Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Internet, snadná a rychlá cesta do Vaší peněženky

Miroslava Kundrtová

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Kundrtová Miroslava

Veřejná správa a regionální rozvoj nav.- Most

Název práce

Internet, snadná a rychlá cesta do vaší peněženky

Anglický název

Internet, easy and quick way to your wallet

Cíle práce

Cílem mé práce je na základě analýzy primárních a sekundárních zdrojů seznámit s podvodnými praktikami vylákávání peněz prostřednictvím internetu a pomocí analýzy dotazníkového šetření respondentů, kteří se s tímto jednáním setkali, zjisit zda lze účinně společnost v této oblasti informovat a zvýšit tak jejich bezpečnost v prostředí internetu. Součástí tohoto řešení bude i vytvoření internetových stránek s preventivním obsahem.

Metodika

Práce se skládá ze dvou částí - teoretické a praktické. Teoretická část bude zpracována na základě analýzy primárních a sekundárních zdrojů. Praktická část bude zpracována na základě dotazníků z kvantitavního/kvalitativního šetření.

Harmonogram zpracování

1. Příprava spojená se studiem odborných informačních ztrojů a upřesnění cílů práce: 05/2013 - 06/2012
2. Zpracování přehledu řešené problematiky dle dostupných informačních zdrojů: 07/2013 - 09/2012
3. Analýza zkoumané technologie: 10/2013 - 11/2013
4. Zpracování a zhodnocení výsledků analýz řešené problematiky: 11/2013 - 12/2013
5. Vytvoření návrhu řešení problematických míst zkoumané technologie: 12/2013
6. Tvorba finálního dokumentu diplomové práce: 01/2014 - 02/2014
7. Odevzdání diplomové práce 03/2014

Rozsah textové části

60 - 80 stran

Klíčová slova

internet, kriminalita, phishing, prevence, facebook, trojský kůň,

Doporučené zdroje informací

Polčák R.. Právo na internet, spam a odpovědnost, Brno, Computer Press, a.s. 2007, ISBN: 978-80-251-1777-4

Gřivna T., Polčák, R. a kol., Kyberkriminalita a právo, Praha, Auditorium 2008, ISBN: 978-80-903-7867-4

Matějka, M. Počítačová kriminalita, Praha, Computer Press, 2002, ISBN: 80-7226-419-2

Lance J., Phishing bez záhad, Grada Publishing 2007, Praha, ISBN: 978-80-247-1766-1

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

Vedoucí práce

Brechlerová Dagmar, RNDr., Ph.D.

Termín odevzdání

březen 2014

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

doc. Ing. Zdeněk Havlíček, CSc.
Vedoucí katedry

prof. Ing. Jan Hron, DrSc., dr. h. c.
Děkan fakulty

V Praze dne 30.10.2013

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Internet, snadná a rychlá cesta do Vaší peněženky" jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 27. 3. 2014 _____

Poděkování

Ráda bych touto cestou poděkovala vedoucí diplomové práce RNDr. Dagmar Brechlerové, Ph.D. za odborné rady a podporu při vedení mé diplomové práce.

Internet, snadná a rychlá cesta do Vaší peněženky

Internet, easy and quick way to your wallet

Souhrn

Tato diplomová práce se zabývá počítačovou kriminalitou. Toto téma je velice rozsáhlé a zahrnuje mnoho různých trestných činů páchaných za použití internetu, já jsem se zaměřila na trestný čin podvodu. Práce je psaná z pohledu policistky pracující na odboru informační kriminality, denně se setkávající s případy podvedených lidí, kdy z převážné většiny se pachatel dostal k penězům poškozených díky nedostatečným znalostem bezpečného chování na internetu a zbytečné důvěřivosti těchto uživatelů. V této práci poukazuji na fakt, že neustále se vyvíjející technická zabezpečení nemají na snížení podvodů přes internet takový vliv, jaký by měla dostatečná informovanost těchto uživatelů.

Summary

This thesis deals with the issue of computer crime. Internet crime is abroad term that is used to identify quite a large number of criminal offenses which are committed on, through or using the internet, I focused my thesis with the offense of fraud. The thesis is written from the perspective of the law enforcement member working at the cybercrime unit which daily encouter with deceived people on the Internet, where the vast majority of this victims was damaged by the perpetrators due to lack of knowledge of safe behavior on the Internet and unnecessary gullibility of those users. In this Thesis, evidenced by the fact, that the constantly evolving technical security does not have influence to reduce fraud over the internet what which should be sufficient awareness for the users.

Klíčová slova: internet, kriminalita, phishing,malware,trojský kůň, horká linka,

Keywords: internet, criminality, phishing, malware, trojan horse, hot line,

Obsah

1 Úvod

Internet je velké médium. Ne už rok od roku, ale téměř hodinu od hodiny se jeho možnosti zvyšují a jeho význam roste. Nebudu lhát, když napíšu, že život bez něj už si jen těžko dovedeme představit. Využíváme jeho možnosti mnozí tak často, že to již hraničí se závislostí. Já sama nosím náramek, který mi měří kroky, kvalitu spánku, dokonce mi určuje i správný čas toho, kdy se mám probudit. Všechny tyto údaje pak odesílá prostřednictvím internetu, abych mohla získat zpětnou vazbu o tom, jak zdravě či nezdravě jsem prožila minulý týden. Jiné aplikace vyhodnocují mé cvičení a posílají mi upozornění, že je čas se začít hýbat. Na internetu nakupuji, obchodníkům platím prostřednictvím platebních karet, využívám internetové bankovnictví. Prostřednictvím internetu vykonávám svoji práci i obstarávám povinnosti do školy. Internet se stal součástí našeho života. Pokud by se někdo rozhodl ovládnout mou digitální identitu, dozví se o mém životě úplně vše. Když pominu nepříjemnost toho, že o mně někdo ví víc, než moji nejbližší, je zde také hrozba, že takto získané informace zneužije. Mnohdy si totiž ani neuvědomujeme jak tenká je hranice našeho soukromí a bezpečí a jak snadno ji „pachatel“ může překročit.

„*Stalo se děsivě jasné, že naše technologie překročila naše lidství“* (Albert Einstein).

Pracuji na Úřadu služby kriminální policie a vyšetřování, Odboru informační kriminality. Denně se setkávám s novými případy lidí, kteří prostřednictvím internetu přišli o své peníze. Mají-li tyto činy něco společného je to využití nejslabšího článku v jinak dost pevném bezpečnostním „řetězu“. Můžete mít nejnovější antivirový systém, neprostupný firewall, bezpečný router, zakryptovaná citlivá data, ale ani to vás neochrání před odcizením peněz prostřednictvím internetu, protože tím nejslabším článkem je člověk. Průměrný uživatel internetu, který dřív nebo později část svých peněz pachateli v dobré víře odevzdá.

