bezpečnosti, zákon č. 181/2014 Sb. ve znění pozdějších předpisů, upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.

Kromě zákonných norem existuje na internetu ještě jedna, tato ovšem není právně závazná a hlavně není jakkoli vynutitelná. Je jí takzvaná Netiketa.

4.1.2 Autorský zákon

„Autorský zákon upravuje tzv. autorská práva. To jsou práva autorů k jejich dílům. Dílo je zákonem definováno jako literární a jiné dílo umělecké a dílo vědecké, které současně je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě. Dílem je např. dílo slovesné (např. román), grafické (např. kresba), hudební (např. znělka), choreografické (např. baletní choreografie), fotografické, audiovizuální (např. film), architektonické (stavba) nebo počítačový program. Autorským dílem není pouhý nápad nebo myšlenka, dílo musí být vyjádřeno tak, aby jej někdo jiný mohl vnímat. Od tohoto okamžiku je dílo chráněno autorským právem, není tedy nutná žádná registrace, jako např. u patentů.

Autorská práva se dělí na osobnostní a majetková. Osobnostní zahrnují především právo osobovat si autorství, rozhodnout o zveřejnění díla, právo na nedotknutelnost díla, zejména právo udělit souhlas ke změně nebo jinému zásahu do díla. Majetková práva zahrnují hlavně právo dílo užít a udělit souhlas k užití.

Autorský zákon stanoví, že nikdo nesmí užívat autorská díla bez souhlasu držitele autorských práv, není-li zákonem stanovena výjimka. Pojem „užívání“ přitom znamená:

- **rozmnožování** - zhotovování dočasných nebo trvalých, přímých nebo nepřímých rozmnoženin díla nebo jeho části,
- **rozšiřování** - zpřístupňování díla v hmotné podobě převodem vlastnického práva,
- **pronájem** - zpřístupňování díla za účelem hospodářského nebo obchodního prospěchu poskytnutím originálu nebo rozmnoženiny díla,
- **půjčování** - zpřístupňování nikoli za účelem zisku,
- **vystavování** - umožnit dílo zhlédnout nebo jinak vnímat,

- **sdělování díla veřejnosti** - zpřístupňování díla v nehmotné podobě, živě nebo ze záznamu.

Autorský zákon upravuje udělování licencí k užití díla a stanovuje také případy, kdy licence není třeba. Protože není možné, aby si každý autor ohlídal, zda jeho dílo není užíváno bez jeho souhlasu, ustanovuje zákon tzv. kolektivní správu autorských práv. Pověřená sdružení pak vybírají poplatky za užívání děl (např. od rozhlasových stanic) a zisk rozdělují mezi autory.“[35]

4.1.3 Nepsaná norma – Netiketa

„Uvádí základní pravidla chování v síti "Network Etiquette - Netiquette", tedy jakousi etiketu sítě Internet.“[36]

Není závazným předpisem, který musí být dodržován. Je jen souborem pravidel, která by měl dodržovat každý člověk, šířící informace na internetu. Dodržování netikety (česká zkratka nahrazující anglickou zkratku Netiquette) neznamená, že server a informace na něm budou důvěryhodné, ale okrajově může netiketa k důvěryhodnosti napomoci. Pravidla netikety udává „RFC 1855 Netiquette Guidelines“. Pocházející sice z roku 1995, kdy u nás o existenci internetu vědělo málo lidí a od té doby se mnoho věcí změnilo, ovšem základ pravidel slušného chování na síti zůstává zachován.“

Pravidla jsou v tomto dokumentu rozdělena do tří skupin

- Komunikace „jednoho s jedním“
- Komunikace „jednoho s mnoha“
- Informační služby

Tyto jsou obsáhlé, ale jedno pravidlo zcela vystihuje problém týkající se důvěryhodnosti informací:

„Nepředpokládejte, že JAKÁKOLI informace, kterou naleznete je aktuální a přesná. Mějte na paměti, že nové technologie pouze dovolují komukoli publikovat, ale zdaleka ne všichni cítí odpovědnost, jakou s sebou publikování přináší.“[37]

[35]BEZPEČNÝ INTERNET.CZ. *Autorský zákon*, [online], [cit. 2018-01-03]. Dostupné z WWW: <http://www.bezpecnyinternet.cz/skoly/zakony/autorsky-zakon.aspx>.
[36]DŽUBÁK, J. & HOAX.cz. *Co je to hoax, Co je to phishing, Co je to SCAM-419, Co jsou to podvodné loterie* [online], ©2000-2017, [cit. 2018-01-16]. Dostupné z WWW: <http://hoax.cz/cze/>.
[37]DŽUBÁK, J. & HOAX.cz. Co je to hoax, Co je to phishing, Co je to SCAM-419, Co jsou to podvodné loterie [online], ©2000-2017, [cit. 2018-01-16]. Dostupné z WWW: <http://hoax.cz/cze/>.

4.2 Případy protiprávních jednání spojených s informacemi, které lidé považují za důvěryhodné

Pokud jen slepě věříme informacím z internetu a považujeme je za důvěryhodné bez ověření, může dojít k mylnému výkladu informace. Navíc v mnoha případech dochází ze strany poskytovatele těchto informací k protiprávnímu jednání. Mnohdy lidé svou slepou důvěrou přijdou jen o peníze. Někdy ovšem nevědomky šíří pomluvy a poplašné zprávy. V tu chvíli se mohou stát podezřelými i z trestného činu. Dále jsou popsány některé nejznámější situace, které jsou protiprávního charakteru.

4.2.1 Phishing

„Slovem PHISHING označujeme podvodné e-mailové útoky na uživatele internetu, jejichž cílem je vylákat důvěrné informace. Nejčastěji jsou to údaje k platebním kartám včetně PINu nebo různé přihlašovací údaje k účtům. Nemusí jít jenom o účty přímo bankovní, ale také ostatních organizací, kde dochází k manipulaci s penězi nebo je možné jakýmkoliv způsobem zneužit jejich služeb. Příkladem může být PayPal, eBay, Skype, Google.

Základní znaky phishingového e-mailu:

- Snaží se vyvolat dojem, že byl odeslán organizací, z jejichž klientů se snaží vylákat důvěrné informace. Toho se snaží docílit grafickou podobou e-mailu a zfalšováním adresy odesílatele.
- Text může vypadat jako informace o neprovedení platby, výzva k aktualizaci bezpečnostních údajů, oznámení o dočasném zablokování účtu či platební karty, výzkum klientské spokojenosti nebo jako elektronický bulletin pro klienty.
- V textu zprávy je link, který na první pohled většinou vypadá, že směřuje na stránky organizace (banky). Při jeho bližším prozkoumání zjistíte, že ve skutečnosti odkazuje na jiné místo, kde jsou umístěné podvodné stránky.

Banka takové zprávy nikdy nerozesílá a nemá důvod tyto informace od vás požadovat!

Pokud uživatel klikne na odkaz v e-mailu, dostane se na falešné stránky podvodníků, které jsou vytvořeny ve stejném stylu, jako originální stránky organizace

(banky). Na podvodných stránkách je připraven formulář, kde jsou požadovány důvěrné informace - čísla účtu, kódy k internetovému bankovnictví, PIN k platební kartě, přihlašovací údaje ke službám a podobně.“[38]

4.2.2 Podvodné loterie

„Uživatelům jsou formou spamu rozeslány e-maily, s oznámením vysoké výhry v nějaké mezinárodní loterii. Loterie je často pojmenována nebo jiným způsobem spojována s některou ze známých nadnárodních firem. Do údajného slosování se oslovení uživatelé dostali například výběrem e-mailových adres z celého světa a právě ta jejich vyhrála. Většinou bývá doporučeno, nikomu se o svém štěstí nezmiňovat (dotyčný by pak zjistil, že není jediný). Když se šťastlivec o svoji výhru přihlásí, dozví se kromě gratulace, že musí před vyplacením výhry zaplatit manipulační poplatek nebo daň ve výši několika desítek až tisíce EUR. Tento poplatek samozřejmě není možné strhnout z vyplácené výhry. Někdy po zaplacení prvního poplatku jsou požadovány další, mnohem větší částky.

V krajním případě jsou požadovány od "výherce" důvěrné informace nebo přístupové údaje k účtům například pod záminkou problému s převodem slibované výhry. Takto získané informace mohou podvodníci dále snadno zneužít.

Dalším možným způsobem, jak vylákat peníze z napálených lidí je zneužití tzv. žlutých linek, kdy údajný výherce je nucen z důvody získání informací o výhře zavolat na čísla se zvláštním tarifem. Než se automat na druhé straně "vypovídá", naskakují poplatky za telefon ve výši až několika stovek korun.“[39]

4.2.3 Scam419

„SCAM419 je označení pro druh podvodu u nás známého spíše jako Nigerijské dopisy. Tyto podvody nejsou žádnou novinkou, existovaly již dříve, buď ve formě klasického dopisu, nebo byly rozesílány faxem.

Rozvoj e-mailové komunikace umožnil za velice nízké náklady oslovit v krátkém časovém období milióny uživatelů. Tyto podvody se masově rozšířily, ale princip zůstává stejný: osloví vás neznámý člověk, že zdědil, získal nebo dokonce

[38]DŽUBÁK, J. & HOAX.cz. Co je to hoax, Co je to phishing, Co je to SCAM-419, Co jsou to podvodné loterie [online], ©2000-2017, [cit. 2018-01-16]. Dostupné z WWW: <http://hoax.cz/cze/>.
[39]DŽUBÁK, J. & HOAX.cz. Co je to hoax, Co je to phishing, Co je to SCAM-419, Co jsou to podvodné loterie [online], ©2000-2017, [cit. 2018-01-16]. Dostupné z WWW: <http://hoax.cz/cze/>.

spravuje něčí majetek ve výši několika desítek miliónů dolarů a potřebuje pomoc při jeho převodu ze země. Za to je slíbená tučná odměna ve výši několika desítek procent z celkové částky. Princip podvodu spočívá v tom, že oběť musí neustále platit nečekané administrativní poplatky a převod majetku se stále oddaluje.“[40]

4.2.4 Kybergrooming

Zatímco výše uvedené případy se řadí mezi podvodné jednání, tak fenomén posledních let tzv. „kybergrooming“ lze zařadit do oblasti cílené manipulace. „Kybergrooming je termín, který označuje chování uživatelů internetu, které má v dítěti vyvolat falešnou důvěru a připravit ho na schůzku, jejímž cílem je nezletilou/zletilou oběť pohlavně zneužít. Útočníci jsou tedy často pedofilové. Kybergrooming je velice často vázán na synchronní i asynchronní komunikační platformy, nejčastěji veřejný chat, seznamky, dále ICQ a e-maily. Za kybergrooming se také v širším pojetí považují jakékoli způsoby manipulace dětí a mladistvých prostřednictvím ICT.“[41]

4.2.5 Pomluva, šíření poplašné zprávy

K naplnění skutkových podstat těchto činů dochází uvedením nepravdivé informace jako důvěryhodné. K šíření lze efektivně využít internetu a jeho služeb, hlavně sociálních sítí, kde sdílenou nepravdivou či nebezpečnou informaci vidí všechny osoby, které mají sdílejícího mezi „přáteli“. Kterákoli osoba může informaci dále sdílet s ostatními. Naproti tomu, uvedení informace jen na webové stránce není efektivní. Musí totiž dojít k navštívení dané stránky. Opět platí, že než informaci budeme sdílet dále, měli bychom si jí ověřit. Sdílením pomluv a poplašných zpráv se můžeme dopustit protiprávního jednání nebo být z protiprávního jednání podezřelý. Vysvětlování a dokazování neviny následně zabere mnoho času, peněz a někdy i psychických sil.

Na internetu dochází k páchání i jiných protiprávních jednání jako zneužití osobních údajů, vydírání, nebezpečné vyhrožování, kyberšikana apod. Tyto málokdy mají něco společného s důvěryhodností informací. Výše byly popsány jen některé případy protiprávních jednání, jejichž popis je uveden k pochopení potřeby prevence.

[40]DŽUBÁK, J. & HOAX.cz. Co je to hoax, Co je to phishing, Co je to SCAM-419, Co jsou to podvodné loterie [online], ©2000-2017, [cit. 2018-01-16]. Dostupné z WWW: <http://hoax.cz/cze/>.

[41]CENTRUM PREVENCE RIZIKOVÉ VIRTUÁLNÍ KOMUNIKACE, Pedagogická fakulta Univerzity Palackého v Olomouci, *Kybergrooming* [online], © Centrum PRVoK PdF, Univerzita Palackého v Olomouci 2008 – 2017 ze dne 13. 09. 2008, [cit. 2018-01-03]. Dostupné z WWW: <https://www.e-bezpeci.cz/index.php/temata/kybergrooming/125-42>.