Ve své práci se nebudu zabývat trestnými činy spáchanými prostřednictvím internetu, kde pachatelé technickým způsobem překonali přístupové údaje a pronikli tak například na bankovní účet, ale trestnými činy, kde k tomu, aby pachatel mohl získat uživatelovo peníze, potřeboval jeho spolupráci, alespoň částečnou. Popíšu tedy praktiky, které zneužívají naivitu či neznalost běžných uživatelů internetu a ti dobrovolně a nevědomky tak otevírají své elektronické peněženky. Zastávám totiž názor, že ačkoliv je internet nebezpečný, tak správná a dostatečná informovanost a následná opatrnost uživatelů by trestné činy páchané prostřednictvím internetu značně omezila.

V této práci se chci pokusit svůj názor prokázat jako správný a zjistit v čem informovanost lidí v téhle oblasti selhává, ačkoliv se státní i nestátní informace snaží tento negativní jev napravit. Věřím, že postupem času se internetová gramotnost lidí změní k lepšímu a budou si své finance lépe chránit a ne je tak snadno odevzdávat podvodníkům.

„*Není to víra v technologii, je to víra v lidi*“ (Steve Jobes).

2 Cíl práce a metodika

2.1 Cíl práce

Cílem této diplomové práce je prostřednictvím analýzy primárních a sekundárních zdrojů, zejména z odborné literatury a osobních zkušeností při výkonu mé profese seznámit čtenáře se současnou situací internetové kriminality, konkrétně podvodů spáchaných prostřednictvím internetu, ke kterým dochází nedostatečnou informovaností uživatelů nakupujících zboží přes internet či jiným způsobem transferujících svých peněz přes internet a poukázání na skutečnost, že zatímco se zvyšuje technické zabezpečení počítačových systémů a možnosti využití internetu, nezvyšují se vědomosti uživatelů.

2.2 Metodika zjišťování a zpracování dat

Pro řešení problematiky mé diplomové práce jsem jako metodiku zvolila studium a analýzu odborných informačních zdrojů týkajících se informační kriminality a poznatků získaných při výkonu mé profese, která mimo jiné spočívá v přijímání, analýze a následném zpracování poznatků týkajících se kyberkriminality přijatých prostřednictvím tzv. horké linky provozované Policií České republiky.

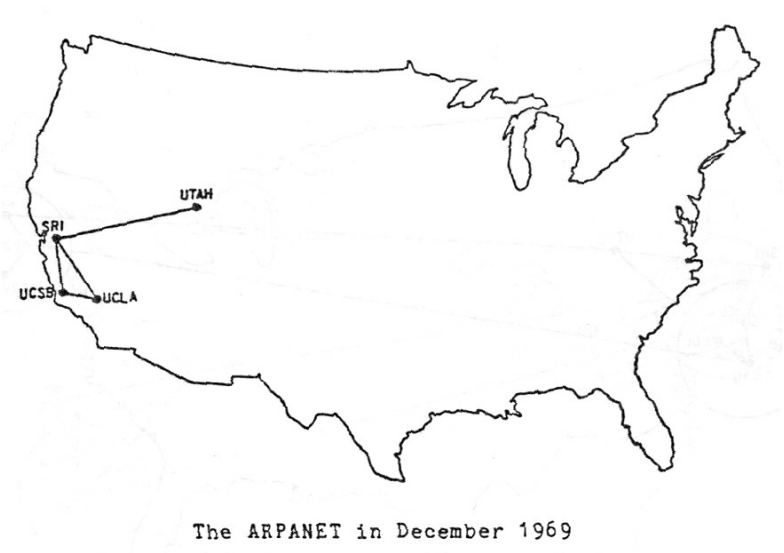
Praktická část zaměřena na provedení a vyhodnocení kvantitativního výzkumu vedeného formou anonymního dotazníkového šetření u 84 respondentů, kdy cílem tohoto kvantitativního průzkumu je ověření dvou stanovených hypotéz: 1) Mezi muži a ženami není rozdíl ve znalostech bezpečného užívání internetu, 2) Mezi věkovými generacemi není rozdíl ve znalostech bezpečného užívání internetu. Následně jsem provedla analýzu konkrétního podvodu spáchaného prostřednictvím internetu u jednoho z respondentů, jednalo se tedy o kvalitativní sběr dat za účelem ukázání konkrétního postupu spáchání podvodu a následného popisu chyb v počínání uživatele. V závěru praktické části této diplomové práce jsem provedla analýzu současné situace v oblasti vzdělávání uživatelů internetu v jeho bezpečném užívání se zaměřením na školní instituce a média.

3 Teoretická východiska

3.1 Historie internetu

Internet je komunikační síť, která propojuje navzájem počítačové sítě po celém světě prostřednictvím sady protokolů TCP/IP.

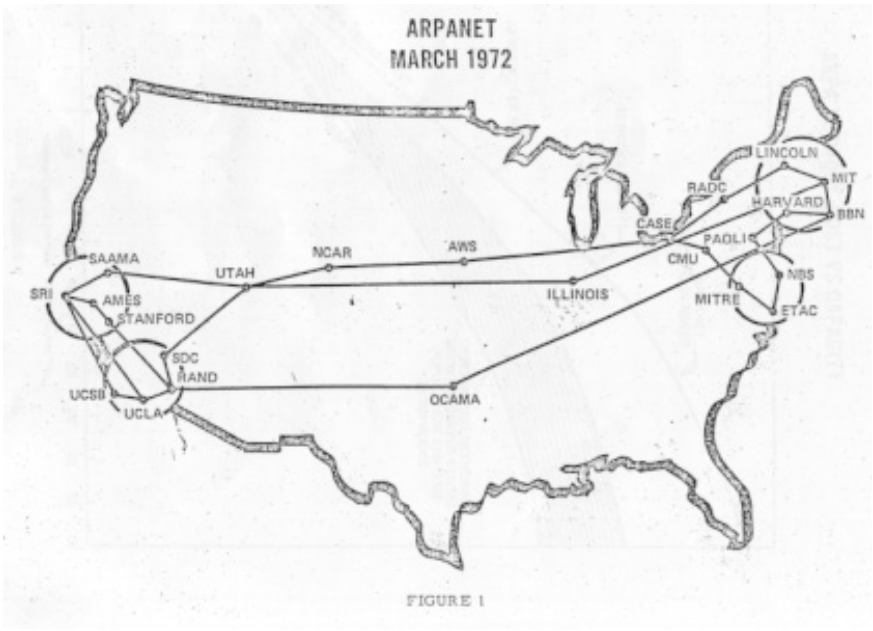
Za prvního předchůdce internetu je považována počítačová síť instalována v Národní výzkumné laboratoři ve Velké Británii, ale tato síť byla funkční pouze v budově této výzkumné laboratoře. Za první síť, která byla užívána mimo jednu budovu, je považována síť s názvem ARPANET. Tato síť byla vytvořena americkou vládní agenturou Advanced Research Projects Agency (ARPA) a sloužila především pro vojenské a vládní účely. Tato síť neměla žádnou centrální složku, aby zůstala funkční i v případě, že by některé její části byly zničeny. Základem této sítě se v roce 1969 staly počítače na čtyřech univerzitách – UCLA (University of California Los Angeles), SRI (Stanford Research Institute), UCSB (University of California Santa Barbara), Universtity of UTAH *(viz. obr. 1)*. Pro vzájemnou komunikaci mezi uzly byl tehdy používán protokol NCP (network Control Protocol).



Obrázek 1 Síť Arpanet, prosinec 1969[1]

Komunikační uzly začaly během let postupně přibývat a propojovat celé území USA. V roce 1970 již stoupl počet těchto uzlů ze čtyř na 13 a v roce 1972 již bylo těchto komunikačních uzlů 29 *(viz. obr. 2)*. V roce 1983 byl NCP definitivně nahrazen protokoly TCP/IP.[2]

[1] http://mercury.lcs.mit.edu/ , 15. 12. 2013
[2] *cs.wikipedia.org*



Obrázek 2 Síť Arpanet, březen 1972[3]

Nejpoužívanějšími službami internetu jsou WWW (World Wide Web) stránky a emailová služba. Abychom mohli internet používat v podobě jako teď, bylo vynalezení služby WWW stránek opravdu převratné. Tento vynález usnadnil přístup k užívání internetu běžným uživatelům po celé planetě. Předchozí možnost využívání internetu spočívala pouze v přenosu souborů přes FTP a ve využívání emailové služby. V roce 1989 Evropská organizae pro jaderný rozvoj dostala nápad vymyslet technologii s jejíž pomocí by mohli vědci mezi sebou komunikovat na internetu snadněji. Otec WWW stránek Tim Berners-Lee, syn britských matematiků a vědců Mary Lee Woods a Conway Berners-Lee navrhl, že by jednotlivé dokumenty umístěné v počítačích mohly na sebe odkazovat a být seřazeny v organizované struktuře. V roce 1990 vytvořil Berners-Lee prohlížeč společně se základy hypertextového protokolu http a jazyka HTML. Tento první internetový prohlížeč nazval „WorldWideWeb.app“ a použil ho na počítači NeXT. Jen pro zajímavost Steve Jobs na nějakou dobu opustil tehdy společnost Apple, aby vytvořil společnost NeXT, která tyto počítače začala vyrábět. Na konci roku 1990 pak Berners-Lee spustil první webový server info.cern.ch. Od roku 1993 umožnila organizace CERN užívání této technologie ostatním lidem a zcela zdarma. Od poloviny roku 1994 vzniklo WWW Consorcium (W3C), jehož členy je několik členských organizací, které společně s veřejností schvalují webové standardy

[3] *www.packet.cc, 15. 12. 2013*

a dohlížejí na rozvoj této služby. V tomto roce 2014 je tomu přesně 25 let, co tento návrh Berners-Lee CERNu předal.

Webové stránky se rozvíjí obrovskou rychlostí a tak od jedné webové stránky z roku 1991 jich v roce 2013 bylo přes 700 milionů. Tento počet ovšem neustále stoupá a tak ke dni 23. 3. 2014 jich bylo už 926 564 000, s tím, že každou další vteřinu přibude další webová stránka.

Vzhledem k tomu, že se síťová informační struktura začala původně vyvíjet ve Spojených státech amerických, přebírá celosvětová informační společnost z větší části v těchto státech platné modely práva na internetu. Zde je nutno podotknout, že právě ve Spojených státech je liberální přístup k regulacím. Ve Spojených státech amerických je zejména uzákoněna a uplatňována svoboda projevu, která je uvedena v prvním dodatku Ústavy. Přesto některé zákony používané v prostředí internetu jsou ve Spojených státech přísnější než u nás. Například stahování filmů a hudby. V duchu odstranění nejrůznějších forem regulace omezující jednotlivce v realizaci jeho záměrů a dosažení prospěchu se nesou aktivity hnutí za „svobodný internet“ organizace Electronic Frontier Foundation, jejímž zakladatelem je John Perry Barlow. Tato organizace vznikla v roce 1990 a velice výrazně se zapojuje do soudních sporů ve formě právní pomoci proti omezování jedince na internetu. Jejich základním dokumentem je „Deklarace nezávislosti kyberprostoru“.

3.2 Deklarace nezávislosti kyberprostoru

„Vy vlády všech průmyslových světů, Vy unavení obři z masa a oceli. Já přicházející z Kyberprostoru, nového sídla Mysli, Vás v zájmu budoucnosti vyzývám: Nechte nás být! Nejste mezi námi vítáni. Nemáte žádnou moc nad místy, kde pobýváme.

Nemáme vládu, ani žádnou nechceme. Mluvím k Vám tedy z pozice autority ne větší, než jakou má sama Svoboda. Vyhlašuji, že globální společenství, jež budujeme, nezávisí na tyranii a zákazech, kterými jste nás svázali. Nemáte morální právo nás řídit a nemáte ani nástroje, kterých bychom se museli obávat.

Dovoláváte se problémů okolo nás a říkáte, že je potřeba je řešit. Používáte je k ospravedlňování svých výpadů vůči nám. Mnoho z nich však neexistuje. Když se objeví skutečný konflikt, nebo jiná špatnost, poznáme to a vyřešíme to vlastními nástroji. Máme novou společenskou smlouvu. Taková vláda se nezakládá na podmínkách Vašeho světa, ale toho našeho a ten je jiný.

Pojmy Vašeho práva jako jsou vlastnictví, vyjadřování, subjektivita, pohyb nebo okolnosti se na nás nevztahují. Všechny jsou založeny na hmotné podstatě a u nás žádná hmotná podstata není.

Nemáme těla a na rozdíl od Vás se řád mezi námi vytváří prostřednictvím násilí. Věříme v nastolení pořádku díky etice, osvícenému individualismu a smyslu pro všeobecné blaho. Můžeme se volně přemisťovat mezi Vašimi jurisdikcemi a tak jediné pravidlo, které skutečně ustavuje naše společenství, je zlaté pravidlo morálky. Na tomto základě chceme řešit všechny problémy a nepřijímáme způsoby, které se nám snažíte vnutit.