4.3 Prevence počítačové kriminality

V České republice je prevence kriminality dána do pravomoci ministerstva vnitra, které vydává metodiku, doporučení a krajské koncepce prevence, zastřešuje spolupráci mezi jednotlivými organizacemi, dále finančně podporuje a provádí některé programy. Preventivní činnost je „organizována na třech úrovních:

1. Na meziresortní úrovni - těžiště meziresortní spolupráce spočívá ve vytváření preventivní politiky vlády ve vztahu k tradiční (obecné) kriminalitě a koordinace preventivních činností jednotlivých resortů zastoupených v **Republikovém výboru pro prevenci kriminality** a podněcování aktivit nových. Situační prevenci kriminality se věnuje **Poradní sbor pro situační prevenci kriminality**.

2. Na resortní úrovni - programy prevence kriminality vycházejí z věcné působnosti jednotlivých ministerstev, obohacují jejich běžné činnosti o nové prvky a přístupy a ovlivňují tvorbu příslušné legislativy.

3. Na místní úrovni - do níž jsou zapojeny orgány veřejné správy, police, nevládní organizace a další instituce působící v obcích. Podstatou systému prevence kriminality na místní úrovni je optimální rozložení působnosti v oblastech sociální a situační prevence s ohledem na místní situaci, potřeby i možnosti.

Z hlediska účinnosti jsou nejefektivnější **programy prevence kriminality na místní úrovni**. Představují systém metodické, koncepční a finanční podpory ze strany ústředních orgánů státní správy a samosprávy a podpory vzniku programů prevence kriminality v krajích, ve městech a obcích zatížených vysokou mírou kriminality a dalšími kriminálně rizikovými jevy.“[42] Ministerstvo vnitra také vydalo dokument „Typy projektů prevence kriminality“[43] ve kterém jsou popisovány preventivní opatření nejčastěji realizovaná na místní úrovni.

[42] ČESKO. MINISTERSTVO VNITRA, odbor prevence kriminality. Prevence kriminality: Systém prevence kriminality v ČR [online], Prevence kriminality v České republice © 2018 made by Galileo Corporation s.r.o., [cit. 2018-03-02]. Dostupné z WWW: <http://www.mvcr.cz/clanek/web-o-nas-prevence-prevence-kriminality.aspx?q=Y2hudW09NA%3d%3d>.

[43] ČESKO. MINISTERSTVO VNITRA, odbor prevence kriminality. *Prevence kriminality na regionální a místní úrovni: Metodiky, doporučení a krajské koncepce prevence kriminality* [online], Prevence kriminality v České republice © 2018 made by Galileo Corporation s.r.o., [cit. 2018-03-02]. Dostupné z WWW: <http://www.mvcr.cz/clanek/prevence-kriminality-na-regionalni-a-lokalni-urovni.aspx?q=Y2hudW09Mg%3d%3d>.

Základními kameny prevence kriminality jsou ovšem rodina a škola, které nejvíce ovlivňují budoucí pachatele či oběti trestné činnosti. Těmto v oblasti prevence pomáhají organizace vystupující na místní úrovni, které jsou ovlivňovány metodikami a doporučeními vydávanými na resortní a mezirezortní úrovni. Práce je zaměřena na obyvatele území města Děčín, kteří se setkávají s preventivními opatřeními místního charakteru, proto se dále zabývá jejich analýzou.

4.3.1 Situační prevence počítačové kriminality

Z hlediska situační prevence nelze na místní úrovni podnikat mnoho kroků, jelikož orgány a organizace místní samosprávy mohou zasahovat jen do počítačů, které sami vlastní a ne do soukromých. Většina počítačové kriminality je páchána ze soukromých počítačů, které se často nenachází ani na území České republiky. V případě situační prevence lze hovořit jen o opatřeních, která poskytují, buď jednotlivé programy instalované na servery, technologie přenosu informací nebo samotné programy instalované do koncového zařízení uživatele. Těchto je v současné době obrovské množství a není v lidských silách je všechny obsáhnout.

Z pohledu poskytovatelů služeb na internetu lze hovořit hlavně o Firewallech, Antivirech, Spamových filtrech a v neposlední řadě i projektech soukromých společností např. projekt CZ.NIC (správce domény cz) s názvem DNSSEC.

4.3.1.1. Firewall

Z širšího hlediska se jedná o „sadu opatření (hardwarových, softwarových či personálních), která mají za cíl propojit dvě nebo více sítí s různou úrovní důvěryhodnosti tak, že sníží (předem definovaná) rizika vyplývající pro chráněné sítě z tohoto propojení.“[44] Může být softwarový či hardwarový. Zatímco hardwarový se vzhledem k jeho ceně užívá u aktivních síťových prvků, softwarový bývá užíván v kterémkoli počítači. V současné době jsou firewally implementovány v základní verzi již v některých operačních systémech, například v Microsoft Windows XP, Vista, 8, 8.1, 10 ve všech dostupných verzích.

4.3.1.2. Antivir

Antivir je program sloužící k vyhledávání škodlivého softwaru, který napadá počítač a následně z něj může zasílat bez vědomí uživatele e-maily, informace a mnohé další. Napadením se z koncové stanice stává nedůvěryhodný počítač nebo zdroj

[44] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* Brno: Computer Press, a.s., 2004, str. 116.

škodlivých informací. „Je zajímavé, že označení jim zůstalo i přesto, že vyhledávají kromě virů mnoho jiných škodlivých programů.“[45] „Všechny druhy programů, které nějakým způsobem uživateli škodí, se označují souhrnným názvem škodlivý software, občas se můžete setkat s povedenějším anglickým označením malware (zkratka z malicious software).

Pravděpodobně nejznámější odrůdou škodlivého software je počítačový virus. Označení je zvoleno kvůli nezaměnitelné podobnosti s biologickými viry. I počítačový virus totiž potřebuje k životu a šíření hostitele[46] (to je jeden z rozdílů oproti jiným formám škodlivého software)“[47] Dále se setkáváme se skupinou označenou jako červi. „Na rozdíl od virů nepotřebují ke svému šíření hostitele. Jedná se o samostatné programy, které ke svému šíření využívají především sítě internet. Samy se rozešlou všem osobám, které máte ve svém adresáři, často jako příloha e-mailové zprávy s lákavým názvem (lechtivá fotka známé krásky, milostný dopis apod.) I přes stále opakující osvětu se najde řada uživatelů, kteří přílohu otevřou. Moderní červi ovšem nepotřebují, aby je někdo otevíral, dokáží se spustit sami o sobě. Kromě elektronické pošty využívají k šíření otevřené porty počítače, webových stránek a podobně.“[48] Třetí skupinou škodlivého softwaru jsou tzv. trojské koně se svou podskupinou nazývanou Spyware, tyto shromažďují na pozadí běžícího programu informace o uživateli (hesla, PINy a jiná data) a jednou za čas je odešlou na určenou adresu. Takto získané informace jsou dále užity k protiprávním jednáním či k cílené reklamě.

„Antivirové systémy mývají řadu různých částí. Jedna slouží pro kontrolu souborů uložených na disku počítače, jiná je rezidentním scannerem, který kontroluje všechny otevírané soubory a soubory stahované z internetu, další zase kontroluje přílohy příchozí pošty. Pro serverové systémy jsou k dispozici antiviry kontrolující poštu přímo na poštovním serveru a stahované soubory přímo na firewallu.“[49]

4.3.1.3. Spamový filtr

„Ačkoliv jsou nevyžádané e-maily trestně postižitelné, jsou e-mailové schránky denně zahlcovány spamem. Většinu spamu si však ani nepřečtete, neboť i zachytí tzv. spamový filtr, který na základě odesílatele a předem udaných klíčových slov třídí příchozí na e-maily na vyžádanou a nevyžádanou poštu.

[45] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* Brno: Computer Press, a.s., 2004, str. 16.
[46] Spustitelný soubor či část spustitelného kódu.
[47] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* Brno: Computer Press, a.s., 2004, str. 128.
[48] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* Brno: Computer Press, a.s., 2004, str. 16.
[49] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* Brno: Computer Press, a.s., 2004, str. 16.

Filtrování probíhá v první řadě podle e-mailové adresy (případně IP adresy) odesílatele. Jestliže je umístěna na tzv. blacklistu, je zpráva z této adresy automaticky označena jako spam. Následně spamový filtr prochází samotný obsah e-mailu. Porovnává text s obsahem předešlého spamu a pokud najde vícero podobností, označí zprávu jako spam.

Spamový filtr ve většině e-mailových schránek lze ručně upravit. Můžete do databáze například přidat slova a slovní spojení, která – vyskytují-li se v e-mailu – naznačují, že se jedná o spam. Rozeznání spamu však nemůže být nikdy dokonalé, protože posouzení toho, zda se u konkrétního e-mailu jedná o spam, může být často velice individuální.“[50]

4.3.1.4. DNSSEC

„Podobně jako jiné služby, které internet nabízí, i systém doménových jmen (DNS – Domain Name System) byl vytvořen v době, kdy bylo k internetu připojeno pouze malé množství uzlů a provozovatelé těchto uzlů se vzájemně znali. Vzhledem k tomu, do jaké míry později internet narostl co do počtu připojených lidí a počítačů, bylo nutné začít řešit otázku bezpečnosti jednotlivých služeb. Všichni uživatelé internetu se už neznají a je smutným faktem, že ne všichni se k němu připojují s bohulibými úmysly.

DNSSEC je rozšíření systému DNS, které zvyšuje bezpečnost služby doménových jmen. Principem DNS je překlad jmenných internetových adres, jako například www.nic.cz nebo www.dobradomena.cz, na adresy číselné, kterým počítače rozumějí a jejichž pomocí dokážou zajistit zobrazování webových stránek, odesílání e-mailů, telefonování po internetu a další běžné internetové služby. DNSSEC zvyšuje bezpečnost při používání DNS tím, že zabraňuje podvržení falešných, pozměněných či neúplných údajů o doménových jménech.

Služba DNS, není-li zabezpečena pomocí DNSSEC, poskytuje potencionálnímu útočníkovi několik míst, na kterých je možné komunikaci narušit a zfalšovat údaje. Tím, že útočník změní údaje o doménových jménech, ovlivní fungování dalších internetových služeb, které může tímto zásahem zneužít. Útočník pak může například:

- získávat cizí e-maily

[50] FIŠEROVÁ, K. *Spamový filtr* [online], © 2017 SmartSelling [cit. 2018-03-01]. Dostupné z WWW: <https://www.smartemailing.cz/spamovy-filtr/>.

- pomocí falešných webových stránek získávat hesla, přístupové kódy či údaje o platebních kartách apod.
- obcházet antispamovou ochranu v DNS a spam posílat
- podvrhnout zprávy a informace na webových stránkách
- přesměrovávat či odposlouchávat telefonní hovory, vedené přes internet.

Uživatel přitom nemá ve většině případů šanci poznat, že se děje něco nekalého. Díky zavedení DNSSEC získá jeho uživatel jistotu, že informace, které z DNS získal, byly poskytnuty správným zdrojem, jsou úplné a jejich integrita nebyla při přenosu narušena. DNSSEC zajistí důvěryhodnost údajů, získaných z DNS.“[51]

Z pohledu technologie přenosu informací jsou využívány opatření popisovaná v kapitole 3.2.2, tedy taková, která zajišťují, aby informace došla k uživateli nezměněna. Jsou jimi hlavně šifrování komunikace (zajišťující bezpečný přenos), certifikáty (označující prověřený (důvěryhodný) server, identifikující server, se kterým je vedena komunikace), elektronický podpis, některé vlastnosti samotného protokolu TCP/IP a další.

Z pohledu programů instalovaných do koncových zařízení uživatele můžeme hovořit opět o Firewallech, antivirech a spamových filtrech pro koncové uživatele. Tyto jsou jinak koncipovány vzhledem ke struktuře a účelu jejich použití. K těmto se ovšem přidávají i další opatření, kterými jsou například blokování vyskakovacích oken v jednotlivých prohlížečích internetu (například doplněk ADBlock v prohlížeči Mozilla FireFox) nebo přímo blokování jednotlivých internetových stránek či jejich skupin pro konkrétního uživatele tzv. „rodičovský zámek“ (blokování přístupu na stránky se škodlivým obsahem).

4.3.2 Sociální prevence počítačové kriminality

Jak již bylo uvedeno, základním subjektem sociální prevence je rodina, která působí na osoby již od narození. Zodpovědní za výchovu osob jsou rodiče a preventivní činnost je závislá na jejich ochotě, znalostech, zkušenostech a přístupu k dané oblasti. Pokud je rodina nefunkční, nelze očekávat u dítěte byť i jen základní ponětí o tom co je škodlivé (protiprávní) chování pro společnost. V opačném případě mohou rodiče své

[51] CZ.NIC, SPRÁVCE DOMÉNY CZ, *Jak funguje DNSSEC* [online], © 2018 CZ.NIC, z. s. p. o., [cit. 2018-02-03]. Dostupné z WWW: <https://www.nic.cz/page/444/jak-funguje-dnssec/>.

dítě ovlivnit předáním zkušeností a dobrých návyků. Pokud nemají sami potřebné znalosti, mohou se obrátit na některé nestátní organizace, které poskytují školení a materiály v oblasti prevence.

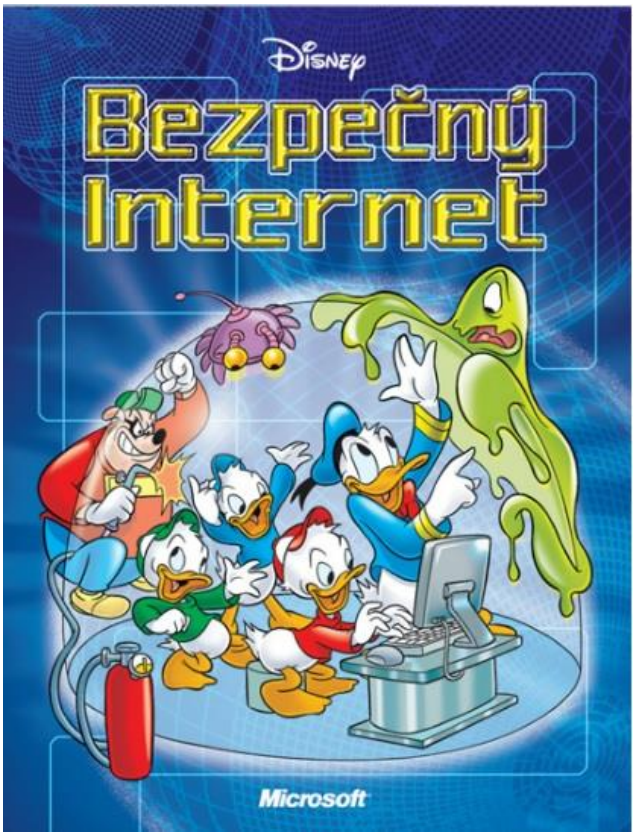
Jedním z mnoha projektů je stránka dostupná z http://www.bezpecnyinternet.cz, která rozděluje osoby přistupující k informacím do kategorií:

- začínající uživatel
- pokročilý uživatel
- rodiče
- děti
- školy

a poskytuje jim bezplatné on-line kurzy jak zacházet s internetem a chovat se bezpečně při jeho užívání.

V neposlední řadě poskytuje i komiksové příběhy, působící preventivně zábavnou formou.

Obr. 2: Přední strana jednoho z komiksů[52]



První institucí, se kterou se osoba setká a jejíž preventivní činnost ovlivňuje stát je školské zařízení pod patronací příslušného ministerstva.

„Základním principem strategie prevence sociálně patologických jevů v resortu školství, mládež a tělovýchovy je výchova dětí a mládeže ke zdravému životnímu stylu, k osvojení pozitivního sociálního chování a rozvoji osobnosti.

[52]Dostupné z WWW: <http://www.bezpecnyinternet.cz/deti/komiksove-pribehy/bezpecny-internet.aspx>.

Působení na mladou generaci musí mít charakter výchovně vzdělávací. Musí jít o proces kdy je nalezeno optimální klima školy a sociálních vztahů, dochází ke zvyšování sociální kompetence dětí a mládeže, k rozvoji dovedností, které vedou k odmítání všech forem sebedestrukce, projevů agresivity a porušování zákona.“[53]

MŠMT udává pouze obecnou formu prevence určitých škodlivých jevů, například kyberšikany. Ukládá každé škole za povinnost jednou ročně vytvořit preventivní program a realizovat jej takovou formou, aby byl přímo implementován do činnosti školy jako běžná aktivita. Následně je úkolem školy analyzovat úspěšnost preventivního programu a vyvodit z něj poznatky pro příští rok. Tedy nelze říci, že by preventivní program v této oblasti byl jednotný. Navíc je školám povoleno přenechat tuto činnost soukromým společnostem či externím spolupracovníkům.

Dalším subjektem, který má i jeden z hlavních úkolů prevenci kriminality je Policie ČR, tuto obstarává v oblasti počítačové kriminality OTP PČR (Oddělení tisku a prevence Policie ČR). Na základě vlastních poznatků a zkušeností jsou vypracovány programy a dokumenty v tištěné, vizuální či audiovizuální podobě. Ty jsou následně prezentovány široké veřejnosti. Jejich prostřednictvím jsou veřejnosti vysvětlena protiprávní jednání a je seznámena s postupem, jak se chovat v případě konfrontace s nimi. Je tedy upozorňováno na nedůvěryhodné zdroje, postupy a informace objevující se na internetu. Dále je formou přednášek prováděna osvětová činnost ve školských zařízeních.

Na webových stránkách www.policie.cz a www.prevencekriminality.cz lze naleznout materiály určené pro preventivní programy. Materiály jsou volně ke stažení.

Mezi ně patří hlavně:

- audiovizuální preventivní projekt krajského ředitelství policie Královéhradeckého a Pardubického kraje s názvem Prevencí k bezpečí. Obsahující videa: *Každý klik si rozmysli* - neobnažuj soukromí! (rizika virtuální komunikace - verze pro děti a mládež) a *Chraňte své dítě i na netu* (rizika virtuální komunikace - verze pro rodiče)[54]

[53] ČESKO. MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY. MŠMT: *Školní preventivní program pro mateřské a základní školy a školská zařízení* [online]. MŠMT, 39 s., [cit. 2018-02-03]. Dostupné z WWW: <www.msmt.cz/file/7347_1_1/> str. 5.
[54]ČÍŽKOVSKÝ, J, KAIZAROVÁ, H., *Prevencí k bezpečí* [online], © 2017 Policie ČR, 31. srpna 2015 [cit. 2018-03-03]. Dostupné z WWW: <http://www.policie.cz/clanek/prevenci-k-bezpeci.aspx>.

- tisknutelné brožury (příloha II) a příručku pro rodiče z internetové adresy http://www.prevencekriminality.cz

Obr. 3: Jeden z letáků dostupných na http://www.prevencekriminality.cz[55]

Na činnost rodiny a státních organizací navazují i některé soukromé firmy, které jí financují ze svých zdrojů. Poskytují školení za úplatu či využívají spolupráce s Ministerstvem vnitra a získaných grantových prostředků. Těchto je mnoho, příkladem je již zmiňované zájmové sdružení právnických osob CZ.NIC (správce domény cz), které vedle své hlavní činnosti provozuje projekty:

„Safer Internet (SIC CZ)

Projekt SIC CZ zahájený v červenci roku 2016 si klade za cíl ve spolupráci s Národním centrem bezpečnějšího internetu pokračovat v aktivitách zaměřených na chování dětí v on-line prostoru. V rámci projektu je šířeno povědomí o bezpečnějším využívání Internetu prostřednictvím přednášek zejm. na základních a středních školách v České republice či vydávání tematických publikací. CZ.NIC v rámci projektu zajišťuje rovněž provoz horké linky zaměřené na oznamování a odstraňování

[55]ČESKO. MINISTERSTVO VNITRA, odbor prevence kriminality. *Tiskoviny*, [online], Prevence kriminality v České republice © 2017 made by Galileo Corporation s.r.o., [cit. 2018-02-03]. Dostupné z WWW: <http://www.prevencekriminality.cz/ke-stazeni/tiskoviny-1/ e-bezpeci-75cs.html>.

nelegálního obsahu, především šíření dětské pornografie. Projekt je spolufinancován Evropskou komisí v rámci programu Connecting Europe Facility.

Jak na Internet

Osvětový projekt, televizní miniseriál, jehož cílem je přiblížit Internet a jeho možnosti široké veřejnosti. Diváci se mohou seznámit s tématy, jako jsou například internetové seznamky, 3D tisk nebo třeba jak funguje Internet. Všechny epizody, včetně rozšiřujících textů, jsou k dispozici na webu.

Nebojte se Internetu

Osvětový projekt a televizní minipořad, jehož cílem je přiblížit Internet a jeho technologie zejména dříve narozeným divákům, kteří na rozdíl od mladé generace novým technologiím často tolik nerozumí, a dokonce mohou mít z jejich používání obavy. Seriál vznikl v roce 2016 a jeho hlavní role ztvárnili Dana Batulková a Václav Kopta.

Nauč tetu na netu

Nauč tetu na netu je další z osvětových projektů sdružení CZ.NIC. Cílovou skupinou tohoto seriálu jsou děti a mladiství, svou veselou formou však zaujme i dospělé. Projekt vznikl ve spolupráci s Českou televizí a je pravidelně vysílán na programu ČT :D, anebo je možné jej zhlédnout online, přímo na webových stránkách.

Edice CZ.NIC

Vydávání odborných a naučných knih je jednou z dalších aktivit sdružení. Cílem je, podobně jako v řadě dalších případů, osvěta v oblasti domén, Internetu a internetových technologií. Kromě tištěných verzí vychází v edici i elektronická podoba knih.“[56]

4.3.3 Souvislost prevence kriminality s důvěryhodností informací

Při analýze preventivních opatření a programů uvedených v minulých kapitolách a podkapitolách se setkáváme několikrát s pojmem „důvěryhodný“ (server apod.), ale hlavním termínem je zde bezpečnost osob užívajících internet. V dostupných

[56] CZ.NIC, SPRÁVCE DOMÉNY CZ, *Projekty pro koncové uživatele* [online], © 2018 CZ.NIC, z. s. p. o., [cit. 2018-03-02]. Dostupné z WWW: < https://www.nic.cz/page/2086/projekty-pro-koncove-uzivatele/>.

materiálech se stále opakují mírně upravené fráze: „neposílejte žádné informace osobám, které neznáte“, „nevěřte informacím, které jste si neověřili“, „nepřipojujte se na stránky a servery, které neznáte“, „neotevírejte soubory, které neznáte a neposlal vám je váš známý“ a podobné. Pokud se zamyslíme, pak tyto fráze hovoří o důvěryhodnosti poskytnutých informací. Daly by se přepsat jako: „posílejte informace jen důvěryhodným osobám“, „věřte jen informacím z důvěryhodných zdrojů, které jsou ověřené“, „připojujte se jen na důvěryhodné stránky a servery“, neotvírejte nedůvěryhodné soubory od nedůvěryhodných lidí“. Jejich významy lze považovat obsahově za totožné. Tedy je vidět, že důvěryhodnost informací na internetu je úzce spojena s prevencí počítačové kriminality.

5 Výzkum

Jak již bylo uvedeno v kapitole 1, výzkum byl proveden kvantitativně kvalitativní formou. Jeho kvantitativní část byla realizována dotazníkovým šetřením v období leden – únor roku 2018 v České republice, Ústeckém kraji, okrese Děčín. Bylo rozdáno celkem 300 anonymních dotazníků. K zajištění rovnoměrného věkového rozložení vzorku, bylo každé věkové skupině předáno 60 ks dotazníků. Aby se předešlo problému s velmi nízkou návratností, byly distribuovány do uzavřených společností – základní škola, střední škola, vysoká škola, útvary policie a domovy důchodců v Děčíně. Problém návratnosti se tímto nepodařil vyřešit, jelikož se vrátilo jen 197 vyplněných dotazníků.