Založíme v kyberprostoru novou civilizaci Mysli. Snad bude humánnější a spravedlivější než svět, který Vaše vlády doposud vytvořily.“ (Text převzat a přeložen z internetové stránky www.homes.eff.org/-barlow/Declaration-Final.html)

3.3 Kriminalita na internetu

3.3.1 Definice počítačové kriminality

Vymezit pojem počítačové kriminality není vůbec jednoduché. V každé publikaci týkající se tohoto tématu nalezneme trochu jinou definici. Vše závisí zejména na různých druzích pohledu těchto autorů. Jednu z prvních definic v České republice prezentoval v roce 1995 Prof. Ing. Vladimír Smejkal, CSc., který ji označil jako páchání trestné činnosti, v níž figuruje počítač jako souhrn hardwarového a softwarového vybavení, data nevyjímaje, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako movité věci nebo jako nástroj trestné činnosti.[4]

Václav Jirovský definoval počítačovou kriminalitu jako pojem používaný i pro tradiční formy kriminality, u níž byly počítače nebo počítačové sítě použity, aby ji usnadnily. Určujícím operacionálním elementem je přitom vždy způsob zneužití výpočetní techniky, vzhledem k jejím specifickým vlastnostem a dominantnímu postavení mezi věcnými komponentami způsobu páchání konkrétního trestného činu.[5]

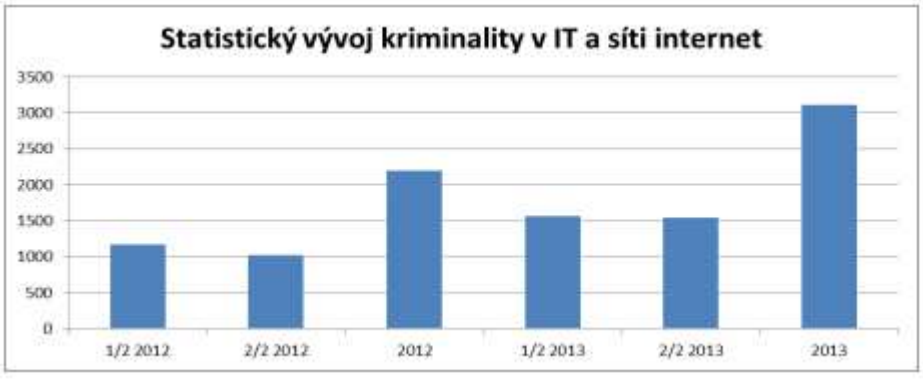
[4] *Smejkal V., Sokol T., Vlček M, Počítačové právo,*
[5] Jirovský V., Kybernetická krimalita,

Definice počítačové kriminality, akceptovaná v rámci Evropské unie zní: Počítačová kriminalita je nemorální a neoprávněné jednání, které zahrnuje zneužití údajů získaných prostřednictvím informačních a komunikačních technologií nebo jejich změnu.

Dále je používán pojem informační kriminalita, který je definován jako trestná činnost, pro kterou je určující vztah k software, k datům, respektive uloženým informacím, respektive veškeré aktivity, které vedou k neautorizovanému čtení, nakládání, vymazání, zneužití, změně nebo jiné interpretaci dat.[6]

3.4 Popularita kyberkriminality

Proč je kriminalita na internetu tak populární a v průběhu let počet trestných činů spáchaných prostřednictvím internetu stoupá geometrickou řadou? Výhody kriminality páchané na internetu oproti kriminalitě páchané tzv. tváří v tvář můžeme vidět na srovnání ozbrojeného přepadení a kybernetického útoku, které uveřejňuje ve své knize Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství Václav Jirovský. Ten ve své knize uvádí, že při průměrném ozbrojeném přepadení co se týká rizika s ohledem na zdraví a život riskuje pachatel, že budete zraněn, případně zabit, při kybernetickém útoku mu žádné fyzické zranění nehrozí. Zisk získaný z ozbrojeného přepadení bývá v průměru 3 až 5 tisíc USD, při kybernetickém útoku od 50 do 500 tisíc USD. Pravděpodobnost dopadení policií bývá u ozbrojeného přepadení 50 – 60% u kybernetického útoku cca. 10 %.



Obrázek 3 Vývoj kyberkriminality[7]

[6] Požár J., Trendy počítačové kriminality a kyberterorismu
[7] ESSK (Evidence statistického systému kriminality)

Sečteme-li škody všech skutků spáchaných prostřednictvím internetu v roce 2013, dosáhneme částky 238 344 400,- Kč. Tedy přes čtvrt miliardy korun. Tato částka bude ale ve skutečnosti vyšší, neboť trestné činy spáchané přes internet nahlásí jen část poškozených. Policii České republiky se z těchto činů podaří objasnit necelých 43% nahlášených skutků.

3.4.1 Členění počítačové kriminality

Členění počítačové kriminality jako souhrn jednání, která mají souvislost s informačními systémy, a které je možné kvalifikovat jako protiprávní jednání podle trestního práva hmotného České republiky, uvádí ve své publikaci Právo informačních a telekomunikačních systémů Smejkal, kdy trestnou činnost rozdělil do těchto subkategorií:

- Trestné činy ve vztahu k hmotnému majetku – klasická majetková trestná činnost.
- Trestné činy ve vztahu k nehmotnému majetku – kriminalita ve vztahu k programům a databázím.
- Trestné činy, při nichž je počítač prostředkem k jejich páchání (v možném souběhu s předchozí položkou), obvykle se jedná o hospodářskou kriminalitu – podvody a zpronevěry.

3.4.2 Rozdělení počítačové kriminality dle Rady Evropy

Rozdělení počítačové kriminality dělí Rada Evropy do čtyř oblastí:

- Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů (neoprávněný přístup, neoprávněné odposlouchávání, narušování dat, narušování systémů, zneužívání zařízení).
- Trestné činy se vztahem k počítači (počítačový podvod, padělání počítačem).
- Trestné činy se vztahem k obsahu počítače (dětská pornografie).
- Trestné činy související s porušováním autorského práva[8].

Dále Rada Evropy rozšířila tento okruh o čtyři skutkové podstaty xenofobních a rasově motivovaných deliktů. Tyto delikty přísluší pod „Trestné činy se vztahem k obsahu počítače“.[9]

[8] *Council of Europe, Convention on Cybercrime, Budapest, 2001*

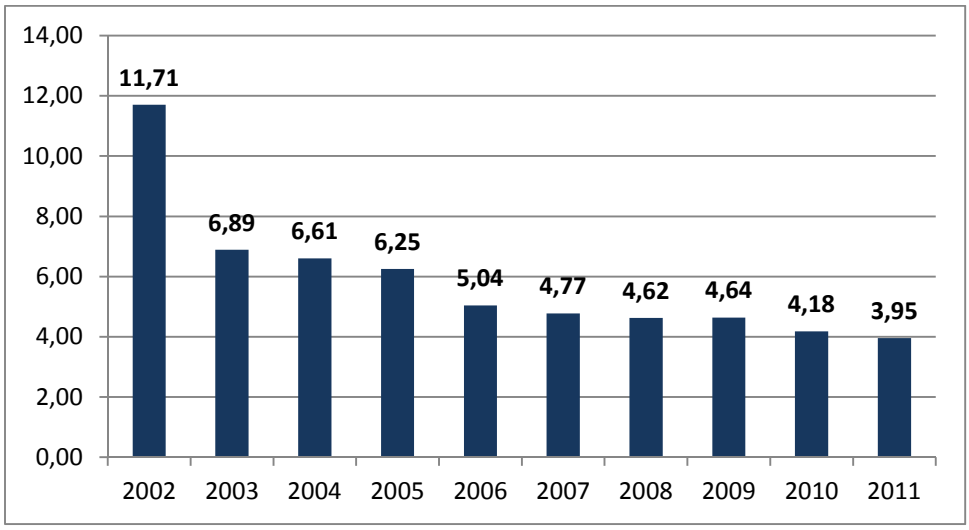
[9] *Council of Europe, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts a racist and xenophobic nature commited through komputer systems, Strasbourg, 2003*

3.4.3 Trestný čin podvod

Počítačový podvod není v trestním zákoníku samostatně specifikován a je zahrnut pod trestný čin podvod. Trestný čin podvodu je v trestním zákoníku, zák. č. 40/2009 Sb., podrobněji rozepsán pod § 209. Zde je jako podvodník popsán ten, kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou.