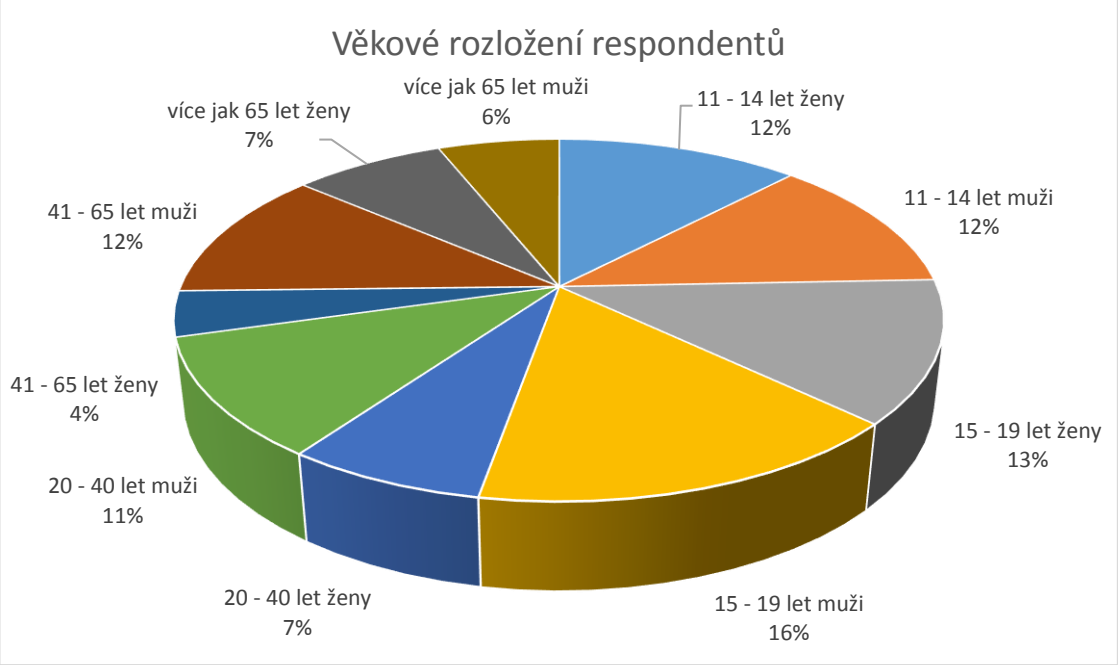
Kvalitativní část byla realizována dne 4. 3. 2018 formou řízeného rozhovoru s policistkou Krajského ředitelství Policie ČR Ústeckého kraje, Územního odboru Děčín, Oddělení tisku a prevence (dále jen KŘP Ústeckého kraje, ÚO Děčín, OTP), nprap.. Petrou Trypesovou. Z rozhovoru bylo zjištěno, že v minulosti došlo ke sloučení funkce tiskového mluvčího a pracovníka prevence kriminality. V tu chvíli se prioritou Policie ČR stala funkce tiskového mluvčího a prevence kriminality zůstala na dobrovolnosti každého pracovníka. Preventivní programy a i samotná prevence přestala být ze strany Policie ČR podporována. Primární prevence v této době není realizována vůbec a občas dochází k prevenci sekundárního a terciálního charakteru. V Ústeckém kraji se preventivní činností zabývá na plný úvazek pouze jeden občanský zaměstnanec. V okrese Děčín je jedinou určenou osobou právě tisková mluvčí a je dána možnost řadovým policistům z obvodních oddělení (dále jen OOP) se podílet na prevenci. V současné době má svého policistu zabývajícího se prevencí jen OOP Děčín-Podmokly, OOP Děčín-město, OOP Varnsdorf, OOP Rumburk a dopravní inspektorát Děčín. Tito policisté nejsou nijak systémově proškolováni, nebyl vydán rozkaz, metodika ani koncepce prevence kriminality. Všechny školení policistů jsou ponechány na jejich dobrovolnosti. Stejně tak policisté realizují preventivní činnost, kdy jsou kontaktování jednotlivými subjekty a je jen na jejich volbě, zda vyhoví vzneseným požadavkům.

5.1 Zhodnocení výzkumu – komparace výsledků

Z celkového počtu vyplnilo dotazník 111 respondentů mužského pohlaví a 86 respondentů ženského pohlaví, čehož se týkala první otázka.

Pro účely výzkumu bylo věkové spektrum rozloženo do skupin *11 – 14 let, 15 - 19 let, 20 – 40 let, 41 – 65 let a více jak 65 let*. První ze skupin odpovídá druhému stupni základní školy, kdy již osoby začínají více komunikovat na internetu a jsou tedy náchylnější k protiprávnímu jednání. Jedná se o nejrizikovější skupinu osob (24% respondentů). Druhá skupina *15 – 19 let* byla zvolena vzhledem k psychickému vývoji (pubertě) osob, kdy jsou tyto snáze ovlivnitelné. Hledají sami sebe a snadno podlehnou tlaku okolí (29 % respondentů). Třetí skupina *20 – 40 let* byla zvolena, jelikož osoby v tomto věku dospívaly a vyrůstaly v období největšího rozvoje internetu a byly jím tedy bezprostředně ovlivněni (18% respondentů). Osoby z předposlední skupiny *41 – 65 let*, byly již v době hlavního rozvoje internetu dospělí či blízko věku dospělosti, tedy ovlivnění nebylo tak velké (16% respondentů). Poslední skupina *více jak 65 let* byla zvolena, aby bylo možno zjistit, jak je prováděna prevence kriminality u osob důchodového věku (13% respondentů). Rozdělení do skupin dle pohlaví je viditelné z grafu 2.

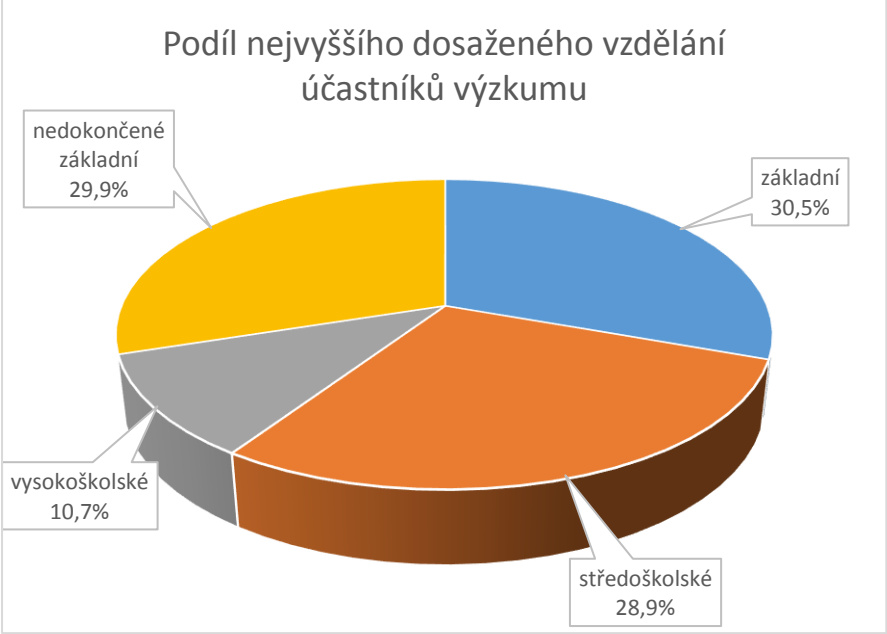
Graf 2: Věkové rozložení respondentů dotazníkového šetření[57]



[57] Vlastní zdroj.

V souvislosti s touto otázkou bylo policistkou zabývající se prevencí konstatováno, že cílovými skupinami preventivních opatření z její strany jsou osoby staršího školního věku (druhý stupeň základních škol), mladistvý (střední odborná učiliště, střední školy), rodiče v rámci třídních schůzek (výjimečně) a senioři v klubech důchodců. V domovech důchodců není preventivní činnost prováděna, jelikož bylo zjištěno, že osoby tohoto věku, mající přístup k internetu, bydlí ve většině případů ve vlastních bytech.

Graf 3: Podíl nejvyššího dosaženého vzdělání účastníků výzkumu[58]



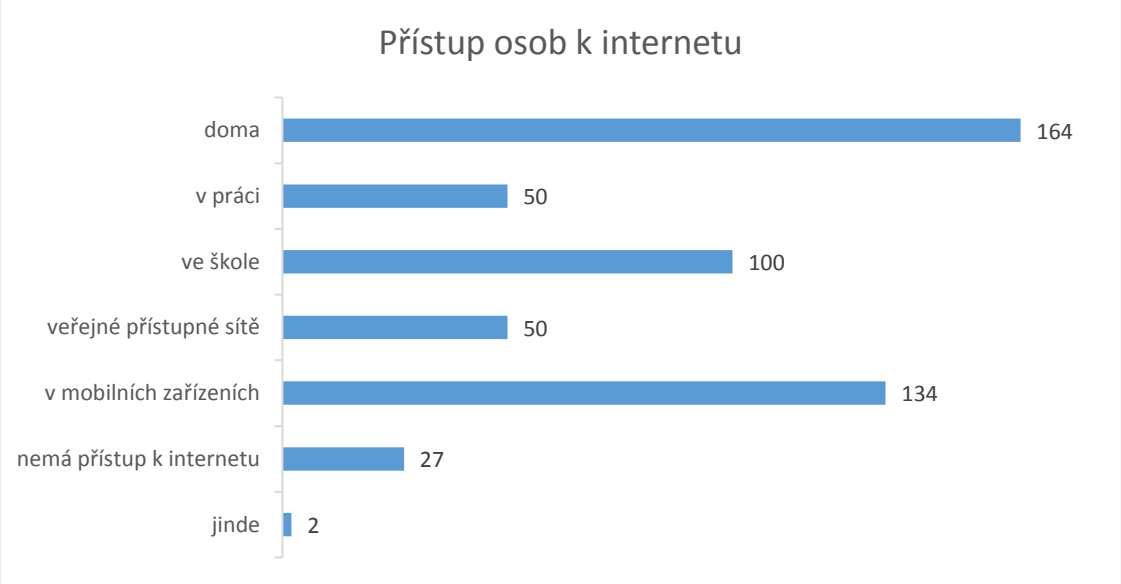
Další otázka byla zaměřena na zjištění nejvyššího dosaženého vzdělání zúčastněných osob. Výzkumu se zúčastnilo 59 osob s nedokončeným základním vzděláním, 60 osob se základním vzděláním, 57 osob se středoškolským vzděláním a 21 osob s vysokoškolským vzděláním. Procentuální poměr je viditelný z grafu 3.

V následné otázce bylo zkoumáno, kde všude přistupují respondenti k internetu. Tedy v jakých místech a zařízeních by bylo možné realizovat situační prevenci počítačové kriminality. Dotazovaným byla ponechána možnost více odpovědí, včetně doplnění vlastního názoru. Bylo zjištěno, že nejčastěji (164 případů ze 197 možných) osoby přistupují k internetu z domova. Druhou nejčastější odpovědí byla možnost, že se osoby připojují z mobilních zařízení, tedy odkudkoli. Jako třetí nejčastější bylo uvedeno připojení z domova. Část vzorku, konkrétně 27 lidí uvedlo, že nemá přístup k internetu

[58] Vlastní zdroj.

vůbec. Při bližším pohledu na dotazníky, které měly vyplněnou tuto možnost, bylo zjištěno, že se jedná o obyvatele domova důchodců, tedy osoby starší 65 let. Jak bylo řečeno výše, došlo k malé návratnosti dotazníků, na čemž se podílely právě velkou měrou osoby starší 65 let. Z 60 distribuovaných dotazníků se vrátilo pouze 27 a u všech byla zatržena možnost „*nemám přístup k internetu*“ a zbylé otázky nebyly vyplněny. Z tohoto důvodu nebyla tato skupina dále posuzována a hodnocena. Dva subjekty vypsaly ve volné části otázky odpovědi: „u babičky“ a „Téměř všude a pořád“. První z odpovědí by se dala logicky zařadit pod kategorii „*doma*“. Druhá je všeobecná a nic neříkající. S největší pravděpodobností by se dala zařadit k odpovědím „*v mobilních zařízeních*“.

Graf 4: Kde využívají internet subjekty výzkumu[59]

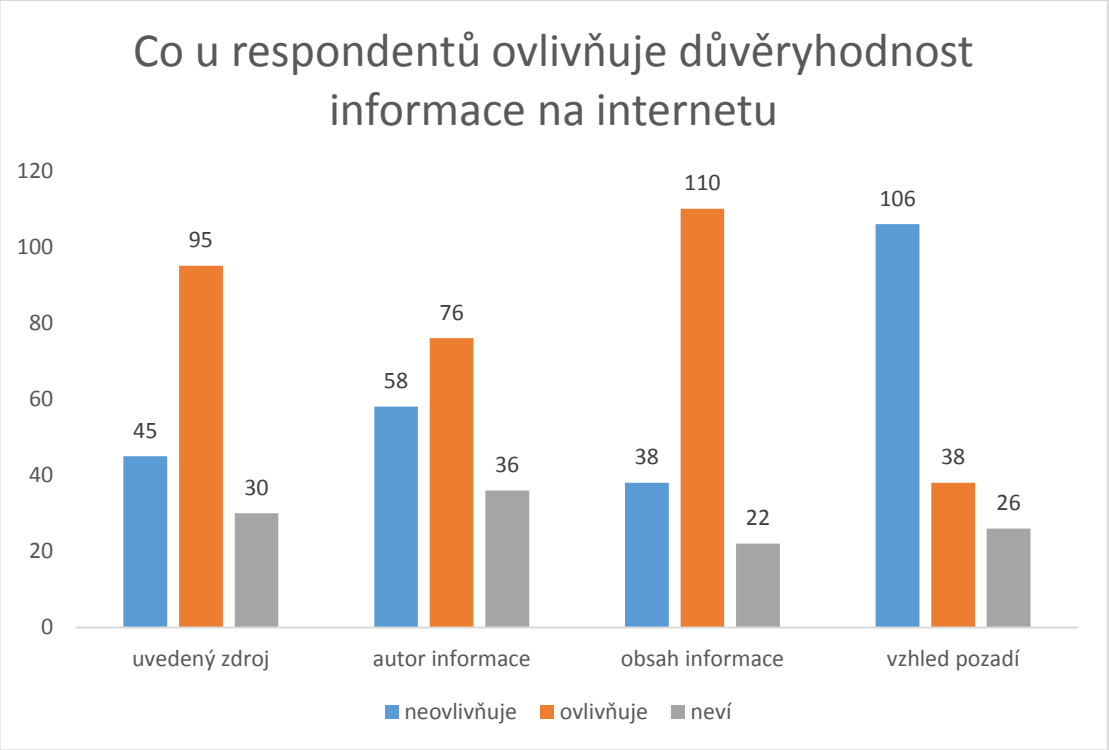


Další otázka: „*Jakou měrou, podle vás, ovlivňuje důvěryhodnost informace na internetu:*“ s následným výčtem faktorů a možným výběrem hodnoty: „*neovlivňuje, spíše neovlivňuje, nevím, spíše ovlivňuje, zcela ovlivňuje*“, byla zařazena do dotazníku k potvrzení či vyvrácení hypotéz I[60], II[61], III[62], IV[63]. Pro účely výzkumu byly první dvě hodnoty zařazeny do skupiny „*neovlivňuje*“ a poslední dvě hodnoty do skupiny „*ovlivňuje*“, jelikož jsou stejného charakteru. Výsledky jsou shrnuty v grafu 5. Je tedy

[59] Vlastní zdroj.
[60] Hypotéza I: Pro většinu osob je důvěryhodnost informace zaručena jejich autorem.
[61] Hypotéza II: Pro většinu osob je důvěryhodnost informace zaručena jejím obsahem.
[62] Hypotéza III: Méně jak 50 % osob získávajících informace z internetu nepovažuje za důležitý zdroj informace.
[63] Hypotéza IV: Pro více jak 50% osob není důležitý vzhled stránky při určování důvěryhodnosti podávané informace.

viditelné, že pro většinu osob účastnících se výzkumu je pro určování důvěryhodnosti informace důležitý její obsah, zdroj uvedený u informace a následně autor této informace. Pozadí, na kterém je prezentována informace, je pro většinu dotazovaných nedůležité. Hypotéza I a II byla tímto pro zkoumaný vzorek potvrzena. Celkem 45 osob (26,47%) respondentů považuje za nedůležitý pro důvěryhodnost informace její zdroj, čímž byla potvrzena i hypotéza III. 106 osob (62,35%) účastnících se výzkumu považuje za nedůležité pozadí, na němž je prezentována informace. Z toho vyplývá, že byla potvrzena i hypotéza IV.

Graf 5: Co u respondentů ovlivňuje důvěryhodnost informace na internetu[64]



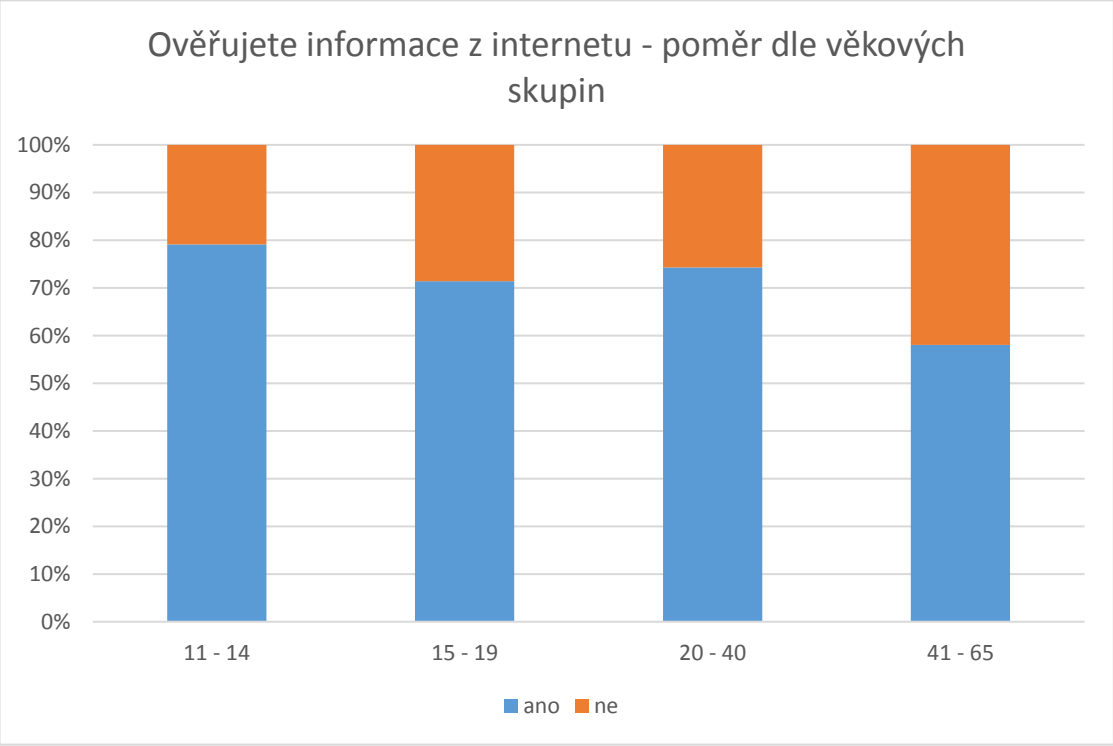
Otázka: „*Ověřujete si pravdivost informace získané na internetu?*“, byla zařazena do dotazníku k ověření hypotézy V[65], u které musí být výsledky kombinovány s daty získanými z otázky týkající se věku. A dále hypotézy VI[66]. Odpověď zde byla možná jen kladná či záporná, kdy 122 osob (68,92%) označilo pole s popiskem „ano“. Tímto byla vyvrácena hypotéza VI, jelikož jen 31,08% respondentů neověřuje pravdivost informace získané z internetu. V kombinaci se získanými údaji o věku a skutečností, že zúčastněné osoby starší 65 let při výzkumu neodpověděly na tuto

[64] Vlastní zdroj.
[65] Hypotéza V: Osoby mladší 15 let a starší 40 let více důvěřují informacím na internetu bez jejich ověření než ostatní.
[66] Hypotéza VI: Více jak 70% osob neověřuje pravdivost informací získaných z internetu.

otázku, bylo zjištěno, že ve skupině osob mladších 15 let a starších 40 let odpovědělo kladně 56 respondentů ze 79 (70,89%) a z ostatních osob odpovědělo kladně 66 z 91 respondentů (72,53%). V procentuálním srovnání více ověřují informace z internetu osoby ve věku 15 – 40 let, což potvrzuje hypotézu V.

K těmto dvěma otázkám bylo ze strany policistky uvedeno, že při přednáškách jsou posluchači upozorňováni, aby ověřovali získané informace a nespoléhali jen na uvedené informace o zdroji, autorovi či jen na samotný obsah. Na vzhled stránek není upozorňováno, jelikož se ze vzhledu stránky nedá nic usuzovat. V souvislosti s tímto faktorem je uváděno podvodné jednání k získání informací k uživateli tzv. „phishing".

Graf 6: Ověřujete informace z internetu – poměr dle věkových skupin[67]



Otázka: „*Se kterými z tvrzení se nejvíce ztotožníte:*" byla zařazena jako ověřovací k předešlým dvěma. Každá z odpovědí byla koncipována tak, aby svým významem potvrzovala předpokládané výsledky hypotéz. Postupně mají tvrzení tento význam (počet odpovědí): neověřuji si informace (10), ověřuji si informace (114), autor informace zcela ovlivňuje její pravdivost (7), zdroj informace zcela ovlivňuje její pravdivost (3), pozadí, na kterém je informace podávána neovlivňuje její pravdivost (6) a obsah informace ovlivňuje její pravdivost (50). Tímto byly potvrzeny výsledky

[67] Vlastní zdroj.

předešlé otázky zabývající se ověřováním informacím, ovšem u zbylých odpovědí není možno konstatovat jakýkoli závěr, jelikož při komparaci odpovědí u jednotlivých dotazníků se ve většině případů respondenti neshodují s odpověďmi z páté otázky. Důvod těchto neshod není jasný a nelze jej určit z dostupných dat.

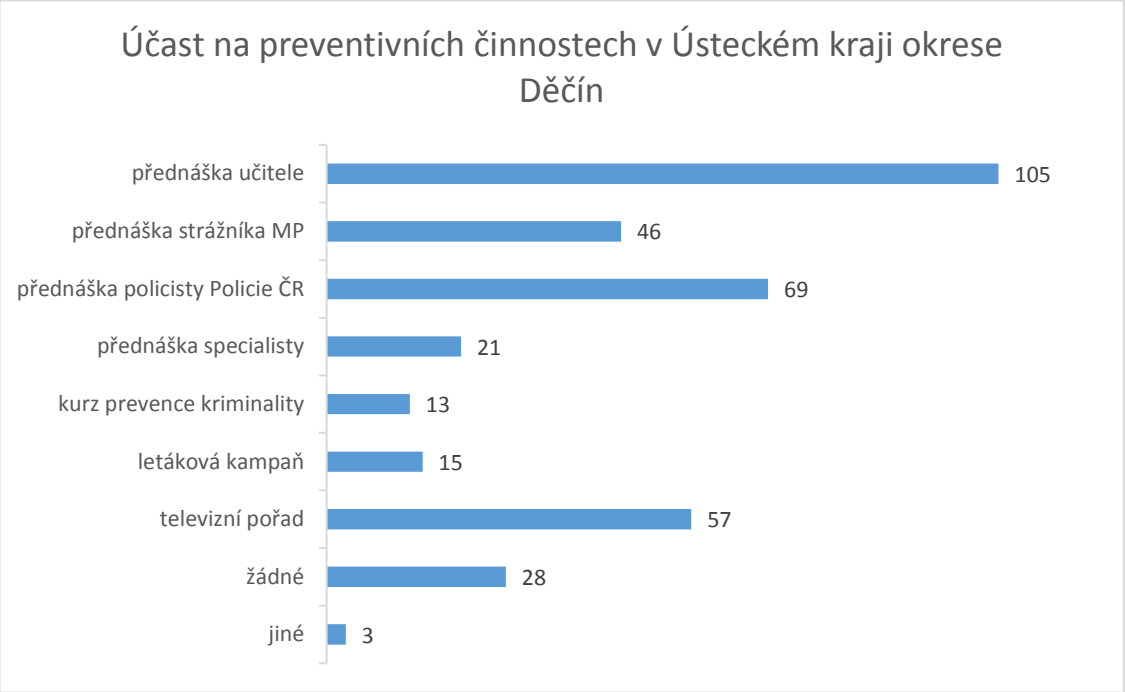
Otázka: „*Které z těchto preventivních opatření počítačové kriminality využíváte v běžném životě:*“ se vztahuje k hypotéze VII[68], kdy nejčastější odpovědí (123 respondentů) byla blokace nežádoucích stránek. Záměrně byly dále vybrány ne zcela známá opatření (certifikáty – 29 odpovědí, elektronický podpis – 6 odpovědí a šifrování komunikace – 28 odpovědí) a ponechána možnost osobám vyjádřit se. Bylo očekáváno mnoho odpovědí ve znění: Antivir, Firewall, Spamový filtr apod., ale pouze 11 respondentů naplnilo toto očekávání. Byly zaznamenány tyto odpovědi: 4 x antivir, 1 x neotvírám neznámé e-maily, 1 x zdroj, blokace podezřelé osoby, 1 x druhé zaheslování, 1 x blokování nežádoucích stahování, 1 x AdBlock, 1 x odmítám spam a neznámý obsah, 1 x ani jedno. Tímto byla prokázána latentnost preventivních opatření situačního charakteru. Spamový filtr dnes užívá každý, kdo má e-mailovou schránku a firewall je obsažen přímo v operačním systému Windows. Logicky by tedy mělo tuto odpověď zvolit o mnoho více lidí, ne-li všichni. Je tedy zřejmé, že kromě jednoho opatření nejsou jiná opatření situační prevence v oblasti počítačové kriminality většině osob známá, čímž byla potvrzena hypotéza VII.

K tomu bylo ze strany policistky uvedeno, že při preventivních činnostech na školách není upozorňováno na prvky situační prevence. Na tyto jsou upozorňovány cílové skupiny rodičů a seniorů formou letáků, v nichž je popisován spíše způsob nastavení nejběžnějších programů.

Hypotéza VIII tvrdí, že v Ústeckém kraji okrese Děčín není prováděna preventivní činnost v oblasti počítačové kriminality. Na nalezení odpovědi byla zaměřena další otázka: Které z těchto preventivních činností v oblasti počítačové kriminality jste se v minulosti zúčastnili. Odpovědi vycházely ze zjištěných preventivních činností uvedených v předchozí kapitole a respondentům byla dána možnost vyjádřit se. Výsledky jsou shrnuty v následujícím grafu.

[68] Hypotéza VII: Situační prevence je latentního charakteru a není většině osob známa.

Graf 7: Účast na preventivních činnostech v Ústeckém kraji okrese Děčín[69]



Je tedy zjevné, že preventivní činnost je v okrese Děčín prováděna, čímž byla vyvrácena hypotéza VIII. Ve 28 případech respondenti uvedli, že se žádné preventivní aktivity nezúčastnili, tyto odpovědi jsou rozloženy téměř rovnoměrně ve věkových skupinách (konkrétně bylo zaznamenáno 6 odpovědí u osob ve věku 11 – 14 let, 3 odpovědi u osob ve věku 15 – 19 let, 10 odpovědí u osob ve věku 20 – 40 let a 9 odpovědí u osob ve věku 40 – 65 let, starší osoby 65 let neodpovídaly, jak je uvedeno již výše). Lze konstatovat, že na všechny věkové skupiny bylo v minulosti v oblasti počítačové kriminality preventivně působeno. 3 osoby uvedli odpověď jiné, kdy 2 x se jednalo o odpověď „přednáška od rodičů“ a jednou bylo uvedeno: „rady od přátel z oboru“.