Ve statistice TSK za období od roku 2002 do roku 2011 je vidět značný pokles. Jak je zobrazeno v grafu na obrázku č. 4 dosahoval index registrovaných trestných činů podvodu v roce 2002 11,71 skutků na 10 000 obyvatel. Hned v roce 2003 je patrný výrazný pokles celkem o 41,14 % na hodnotu již jen 6,89 skutků na 1000 obyvatel. Tato klesající tendence avšak ne již v takovém rapidním poklesu pokračovala až do roku 2011.

Trestný čin podvodu nespadá do kategorie latentní kriminalita. Orgány činné v trestním řízení ji tedy nemusejí vyhledávat, ale bývá převážně oznamován poškozenými. Z tohoto faktu vyplývá, že zmiňovaný pokles tohoto trestného činu byl pravděpodobně způsoben poklesem spáchaných podvodů. Tato skutečnost by mohla nasvědčovat tomu, že lidé jsou již v oblasti podvodů vzdělanější a ke svému majetku opatrnější než byli v roce 2002.

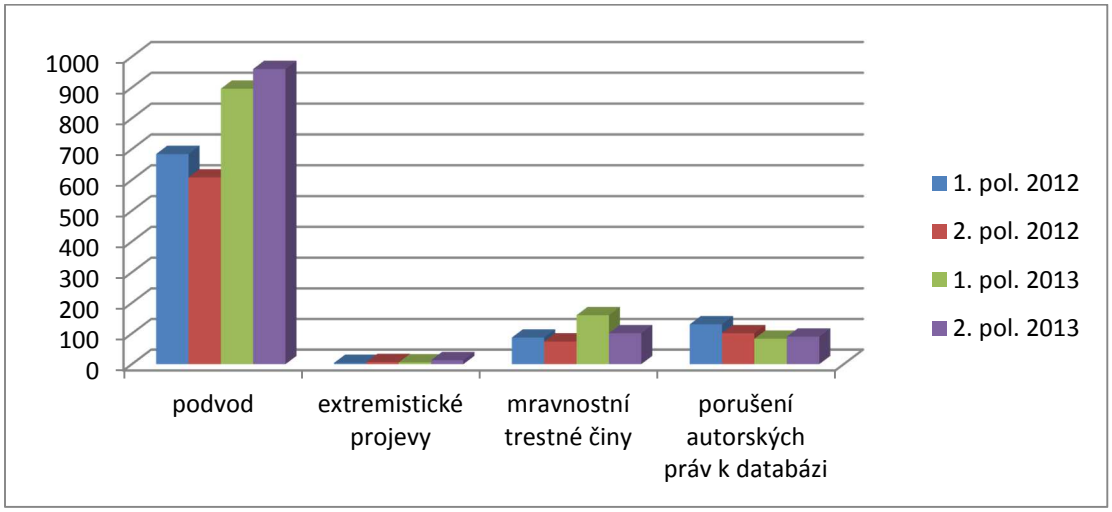


Obrázek 4 Vývoj registrovaných trestných činů spadajících pod TSK podvod v ČR v letech 2002 - 2011, počet činů na 1000 obyvatel[10]

[10] ESSK (evidence statistického systému kriminality)

Tato čísla hovoří příznivě, avšak právě podvody spáchané prostřednictvím informačních technologií mají tendenci opačnou a jejich výskyt naopak stoupá. Na neustálém vzestupu jsou zejména formy podvodů v podobě phishingu, které se šíří plošným rozesíláním spamů.

Celkem bylo za rok 2013 prostřednictvím sítě internet spácháno a nahlášeno 3 108 trestných činů. Z tohoto počtu tvořily různé formy podvodů 1740 činů. Je to tedy více jak 50% spáchaných a nahlášených internetových trestných činů. Na druhém místě je pak trestný čin neoprávněný přístup k počítačovému systému a nosiči informací, který činil 196 činů.



Obrázek 5 GRAF znázorňující vybrané trestné činy prostřednictvím internetu za období 2012 - 2013[11]

3.5 Právní stránka řešení internetové kriminality

3.5.1 Právní normy regulující kyberprostor

Právních norem regulující kyberprostor existuje větší množství. Pro účely této diplomové práce vyjmenuji jen některé, ty které považuji za stěžejní. Z hlediska Evropské unie jsou to:

- Úmluva Rady Evropy č. 185 o kyberkriminalitě
- Dodatkový protokol k Úmluvě o kyberkriminalitě
- Směrnice Rady 91/250/EHS o právní ochraně počítačových programů
- Rozhodnutí Rady 92/242/EHS o bezpečnosti informačních systémů
- Rámcové rozhodnutí Rady 2001/413/SVV o potírání podvodů a padělání bezhotovostních platebních prostředků
- **Směrnice Evropského parlamentu a Rady 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně**

[11] Ministerstvo vnitra České republiky, www.mvcr.cz

dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí.

Z pohledu České republiky jsou to zejména:

- Zákon č. 40/2009 Sb., trestní zákoník
- Zákon č. 141/1961 Sb., o trestním řízení soudním
- Zákon č. 160/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 227/2000 Sb., o elektronickém podpisu
- **Návrh zákona o kybernetické bezpečnosti**

V létě roku 2013 Česká republika zároveň ratifikovala budapešťskou Úmluvu o počítačové kriminalitě, která je platná od 1. 12. 2013. Jedná se o dokument Rady Evropy, který do dnešního dne podepsalo 51 států a ratifikován byl již ve 40ti z nich. Jejím užitkem je zejména sjednocení skutkové podstaty trestných činů tak, aby je bylo možno stíhat na mezinárodní úrovni.

3.5.2 Směrnice Evropského parlamentu a Rady 2006/24/ES o uchovávání údajů …

V prostoru internetu je uchováváno velké množství dat o pohybu jednotlivých počítačů / uživatelů v tomto prostoru. Každý krok za sebou zanechává nějakou stopu. Tato Směrnice Evropského parlamentu ze dne 15. 3. 2006 obsahuje mimo jiné tento text:

„Vzhledem k významu provozních a lokalizačních údajů pro vyšetřování, odhalování a stíhání trestných činů, jak názorně dosvědčují výzkum i praktické zkušenosti několika členských států, je nutné na evropské úrovni zajistit, aby se po určitou dobu a za podmínek stanovených v této směrnici uchovávaly údaje vytvářené a zpracovávané poskytovateli veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí při poskytování komunikačních služeb.“

Informace o uživatelích, tedy informace o přístupech uživatelů a jejich pohybu na internetu jsou totiž jedním ze základních stop, které mohou být využity při boji proti kyberkriminalitě. Bez těchto údajů od poskytovatelů internetu je často nemožné vypátrat pachatele této činnosti. V praxi ne všichni poskytovatelé policii tyto informace ochotně sdělují a často se chrání tvrzením, že data o přístupu uživatelů neuchovávají.