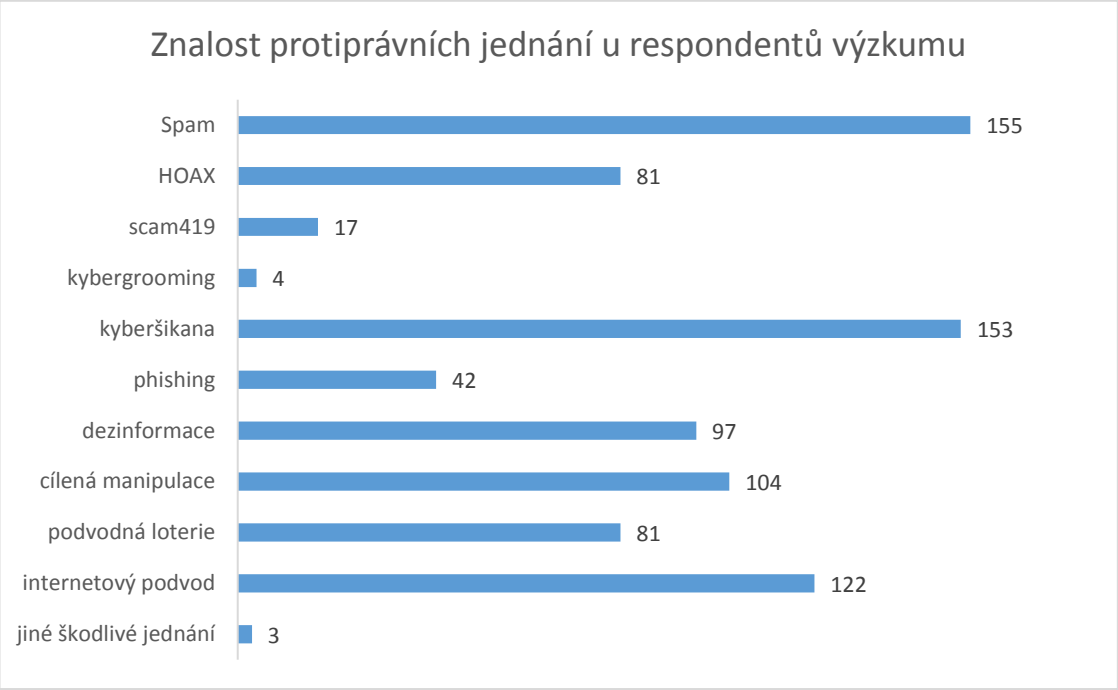
Ke skutečnosti, zda je prováděna preventivní činnost v oblasti počítačové kriminality v okrese Děčín ze strany policie uvedla nprap. Trypesová, že jí realizuje v rámci obecné preventivní činnosti, podle zájmu jednotlivých subjektů. Není tedy pravidelná. Většinou se jedná o přednášky na školách, besedy s cílovými skupinami a prezentaci spojenou s videi zaměřenými na prevenci. Zvláště se osvědčila videa, která jsou šokujícího charakteru, například videa s názvy OVCE.SK nebo Happy slapping. Dále jsou distribuovány mezi cílové skupiny letáky a komiksy. Velice zajímavá je hra s obálkami, na kterých jsou napsány informace získané z profilu uživatele na

[69] Vlastní zdroj.

Facebooku. Na základě těchto informací se žáci rozhodují, zda je pro ně osoba důvěryhodná a jestli by si jí přidali do přátel. Poté otevřou obálku, kde je lísteček se skutečnými údaji osoby. Takto je upozorňováno na skutečnost, že internet je anonymní a nelze věřit všem uvedeným informacím či osobám. Spolupráce se subjekty v rámci místní preventivní činnosti je realizována pouze jednou měsíčně, kdy zasedá komise prevence kriminality. Jsou zde ovšem projednávány možnosti situační prevence netýkající se počítačové kriminality. Jiná spolupráce v okrese Děčín neexistuje.

Otázky: „*Které z těchto jednání znáte a dokázali byste je vysvětlit:*“ a „Víte co znamená pojem „Netiketa“?“ byly zaměřeny na zjištění obsahu prováděných preventivních činností (pravidla Netikety se objevují jako základní kameny prevence počítačové kriminality).

Graf 8: Znalost protiprávních jednání u respondentů výzkumu[70]



Z grafu 8 zachycujícího odpovědi na první z otázek je zřejmé, že nejvíce jsou známy pojmy spam a kyberšikana. Nejméně známým je pojem kybergrooming, který je nebezpečnějším jednáním než internetový podvod, jelikož je cílený na dětské uživatele. V rozhovoru s policistkou bylo zjištěno, že na jednání zvané kybergrooming je při přednáškách upozorňováno, ovšem není uváděn přímo jeho název. Tedy výsledek je ovlivněn spíše neznalostí termínu a ne jeho obsahu. Pouze tři osoby uvedly jiné

[70] Vlastní zdroj.

škodlivé jednání související s internetem, konkrétně „okradení o virtuální měnu“ (řadí se do kategorie internetový podvod), „Internetový predátoři“ (nenalezena žádná shoda se známým protiprávním jednáním, tedy z významu bylo dovozeno, že se jedná o odpověď spadající do kategorie kybergrooming), „falšování dat“ (je možné zařadit do více kategorií), je tedy zjevné, že tyto odpovědi neoznačují jiná jednání než která bylo možné vybrat, pouze je jejich autor (věk 11 – 19 let) neuměl zařadit do správných kategorií. Hypotéza IX[71] byla tedy potvrzena, i když jen o dvě odpovědi.

Netiketa je souborem pravidel chování na internetu, kdy sama o sobě vznikla již v počátcích internetu. Tato pravidla se stala základem preventivní činnosti. Na otázku, zda je v přednáškách prevence kriminality osvětlován pojem Netiketa uvedla policistka, že nikoli a tento pojem nezná. Po vysvětlení tohoto pojmu ovšem doplnila, že pojem jako takový není užíván ani vysvětlován. Mnoho z pravidel Netikety je předkládáno posluchačům jako pravidla chování při práci s internetem, aby se nestaly obětmi trestné činnosti. Při dotazníkovém šetření odpovědělo správně na otázku: „Víte co znamená pojem „Netiketa“?“ celkem 128 osob (75,29%) tedy byla vyvrácena hypotéza XI[72].

Poslední z otázek: „*Stal(a) jste se někdy obětí některého z výše uvedených jednání:*“, zkoumá úspěšnost preventivních činností a opatření. Na tuto otázku bylo možno odpovědět jen kladně či záporně, v případě kladné odpovědi bylo požadováno doplnění názvu protiprávního jednání. Možnost ano zvolilo 57 osob (33,53%). 22 respondentů uvedlo jen pojem „spam“, tedy obětí protiprávního jednání se stalo jen 35 osob (20,59%). Hypotéza X: „Méně jak 50% osob se stalo obětí protiprávního jednání na internetu.“ byla tímto potvrzena. Dále byly uvedeny pojmy: 16 x „HOAX“, 14 x „dezinformace“, 6 x „internetový podvod“, 2 x „podvodné loterie“, „phishing“, „cílená manipulace“, „Scam“. Překvapivou byla odpověď respondenta věku 15 – 19 let: „HOAX – Viděl jste někdy FB stránky politické strany SPD?“. Na tuto otázku nebylo možno odpovědět, vzhledem k anonymitě dotazníku. Stejně neočekávanou byla také informace policistky, že výstupy (statistiky) z preventivní činnosti policie nejsou vedeny, tedy není známo, kolik osob se zúčastnilo přednášek a jiných preventivních aktivit ani kolik z nich se stalo oběťmi protiprávních jednání.

[71] Hypotéza IX: Nejznámějším protiprávním jednáním na internetu je SPAM.
[72] Hypotéza XI: Většina respondentů nezná pojem Netiketa.

Závěr

Při zkoumání základního pojmu „důvěryhodnost“, bylo zjištěno, že se jedná o zcela subjektivní vlastnost informace, kterou hodnotí každá osoba jinak a nelze tedy říci, že je kterákoli informace důvěryhodná pro každého člověka na světě. To platí obecně pro média, zvláště však pro internet, kde je vysoká míra anonymity autora a tím i skoro nulová odpovědnost za poskytované informace. Dále bylo zjištěno, že 55,88% respondentů považuje zdroj uvedený u informace jako faktor ovlivňující důvěryhodnost. 44,70% osob, účastnících se výzkumu, pokládá autora za činitele, který kladně ovlivňuje důvěryhodnost. Výsledek ale není zcela přesvědčivý, jelikož 34,12% osob je opačného názoru. 64,71% dotazovaných hodnotí důvěryhodnost informace podle jejího obsahu a 62,35% nepovažuje za faktor ovlivňující důvěryhodnost vzhled stránky na které je informace prezentována. Bylo prokázáno, že v současné době při posuzování důvěryhodnosti informace, nezáleží na věku, pohlaví či nejvyšším dosaženém vzdělání hodnotící osoby. První čtyři hypotézy tedy byly potvrzeny.

Ze zjištěných informací vyplývá, že důvěryhodnost informací na internetu je úzce spjata s prevencí počítačové kriminality, jelikož je obsažena v základních pravidlech bezpečného chování na internetu. K překvapení autora se v preventivních činnostech užívá i tzv. Netikety, tedy spíše jejího obsahu. Samostatný pojem nebyl znám policistce zabývající se prevencí, ale jeho obsah byl užíván při každé z přednášek. Oproti faktu uváděnému v literatuře a předpokladu autora, že Netiketa je již přežitkem a již byla zapomenuta, odpovědělo 75,29% respondentů, že pojem znají.

Byla zjištěna těsná souvislost mezi důvěryhodností a ověřováním pravdivosti získané informace. Ověřením se pro většinu osob změní nedůvěryhodná informace na důvěryhodnou. Předpoklad autora, že více jak 70% lidí neověřuje informace získané z internetu, byl ve zkoumaném vzorku vyvrácen, jelikož 68,92% odpovědělo, že informace ověřuje. Stejně tak byla vyvrácena hypotéza, že preventivní činnost zaměřená na internetovou kriminalitu související s důvěryhodností informací není na katastrálním území města Děčín prováděna. Ze zkoumaného vzorku odpovědělo jen 16,47% respondentů, že se nikdy nezúčastnilo žádné preventivní činnosti, což je mizivé procento. Pro autora byly nejvíce překvapujícím sdělení policistky zabývající se prevencí kriminality, která uvedla, že pro Policii ČR již není prevence kriminality jednou z priorit. Dále, že neexistuje její primární podoba. Že je samotná preventivní činnost prováděna dobrovolníky u vybraných subjektů a na jejich výslovnou žádost.

A pokud již je prováděna, je nepravidelného charakteru. Zarážející je také, že spolupráce s ostatními subjekty, kromě škol, není v oblasti prevence počítačové kriminality realizována.

K samotné preventivní činnosti bylo zjištěno, že je prováděna formou přednášek na školách, besed s cílovými skupinami, prezentací spojenou s videi zaměřenými na prevenci, letákovou kampaní a distribucí komiksů preventivního charakteru. Zajímavým prvkem, který řadí do přednášek nprap. Trypesová je dle autora hra s obálkami, při které jsou napsány informace získané z profilu uživatele na Facebooku na obálku, dále posluchači na základě těchto informací rozhodují, zda je pro ně osoba důvěryhodná a jestli by si jí přidali do přátel. Po otevření obálky se z vloženého lístečku se skutečnými údaji osoby dozví správnost svého rozhodnutí. Dle slov policistky mají největší úspěch šokující videa a právě tato hra.

Výsledky výzkumu potvrdili i tyto hypotézy z kapitoly 1: Osoby mladší 15 let avstarší 40 let více důvěřují informacím na internetu bez jejich ověření než ostatní., Situační prevence je latentního charakteru a není většině osob známa., Nejznámějším protiprávním jednáním na internetu je SPAM., Méně jak 50% osob se stalo obětí protiprávního jednání na internetu (Vyloučen SPAM, jelikož je zachytáván spamovými filtry, tedy osoby se stávají jeho oběťmi bez možnosti si to uvědomit).

Názorem autora je, že by se měla Policie ČR více zajímat o prevenci kriminality a zařadit jí zpět mezi své priority. Dále by měla být pravidelnou aktivitou více vyčleněných policistů se zaměřením na jednotlivé problematiky (například násilná, mravnostní nebo počítačová trestná činnost). Svým výzkumem se autor pokoušel poukázat na nedostatky v provádění preventivních činností a nepřímo i seznámit respondenty s pojmy, které nejsou moc známy. Dále se domnívá, že by tato práce mohla sloužit k pochopení nedůvěryhodnosti informací a poukázat na nutnost jejich ověřování. Také by mohla přispět k rozšíření a prohloubení preventivní činnosti v oblasti počítačové kriminality.

Seznam použitých zdrojů

Literární zdroje

1. CEJPEK, J. *Informace, komunikace a myšlení.* Praha: Univerzita Karlova v Praze, nakladatelství Karolinum, 2005, 233 s., ISBN 80-246-1037-X.
2. DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, a.s., 2004, 190 s., ISBN 80-251-0106-1.
3. HORÁK, J., KERŠLÁGER, M. *Počítačové sítě pro začínající správce.* Praha: Computer Press, a.s., 2003, 178 s., ISBN 80-7226-876-7.
4. JIROVSKÝ, V. *Kybernetická kriminalita nejen o hacking, cracking, virech a trojských koních bez tajemství*. Praha: Grada Publishing, a. s., 2007, 284 s., ISBN 978-80-247-1561-2.
5. MCCLUNG Jr., F. *Otče, sjednoť nás*. Praha: LOGOS, 1991, 174 s. ISBN 80-85335-06-9.
6. NAUMANN, F. *Dějiny informatiky, Od abaku k internetu.* Přeložila M. Voltrová. Praha: nakladatelství Academia, 424 s., 2009. ISBN 978-80-200-1730-7.
7. NOVOTNÝ, O., ZAPLETAL, J., a kol. *Kriminologie*. 2. přepracované vydání. Praha: ASPI Publishing, 2004. 452 s. ISBN 80-7357-026-2
8. SKLENÁK, V. *Data, informace, znalosti a internet*. Praha: C. H. Beck, 2001, 507 s. ISBN 80-7179-409-0.
9. SVATOŠ, R. *Prevence kriminality.* 1. vydání. České Budějovice: Vysoká škola evropských a regionálních studií, o.p.s., 2014. 132 s. ISBN 978-80-87472-76-7
10. VORÁČEK, R. *Slovník počítačových pojmů a zkratek.* Praha: nakladatelství Fortuna, 1998, 183 s., ISBN 80-7168-590-9.

Časopisy:

1. CHIP*: Magazín o digitálních technologiích.* Německá spolková republika: CHIP Holding, G.m.b.H. vydavatelství Burda Praha, spol. s r.o., 2016, 11/2016, 61-64, ISSN 1210-0684

Elektronické dokumenty:

1. BEZPEČNÝ INTERNET.CZ, *Autorský zákon*, [online], [cit. 2018-01-03]. Dostupné z WWW: <http://www.bezpecnyinternet.cz/skoly/zakony/autorsky-zakon.aspx>
2. CENTRUM PREVENCE RIZIKOVÉ VIRTUÁLNÍ KOMUNIKACE, Pedagogická fakulta Univerzity Palackého v Olomouci, *Kybergrooming* [online], © Centrum PRVoK PdF, Univerzita Palackého v Olomouci 2008 – 2017 ze dne 13. 09. 2008, [cit. 2018-01-03]. Dostupné z WWW: <https://www.e-bezpeci.cz/index.php/temata/kybergrooming/125-42>
3. CZ.NIC, SPRÁVCE DOMÉNY CZ, *Jak funguje DNSSEC* [online], © 2018 CZ.NIC, z. s. p. o., [cit. 2018-02-03]. Dostupné z WWW: <https://www.nic.cz/page/444/jak-funguje-dnssec/>
4. CZ.NIC, SPRÁVCE DOMÉNY CZ*, Projekty pro koncové uživatele* [online], © 2018 CZ.NIC, z. s. p. o., [cit. 2018-03-02]. Dostupné z WWW: < https://www.nic.cz/page/2086/projekty-pro-koncove-uzivatele/>
5. ČESKÁ POŠTA. *Kvalifikované certifikáty, Komerční certifikáty,* [online], © 2010 Česká pošta, [cit. 2018-01-18]. Dostupné z WWW:<http://www.postsignum.cz>
6. ČESKO. MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY. MŠMT: *Školní preventivní program pro mateřské a základní školy a školská zařízení* [online]. MŠMT, 39 s., [cit. 2018-02-03]. Dostupné z WWW: <www.msmt.cz/file/7347_1_1/>
7. ČESKO. MINISTERSTVO VNITRA, odbor prevence kriminality. *Prevence kriminality: Systém prevence kriminality v ČR* [online], Prevence kriminality v České republice © 2018 made by Galileo Corporation s.r.o., [cit. 2018-03-02]. Dostupné z WWW: <http://www.mvcr.cz/clanek/web-o-nas-prevence-prevence-kriminality.aspx?q=Y2hudW09NA%3d%3d>
8. ČESKO. MINISTERSTVO VNITRA, odbor prevence kriminality. *Prevence kriminality na regionální a místní úrovni: Metodiky, doporučení a krajské koncepce prevence kriminality* [online], Prevence kriminality v České republice © 2018 made by Galileo Corporation s.r.o., [cit. 2018-03-02]. Dostupné z WWW: <http://www.mvcr.cz/clanek/prevence-kriminality-na-regionalni-a-lokalni-urovni.aspx?q=Y2hudW09Mg%3d%3d>

9. ČESKO. MINISTERSTVO VNITRA, odbor prevence kriminality. *Tiskoviny,* [online], Prevence kriminality v České republice © 2018 made by Galileo Corporation s.r.o., [cit. 2018-02-03]. Dostupné z WWW: <http://www.prevencekriminality.cz/ke-stazeni/tiskoviny-1/ e-bezpeci-75cs.html>
10. ČÍŽKOVSKÝ, J., KAIZAROVÁ H. *Prevencí k bezpečí,* [online], © 2017 Policie ČR, 31. srpna 2015 [cit. 2018-03-03]. Dostupné z WWW: <http://www.policie.cz/clanek/prevenci-k-bezpeci.aspx>
11. DŽUBÁK, J. & HOAX.cz. *Co je to hoax, Co je to phishing, Co je to SCAM-419, Co jsou to podvodné loterie* [online], ©2000-2017, [cit. 2018-01-16]. Dostupné z WWW: <http://hoax.cz/cze/>
12. FARANA, R. *Teorie informace – podklady pro výuku* [online], [cit. 2017-11-11]. Dostupné z WWW: <www1.osu.cz/~farana1/KodovaniKomprese/01TeorieInformace.ppt>
13. FIŠEROVÁ, K. *Spamový filtr* [online], © 2017 SmartSelling [cit. 2018-03-01]. Dostupné z WWW: <https://www.smartemailing.cz/spamovy-filtr/>
14. INFORMATIKA UČEBNÍ TEXT PDF. *Představujeme Vám pohodlné a bezplatné nástroje pro publikování a sdílení informací.* [online]. Copyright © DocPlayer.cz [cit. 2018-01-11]. Dostupné z WWW: < http://docplayer.cz/848837-Informatika-ucebni-texty-2006.html>
15. KREJČÍ, M. Odborný podklad think-tanku Evropské hodnoty, *Fact checking manuál* [online], 22. 10. 2016, [cit. 2018-01-12]. Dostupné z WWW: <http://www.evropskehodnoty.cz/vyzkum/fact-checking-manual/>
16. KUČEROVÁ, H. dezinformace. In: *KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. Praha, Národní knihovna ČR, 2003 [cit. 2018-01-17]. Dostupné z WWW: <http://aleph.nkp.cz/F/?func=direct&doc_number=000000095 &local_base=KTD>
17. KVÍTEK, L. KATEDRA FYZIKÁLNÍ CHEMIE, PŘÍRODOVĚDECKÁ FAKULTA, UNIVERZITA PALACKÉHO, *Internet a zdroje,* [online], Olomouc, 2005 [cit. 2018-01-18]. Dostupné z WWW: <http://fch.upol.cz/skripta/intz/1-NEW/INTZ.pdf>
18. LINGEA s r.o. nechybujte.cz, správně česky. *Pojem důvěra, hodný*, [online], [cit. 2017-12-27]. Dostupné z WWW: <http://www.nechybujte.cz/slovnik-soucasne-cestiny>

19. SSL MARKET od Zoner software. *SSL certifikáty*, [online], © ZONER software, a.s., [cit. 2018-01-18]. Dostupné z WWW: <https://www.sslmarket.cz/ssl/certifikaty#proc-ssl-market>
20. TUČEK, M., CENTRUM PRO VÝZKUM VEŘEJNÉHO MÍNĚNÍ, Sociologický ústav AV CR, v.v.i. *Důvěra k vybraným institucím veřejného života – říjen 2017,* [online], Naše společnost 27. 11. 2017, [cit. 2018-03-01]. Dostupné z WWW: <https://cvvm.soc.cas.cz/cz/tiskove-zpravy/politicke/politicke-ostatni/4464-duvera-k-vybranym-institucim-verejneho-zivota-rijen-2017>

Zákony:

1. ČESKO. Zákon č. 227 ze dne 29. června 2000 o elektronickém podpisu In: Sbírka zákonů Česká republika. 2000, částka 68. s. 3290 – 3297. [online]. [cit. 2018-01-18]. Dostupné také z WWW: <https://www.psp.cz/sqw/sbirka.sqw?r=2000&cz=227>

Ostatní zdroje:

Kromě výše uvedených zdrojů byly při zpracování bakalářské práce využity následující materiály:

- rozhovor s nprap. Petrou Trypesovou, policistkou Oddělení tisku a prevence, Policie ČR, Krajského ředitelství policie Ústeckého kraje, Územního odboru Děčín, ze dne 1. 3. 2018.

Seznam zkratek

ARPA	- Advanced Research Projects Agency
DES	- Data (Digital) Encryption Standard (šifrovací algoritmus)
DNS	- Domain Name System
FBI	- Federal Bureau of Investigation (federální úřad pro vyšetřování)
FTP	- File Transfer Protokol
HDD	- Hard Disk Drive (pevný disk)
HTTPS	- HyperText Transfer Protocol Secure
IAB	- Internet Advisory Board (Koordinační rada internetu)
ICT	- Information and Communication Technologies (Informační a komunikační technologie)
IDEA	- International Data Encryption Algorithm (Mezinárodní algoritmus pro šifrování dat)
ISOC	- Internet SOCiety (Internetová společnost)
KŘP	- Krajské Ředitelství Policie
LAN	- Local Area Network (místní síť)
MŠMT	- Ministerstvo školství, mládeže a tělovýchovy
NASA	- National Aeronautics and Space Administration (Národní úřad pro letectví a kosmonautiku)
OOP	- Obvodní Oddělení Policie
OTP PČR	- Oddělení Tisku a Prevence Policie ČR
RFC	- Request For Comments
RSA	- Rivest, Shamir, Adleman (šifrovací algoritmus)
SSL	- Secure Sockets Layer
TCP/IP	- Transmission Control Protocol / Internet Protocol (protokol síťové vrstvy)
TELNET	- TELetype NETwork
ÚO	- Územní Odbor
WAN	- Wide Area Network

Seznam grafů a obrázků

Seznam grafů

Seznam obrázků

Přílohy

Příloha I – Použitý dotazník

Příloha II – Letáky dostupné z http://www.prevencekriminality.cz

Příloha I

Dobrý den,

jmenuji se Pavel Bílek, jsem studentem třetího ročníku Vysoké školy Evropských a regionálních studií, obor bezpečnostně právní činnost ve veřejné správě. Jako téma své bakalářské práce jsem si zvolil Důvěryhodnost informací na internetu ve vztahu k prevenci kriminality v Ústeckém kraji, okrese Děčín, kdy praktickou část realizuji dotazníkovou formou. Rád bych vás tímto požádal o vyplnění tohoto dotazníku, který je zcela anonymní, informace z něj získané budou využity pouze pro mou bakalářskou práci a poté budou dotazníky skartovány. Předem děkuji za čas strávený při vyplňování dotazníku.

Při vyplňování dotazníku prosím o označení Vámi zvolené odpovědi křížkem ve čtvercovém poli, od čtvrté otázky můžete vybrat i více možností.

Jsem

□ muž □ žena

ve věku

□ 11-14 let □ 15 – 19 let

□ 20- 40 let □ 41 – 65 let □ starší 65 let

s nejvyšším dosaženým vzděláním:

□ základní □ středoškolské

□ vysokoškolské □ nedokončené základní

a využívám internet:

□ doma □ v práci □ ve škole

□ veřejně přístupné sítě □ v mobilních zařízeních

□ nemám přístup k internetu

□ jiná možnost ……...

Jakou měrou, podle vás, ovlivňuje důvěryhodnost informace na internetu:

	neovlivňuje	spíše neovlivňuje	nevím	spíše ovlivňuje	ovlivňuje zcela
uvedený zdroj	□	□	□	□	□
uvedený autor	□	□	□	□	□
obsah článku	□	□	□	□	□
Vzhled pozadí na kterém je informace podávána	□	□	□	□	□

Ověřujete si pravdivost informace získané na internetu?