3.5.3 Návrh zákona o kybernetické bezpečnosti

Návrh zákona o kybernetické bezpečnosti v roce 2013 úspěšně prošel mezirezortním připomínkovým řízením. Dne 2. 1. 2014 byl schválen Českou vládou. Zákon by měl začít platit od 1. 1. 2015. Jedná se o normu, která je vypracována Národním bezpečnostním úřadem. Cílem této normy je zefektivnit reakce na kybernetické hrozby, které by mohly představovat nebezpečí pro zájmy České republiky a zároveň zvýšit spolupráci mezi soukromým sektorem a veřejnou správou v prevenci proti útokům na informační technologie. V České republice jde o první komplexní právní úpravu v této oblasti. Pokud tento návrh ratifikuje parlament a podepíše prezident, bude Česká republika jednou z prvních zemí, která bude mít kybernetickou bezpečnost upravenou zvláštní právní normou.

Tento návrh byl připravován ve spolupráci s několika státními institucemi a zejména pak s Národním bezpečnostním úřadem (NBÚ), který je na základě usnesení vlády ČR č. 781 ze dne 19. 10. 2011 gestorem a národní autoritou pro tuto oblast.

K tomuto zákonu se zároveň váže i „vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních protiopatřeních a o stanovení náležitosti podání v oblasti kybernetické bezpečnosti“. Tato vyhláška je v současnosti dokončována mezirezortní pracovní skupinou pod vedením NBÚ.

Tato norma si dává za cíl dvě zásady. První z nich je minimalizace zásahu do práv soukromých i právnických osob a druhým je individuální odpovědnost za bezpečnost vlastních informačních systémů. Nejdůležitějším posláním tohoto zákona je dle Aleše Špidly, povinnost poskytovatelů elektronických komunikací či správců kritické informační infrastruktury informovat Nejvyšší bezpečnostní úřad o případných incidentech, ale také spolupráce mezi jednotlivými subjekty, které se na bezpečnosti kybernetického prostoru Česka podílí. Případné sankce pro organizace, které nezajistí požadované bezpečnostní standardy, jsou pro fyzické osoby ve výši 50.000,- Kč, pro právnické osoby 100.000,- Kč. Je otázkou, nakolik jsou tyto částky dostatečně odstrašující a pro dané subjekty motivační. Nad dodržením tohoto zákona bude mít pro soukromou a akademickou sféru dohled Národní CSIRT (Computer Security Incident Response Team) a pro státní instituce a kritickou informační strukturu Vládní CERT České republiky (Computer Emergency Response Team).

Dle § 97 tohoto zákona má právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinnost uchovávat po dobu 6ti měsíců provozní a lokalizační údaje. Zároveň má ovšem povinnost,

aby při plnění povinnosti uchovávání provozních a lokalizačních údajů nebyl uchován obsah zpráv a takto uchovávaný dále předán. Jde tedy o jakýsi kompromis.

Tyto informace má povinnost poskytnout orgánům činným v trestním řízení pro účely a při splnění podmínek stanovených zvláštním právním předpisem, Policii České republiky pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě, zjištění totožnosti osoby, nebo totožnosti neznámé mrtvoly, předcházení odhalování konkrétních hrozeb v oblasti terorismu nebo prověřování chráněné osoby a dále také při splnění podmínek stanovených zvláštním právním předpisem.

3.5.4 Místní příslušnost

V kyberkriminalitě nejčastěji dochází k případům, kdy se samotný skutek odehraje na území jednoho státu, avšak jeho účinky nastanou na území státu jiného, je to tzv. distanční delikt. V takovém to případě je možné stíhat pachatele v obou místech. V tomto případě nastává situace, kdy dochází k tzv. mezinárodní spolupráci mezi policiemi jednotlivých zemí. Tato spolupráce je zpravidla hlavně časově náročná a rozhodně ne efektivní. Z tohoto těží hlavně pachatel, který tak má dostatek času na páchání další trestné činnosti či zahlazování stop. Tyto situace nastávají bohužel u trestných činů páchaných přes internet velmi často.

Pro zefektivnění vyšetřování téhle trestné činnosti by tak pomohlo zavedení koncepce nikoli fyzické, ale tzv. „efektivní“ přítomnosti pachatele na území určitého státu. Orgány činné v trestním řízení tak toto řízení obvykle vedou i v případech, kdy se na území jejich jurisdikce pachatel v době spáchání trestného činu nenacházel, ani zde přímo ke spáchání trestného činu nedošlo, ale kde se projevil nebo mohl se projevit efekt trestného jednání. V Praxi kyberkriminality je však častější, že trestní řízení konají orgány na území, kde se pachatel aktuálně zdržuje. Výjimkou z této praxe je Úmluva Rady Evropy o kyberkriminalitě. Členské státy se v této Úmluvě zavázaly provést legislativní opatření, která jejich orgánům umožní tyto trestné činy vyšetřovat a zajišťovat k nim potřebné důkazy.[12]

3.6 Sociální inženýrství

Sociálním inženýrstvím je označován způsob manipulace s lidmi s cílem přimět uživatele k provedení nějaké činnosti či od něj získání nějaké informace. Osoba využívající této

[12] *POLČÁK, Radim, Právo na internetu.*

manipulace je nazývána „sociotechnikem“, nebo „sociálním inženýrem.“ Zdatný sociotechnik se snaží přesvědčit potencionální oběť, že je někým jiným, někým kdo má oprávnění důvěrné informace potencionální oběti znát.

K úspěchu akce sociotechnika přispívá několik psychických slabin potencionálních obětí. Těmi jsou:

- Zbavení oběti odpovědnosti – útočník u oběti vyvolá pocit, že pokud akce nedopadne dobře, nebude odpovědnost ležet pouze na něm. Tato situace nastává většinou při získávání firemních informací, kdy zaměstnanci tím, že nechrání vlastní peníze, jsou méně opatrní. Obvykle se používají fráze typu: „Váš šéf již akci předem schválil, nebo Váš kolega mi v tomto pomohl minulý měsíc.“

Dle Václav Jirovského v knize Kybernetická kriminalita jsou dalšími:

- Důvěra, sympatie
- Morální povinnost
- Odměna
- Pocit viny

3.6.1 Postup sociotehnika

Nyní popíši jednotlivé fáze postupu sociotechnika, tak jak je ve své knize uvádí Václav Jirovský.

1. Fáze – Průzkum volných zdrojů informací neboli získávání a shromažďování informací z veřejně dostupných zdrojů. Jedná se například o internetové vyhledávače (články na internetu, internetová fóra), stránky společnosti. Z těchto informací si sociotechnik sestavuje profil své budoucí oběti, mapuje slabá místa oběti nebo hledá vhodnou taktiku na útok.