□ ano □ ne

Se kterými z tvrzení se nejvíce ztotožníte:

□ Co je na internetu a v televizi je pravdivé.

□ Před přijetím informace jako pravdivé je třeba jí ověřit všemi dostupnými prostředky.

□ K tomu abych uvěřil přijaté informaci, stačí znát jejího autora.

□ K tomu abych uvěřil přijaté informaci, stačí její šíření známou osobností.

□ Informaci, která není prezentována na hezkém pozadí, nečtu.

□ I nepravděpodobný obsah článku může být pravdivý.

Které z těchto preventivních opatření počítačové kriminality využíváte v běžném životě:

□ blokace nežádoucích stránek □ certifikáty

□ elektronický podpis □ šifrování komunikace

□ jiné ……

Které z těchto preventivních činností v oblasti počítačové kriminality jste se v minulosti zúčastnil(a):

□ přednáška učitele □ přednáška strážníka MP □ přednáška policisty Policie ČR

□ přednáška specialisty v oblasti prevence kriminality (soukromá osoba)

□ kurz prevence kriminality □ letáková kampaň □ televizní pořad

□ žádné □ jiné ……

Které z těchto jednání znáte a dokázali byste je vysvětlit:

□ Spam □ HOAX □Scam 419 □KyberGrooming □Kyberšikana

□ Phishing □ Dezinformace □ Cílená manipulace □ Podvodná loterie

□ Internetový podvod

□ jiné škodlivé jednání související s internetem ……

Stal(a) jste se někdy obětí některého z výše uvedených jednání:

□ ne □ ano, kterého ……

Víte co znamená pojem „Netiketa“?

□ Internetová tvorba etiket □ soubor pravidel chování na internetu

□ psychická nemoc □ závislost na internetu

□ neznám tento pojem

Příloha II

HOAX

Co je hoax?

Anglické slovo hoax [houks] v překladu označuje **nepravdivou zprávu, novinářskou kachnu, podvod, výmysl, žert či kanadský žertík.**

V počítačovém světě slovo hoax obvykle znamená **poplašnou zprávu,** která varuje před neexistujícím nebezpečím. Někdy je také označován jako **řetězový dopis,** protože obsahuje výzvu žádající jeho další rozesílání mezi přátele, případně na co největší množství dalších e-mailových adres. U hoaxu je velmi těžké rozeznat, zda je jeho obsah pravdivý. Informace v něm obsažené se zdají být uvěřitelné (např. infikované jehly v tramvaji, AIDS z kontaminovaných potravin, jedovatí pavouci v koupených palmách, vajíčko uvařené mobilním telefonem, jedovaté látky v nápojích a jídle apod.).

Čím vlastně hoax škodí?

1. **Hoax vás obtěžuje a zaplavuje vaše e-mailové schránky.**
2. **Hoax vám nabízí nebezpečné rady.**
3. **Hoax o vás prozrazuje důvěrné informace** (např. e-mail).
4. **Hoax snižuje vaši důvěryhodnost.**
5. **Hoax poškozuje konkrétní firmy** (Coca Cola, Nestlé, Microsoft).
6. **Hoax vyvolává paniku a strach.**

Nikdy hoaxu nedůvěřujte, všechny informace si vždy ověřte!

Příklady hoaxu

Pozor na injekční jehly!

ČR (vír) - Dávejte pozor, na co si sednete! Jde o zdraví i o život! Takové varování putuje po internetu. V textu jsou pak popsány případy, kdy se například návštěvníci kina při usednutí píchli o nastražené injekční stříkačky. Na jehle byl papír se vzkazem: »Právě jsi byl nakažen virem HIV!« Tyto případy se údajně staly v zahraničí i v Praze! Pisatelé v e-mailu tvrdí, že testované jehly opravdu obsahovaly virus HIV nebo žloutenky.

Pozor na infikované injekční stříkačky v tramvajích!

Lidl vás podvádí!

Nalezena kostra obra!

DALŠÍ NEBEZPEČNÉ JEVY

SMS Spoofing

SMS Spoofing [spufin] označuje **zneužití internetu k odesílání falešných SMS zpráv.** Obětí na první pohled nepoznáš, že zpráva, která jí přišla na mobil, byla odeslaná z internetu, protože vjejím mobilním telefonu vypadá stejně, jako zpráva odeslaná z mobilu. Útočník se tak může vydávat za jinou osobu.

SMS Spoofing je v současnosti v ČR blokován všemi mobilními operátory. Poslední výskyt byl zaznamenán v roce 2005.

Phishing

Phishing [fišin] označuje **manipulativní postupy, které prostřednictvím zfalšovaných emailů či www stránek přimějí majitele bankovního účtu vyzradit své přístupové údaje k účtu.** Oběť obdrží e-mailovou zprávu, která ji nutí přihlásit se k bankovnímu účtu. Ve zprávě je uveden odkaz na přihlašovací stránku. Přihlašovací stránka je ale falešná. Pomocí údajů získaných z této stránky se může útočník připojit k bankovnímu účtu oběti, s nímž pak může nakládat jako jeho majitel (např. převést peníze na vlastní účet).

DŮLEŽITÁ ČÍSLA A WWW STRÁNKY

Pomoc online (Internet Helpline)

Telefon: **116 111** či **800 155 555**
E-mail: **pomoc@linkabezpeci.cz**
Chat Linky bezpečí: **xchat.centrum.cz/lb/**
Web: **www.internethelpline.cz**

E-Bezpečí

Web: **www.e-bezpeci.cz**
Web: **www.napisnam.cz**
E-mail: **info@e-bezpeci.cz**

Úřad na ochranu osobních údajů

Web: **www.uoou.cz**
Telefon: **234 665 212**
E-mail: **posta@uoou.cz**

Poradenská linka pro pedagogy

Telefon: **841 220 200, 777 711 439**

bezpečí

NEBEZPEČNÉ JEVY spojené s používáním internetu a mobilních telefonů

Realizováno s podporou Ministerstva vnitra ČR.
Další informace o nebezpečných jevech najdete na **www.e-bezpeci.cz.**

PREVENCE SE MŮŽE VYPLATIT

Projekt E-Bezpečí – Centrum prevence rizikové virtuální komunikace
Pedagogická fakulta Univerzity Palackého v Olomouci, Žižkovo nám. 5, Olomouc, 771 40

Co je to kyberšikana?

Kyberšikana je **šikanování jiné osoby** (ubližování, ztrapňování, obtěžování, ohrožování, zastrašování apod.) **s využitím internetu, mobilních telefonů či jiných informačních a komunikačních technologií**.

Jaké projevy označujeme termínem kyberšikana?

1. **Zasílání urážlivých, zastrašujících, zesměšňujících nebo jinak ztrapňujících zpráv či pomluv** (e-mail, SMS, chat, ICQ, Skype).
2. **Pořizování zvukových záznamů, videí či fotografií, jejich upravování a následné zveřejňování s cílem poškodit zachycenou osobu.**
3. **Vytváření internetových stránek, které urážejí, pomlouvají či ponižují konkrétní osobu** (blogy a jiné www stránky).
4. **Zneužívání cizího účtu** (e-mailového, diskuzního apod.).
5. **Vydírání pomocí mobilního telefonu nebo internetu.**
6. **Obtěžování a pronásledování voláním, psaním zpráv nebo prozváněním.**
7. **A další.**

Případy kyberšikany

Oběť: Ghyslain Raza (14 let, Kanada)

Ghyslain natočil sám sebe při předvádění bojové scény z Hvězdných válek. Spolužáci mu nahrávku ukradli a pro pobavení ostatních ji zveřejnili na internetu. Nahrávka obletěla celý svět, byla mnohokrát upravována, vzniklo množství webů a blogů, na kterých byl chlapec zesměšňován, byl parodován dokonce v seriálech (např. South Park).

Důsledky: Ghyslain se psychicky zhroutil a musel se dlouhodobě léčit.

Oběť: Ryan Patrick Halligan (13 let, USA)

Ryan byl obětí fyzické šikany. Začal se učit kickbox a chlapci, který ho šikanoval, se úspěšně postavil. Hoch ho pak veřejně označil za gaye. Ryan se chtěl této pověsti zbavit, proto navázal internetový vztah s populární dívkou ze školy. Po čase zjistil, že se dívka románkem s ním jen bavila a že jejich důvěrné zprávy přeposílala dalším spolužákům a společně se mu posmívali.

Důsledky: Patrick se oběsil.

Oběť: Anna Halman (14 let, Polsko)

Pět spolužáků podrobilo Annu před celou třídou sexuální šikaně (strhali z ní šaty a předstírali, že ji znásilňují). Celou scénu nahráli na mobil a vyhrožovali jí, že nahrávku zveřejní na internetu, což také později udělali.

Důsledky: Anna spáchala sebevraždu.

Oběť: Megan Meier (13 let, USA)

Megan prožívala několik týdnů virtuální lásku s chlapcem, se kterým se seznámila na internetu. Pak jí chlapec začal psát zprávy plné nenávisti, jak je odporná a jak by byl svět bez ní lepší.

Důsledky: Megan se oběsila.

Při vyšetřování se zjistilo, že **za chlapce se vydávala 50letá matka Meganiny bývalé kamarádky**, a tímto způsobem se jí chtěla pomstít za to, že pomlouvala její dceru.

Co je stalking a kyberstalking?

Kyberstalking [kyberstókin] je **zneužívání internetu, mobilních telefonů** či jiných informačních a komunikačních technologií **ke stalkingu**, což je **opakované stupňované obtěžování**, které může mít různou podobu a intenzitu. Stalker (pronásledovatel) svou oběť například bombarduje telefonáty, SMS zprávami, e-maily, popř. zprávami zasílanými pomocí ICQ, Skypu nebo chatu, posílá jí „dárky", které oběť nechce atd. Nejčastějšími oběťmi stalkingu jsou bývalí partneři, osoby, jež neopětují city stalkera, celebrity, politici apod.

Jaké projevy označujeme termínem stalking?

1. **Opakované a dlouhodobé pokusy kontaktovat oběť** pomocí dopisů, e-mailů, telefonátů, SMS zpráv, zasíláním vzkazů na ICQ, VoIP (např. Skype), v chatu, zasíláním různých zásilek s dárky apod.
2. **Demonstrování moci a síly stalkera** (výhrůžky).
3. **Ničení majetku oběti** (např. oken, auta, domácích zvířat, zasílání počítačových virů apod.).
4. **Stalker označuje sám sebe za oběť.**
5. **Snaha poškodit reputaci oběti** (stalker rozšiřuje o oběti nepravdivé informace v jejím okolí).

Co je kybergrooming?

Termínem kybergrooming [kybergrúmin] označujeme **jednání osoby, která se snaží zmanipulovat vyhlédnutou oběť a řadou psychologických technik ji donutit k osobní schůzce.** Výsledkem schůzky může být sexuální zneužití oběti, fyzické mučení apod. Útočník s obětí komunikuje pomocí informačních a komunikačních technologií, využívá zejména veřejný chat, SMSkování, ICQ a Skype.

Jak probíhá útok?

Útočník (např. manipulátor, deviant) používá postupy, jimiž se snaží získat osobní údaje oběti (jméno, fotografie apod.), aby je mohl následně využít k jejímu vydírání (např. vyhrožuje, že zveřejní fotografie oběti spolu s urážlivým nebo nepravdivým komentářem o její sexuální orientaci).

1. **Etapa vzbuzení důvěry a snaha izolovat oběť od okolí**

   Vždy pochybujte o důvěryhodnosti anonymních uživatelů internetu!
2. **Etapa podplácení dárky či službami, za něž se snaží získat materiály, které lze využít k vydírání oběti**

   Nenechte se podplatit, vaše soukromí a bezpečí je cennější!
3. **Vyvolání emoční závislosti oběti na útočníkovi**

   Nedovolte, aby váš virtuální vztah poškodil vztahy v reálném světě (např. komunikaci s rodiči)!
4. **Osobní setkání**

   Uvědomte si, jak nebezpečná může být schůzka s člověkem, kterého znáte jen z internetu (může vám lhát, vydávat se za někoho jiného)!

Útočník postupuje strategicky. Nenechte se ovlivnit v žádné části manipulace a nikdy neznámému člověku neprozrazujte osobní údaje!

Příklady kybergroomingu

Usvědčený deviant **Pavel Hovorka** (vrátný v tiskárnách) využíval k seznamování s oběťmi několik způsobů – např. chat, inzeráty, v nichž předstíral, že vybírá děti z dětských domovů do soutěže Dítě VIP apod. Osobní informace a fotografie, které od dětí získal, pak použil k vydírání. Kombinací vydírání a uplácení přiměl některé děti k osobní schůzce.

Důsledky: Znásilňování a zneužívání 20 chlapců.

Fotodumentace byla převzata z českých a zahraničních zpravodajských serverů Mediafax.cz, YouTube.com, ABCnews.go.com, Wikipedia.org, Hoax.cz.