2. Fáze - Budování vztahů a důvěry, tato fáze může být časově náročná, zejména pokud se týká podvodného jednání, kde sociotechnik musí s obětí nejdříve nějakou dobu komunikovat. Sociotechnik může při těchto rozhovorech z oběti postupně vylákávat potřebné informace.

3. Fáze – Využití informace, v této fázi sociotechnik již využívá získaných informací k dokončení podvodného jednání a získání financí.

3.6.2 Krádež identity

Máte-li peníze uložené ve své peněžence, máte ji zcela jistě uschovanou ve své kabelce či náprsní kapse a dáváte si pozor, aby Vám ji nikdo neodcizil, zvláště jste-li v místech, kde kvůli většímu počtu lidí jste nuceni být s neznámými lidmi v blízkém kontaktu. Své peníze máte u sebe a víte jak si je ochránit. S rozvojem internetu a služeb, které poskytuje, se ovšem způsob ochrany svých peněz před zločinnými praktikami změnil. S rozvojem internetového bankovnictví jsou Vaše peníze uloženy na místě, které fyzicky ochránit nedovedete. Toto místo by navíc mělo být mnohem bezpečnější než Vaše peněženka uložená náprsní kapse. Bankovní instituce provozující bankovní služby jsou ochotny za zabezpečení Vašich peněz platit nemalé peníze. Jsou si vědomy, že pokud byste přišli o své peníze vinou jejich nedostatečného technického zabezpečení, byly by povinny Vám tyto peníze do určité výše uhradit, nehledě na to, že by tímto ztratily mnohem víc než jen určitý finanční obnos, ale hlavně by tímto přišly o svou spolehlivost a postavení na trhu.

Jak se tedy „zloděj“ může dostat k vašim penězům, není-li nadprůměrně vzdělán v informačních systémech, nemá-li k dispozici finančně nákladné technologické prostředky a dbá-li banka zodpovědně na zabezpečení financí? V tomto je odpověď velice jednoduchá, nejslabším článkem je uživatel. Klient banky, uživatel internetového účtu, v průběhu staletí již vyškolen jak si fyzicky bránit své peníze, ale již zcela neinformovaný v tom, jak si ubránit peníze na svém elektronickém účtu, respektive přístupu k nim.

A tak na dveřích v autobusové dopravě můžeme číst varování „Pozor na kapsáře„ (pro cizince „Beware of pickpocket“), ve zprávách v televizi vídáme varování, aby si zejména staří lidé neukládali peníze doma a nepouštěli cizí lidi do bytu, v obchodech u nákupních vozíků můžeme vidět varování, aby si lidé nenechávali svoji tašku s peněženkou bez dozoru v košíku, ale při používání internetu podobná varování nenajdeme a jsou-li tam, jsou umístěna na stránkách, kam většina uživatelů nezavítá.

Nejčastějším způsobem, jak se neznámá osoba dostane do Vašeho bankovního účtu, je získání Vašich přístupových údajů. Bankovní systém by k Vašemu účtu cizí osobu nepustil, je tedy nutné předstírat, že se přihlašujete Vy. Vaše identita byla tímto ukradena.

3.6.3 Identita

Co se vlastně pod pojmem identita rozumí? Je to souhrn několika osobních údajů. Údajů, prostřednictvím kterých můžeme identifikovat konkrétního člověka. U osob to může být jméno, příjmení, datum narození, adresa bydliště, rodné číslo, číslo bankovního účtu či kreditních/debetních karet, číslo občanského průkazu a jiného osobního dokladu a přístupové údaje k bankovním účtům, emailovým a jiným.

Stále častěji se setkáváme s pojmem digitální identita. Určit co konkrétně tvoří digitální identitu, není snadné. Na jednom místě máme uložené informace o své osobě, a když někam přijdeme, jen jednoduše vložíme příslušné jméno a heslo (či certifikát), čímž se v podstatě představíme serveru na druhé straně a potvrdíme mu tak, že k danému účtu přistupujeme právě my. V prostředí internetu identitu člověka netvoří jeho občanský průkaz, ale spíše soubor jeho zájmů, přátel a myšlenek. Možné je, že se předmětná osoba jmenuje i jinak než ve skutečnosti.

Informace, která se už jednou ocitne na internetu je z něj těžko odstranitelná. Společnost AVG Technologies provedla zajímavý výzkum, kterým prokázala, že čtvrtina má své online profily ještě předtím než se narodí. Jedná se o nahrávání prenatálních fotografií z ultrazvuku, sdělování zkušeností během těhotenství, online fotografická alba dětí od jejich narození až po jejich dospělost. Při průzkumu, který společnost AVG Technologies udělala u matek v USA, Kanadě, Velké Británii, Francii, Německu, Itálii, Španělsku, Austrálii, Novém Zélandě a Japonsku, zjistila, že 81% dětí mladších než dva roky má nějaký druh digitálního profilu se svými online zveřejněnými fotografiemi. V USA je 92% dětí prezentováno online ještě předtím, než dosáhnou dvou let. V Evropských zemích se toto číslo pohybuje okolo 73%. Rodiče ovšem nezůstávají jen u zveřejňování fotografií svých dětí. 7% miminek a batolat má svou vlastní emailovou adresu a profil na některé ze sociálních sítí.

3.7 Techniky internetových podvodů

Postupů jak podvodně vylákat z uživatelů internetu peníze je velké množství. Přesto se dají zařadit do několika kategorií, na které se v této diplomové práci blíže zaměřím. Jde o tyto způsoby podvodů:

- Phishing
- Malware
- Podvodné elektronické obchody

- Podvodné inzeráty na internetu
- Scam (419)

3.7.1 Phishing

Phishing je jednou z nejvíce používaných technik k podvodnému získání osobních údajů, která využívá metody sociálního inženýrství. Jak už název napovídá, jde o tzv. „rybaření“, nebo „nahazování udiček“. Podstatou této metody je snaha o zcizení digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtů, za účelem jejich následného zneužití. Tato metoda probíhá nejčastěji vytvořením podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží zmást uživatele a zmíněné údaje z něj vylákat. Rozesílané zprávy jsou maskovány tak, aby co nejvíce imitovaly důvěryhodné odesílatele.

Tři nejoblíbenější metody phishingových útoků, které dnes phisheři používají, představují útoky typu MITM (man in the middle, neboli prostředník). Těmito metodami jsou útok za pomocí falešné identity, útok přesměrováním a útok vyskakovacím oknem. Útok falešnou identitou je nejjednodušší a tedy nejčastěji užívanou metodou podvodu.[13]

Jedním z nejčastějších zpráv jsou například zprávy vystupující jako bankovní instituce. Banka se v těchto zprávách dotazuje na číslo účtu a přihlašovací údaje pro kontrolu. Aby uživatel nad zprávou moc nepřemýšlel a předmětné údaje co nejdříve zaslal, volí podvodníci taktiku vystrašení. Ve zprávě je tedy klient obeznámen s tím, že právě z jeho účtu proběhla finanční transakce v nezanedbatelné výši a banka si chce jen ověřit, zda transakce proběhla z vůle klienta či někdo neoprávněně získal přístup k jeho účtu. Uživatel na toto reaguje okamžitým kliknutím na odkaz v emailové zprávě, prostřednictvím kterého je přesměrován na fiktivní stránky bankovní instituce a zde zadá své přístupové údaje.

Prvním případem pokusu o uplatnění phishingu v prostředí bankovní sféry v České republice se v březnu 2006 stala Citybank. V březnu 2008 proběhl velký phishingový útok zaměřený na klienty České spořitelny, a.s..

Jak takový phishing funguje v praxi? Většina uživatelů je již obeznámena s tím, že pokud obdrží emailovou zprávu od své banky, nemá zde klikat na žádný odkaz a už vůbec ne vyplňovat své přístupové údaje. Tomuto se ovšem přizpůsobili i podvodníci a své podvodné

[13] James Lance, Phishing bez záhad.

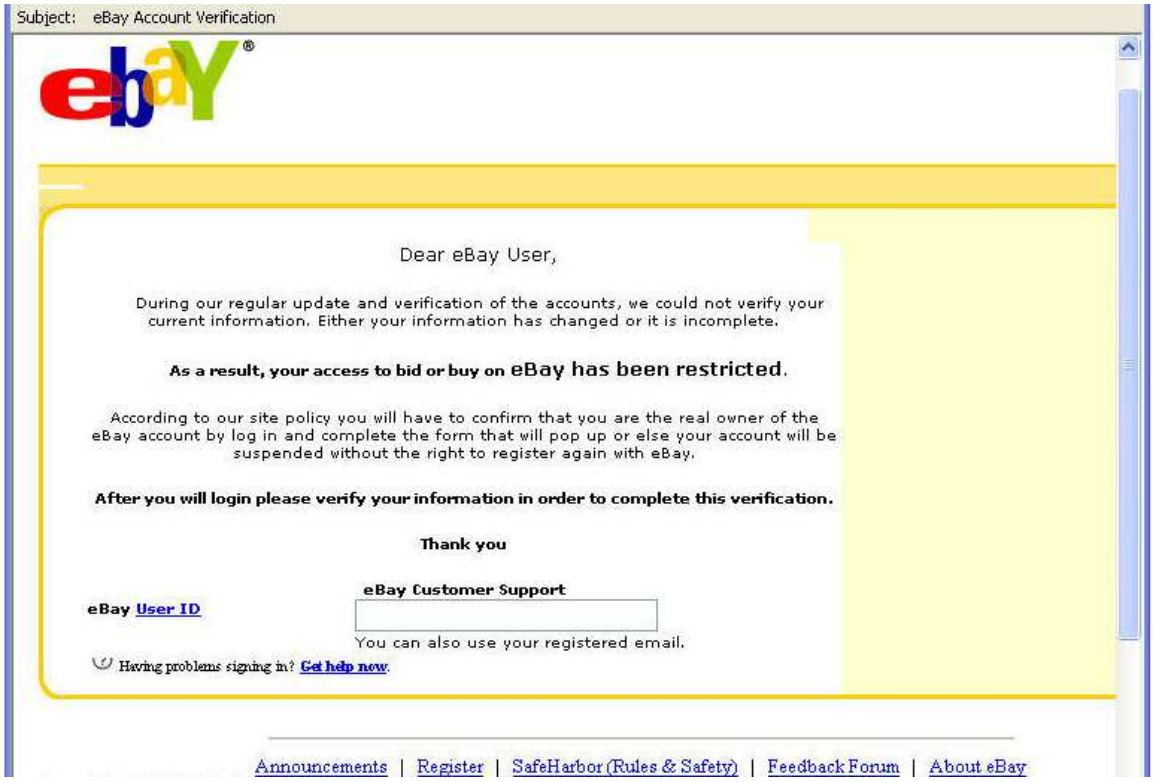
jednání upravili. Jeden z možných způsobů jak vylákat z klienta jeho přístupové údaje a získat z jeho bankovního účtu peníze pak může vypadat třeba takto. Uživatel obdrží emailovou zprávu, kde je z výpisu účtu patrné, že z jeho účtu byla čerpána vyšší částka, o které si je vědom, že ji nezadával. Toto je opět prvotní útok na nervový systém uživatele. Čím větší vystrašení, tím více pravděpodobnější je, že uživatel přestane racionálně uvažovat a stane se obětí podvodníků. V této emailové zprávě je uvedeno podvodné telefonní číslo na telefonního operátora. Vystrašený uživatel zvolí telefonní kontakt jako nejrychlejší cestu k zabránění úniku peněz z jeho účtu. A v tuto chvíli začíná spolupráce minimálně dvou podvodníků. Tito podvodníci sedí zpravidla kousek od sebe. Jakmile se uživatel pokouší dovolat na podvodnou linku, druhý z podvodníků volá pravému operátorovi a požádá ho o převod peněz na účet, který je umístěn mimo Českou republiku, nebo na účet, který byl založen na fiktivní osobu, či tzv. bílého koně. Jak si lze založit účet na fiktivní osobu popíši níže. Operátorka se podvodníka zeptá na číslo účtu a po té také na uvedení dvou znaků z bezpečnostního hesla, operátorka náhodně tyto znaky určí. Podvodník, který telefonuje s již brzy podvedeným uživatelem, opakuje otázky operátorky. Uživatel tak podvodníkům prozradí své číslo účtu i potřebné dva znaky. Do této chvíle se necítí být podveden, neboť prozradil pouze dva znaky z bezpečnostního hesla, tedy, i kdyby tyto znaky řekl neoprávněné osobě, tak by přece přístup k jeho penězům nezískala. Rozčílený uživatel se následně podvodníka dotáže, jak je možné, že z jeho účtu odešla určitá částka a zde je ujištěn, že se jedná pouze o technickou chybu, ale tuto částku samozřejmě na svém účtu má, jde pouze o chybné zobrazení, které již banka řeší, uživatel se tedy nemusí ničeho bát. Zde spočívá druhý trik, podvodníci nejenže převedli peníze na předmětný účet, ale získali i minimálně 24 hodin na to, aby tímto způsobem napálili více lidí a peníze z podvodného účtu vyzvedli či převedli na účet jiný, či jiným způsobem zužitkovali. Podvedený si totiž nejspíše po několika hodinách svůj účet zkontroluje a zde vidí, že ta daná částka je stále vedena jako převedená a ačkoliv již je řádně vystrašen či rozčílen, většinou počká do dalšího dne v domnění, že se skutečně jedná o technickou chybu a banka tuto chybu zatím řeší. Nejdříve po 24 hodinách podvedený uživatel tak začne převod peněz znovu řešit.

3.7.2 Paypal

Uživatelé internetu, kteří nakupují přes internet v zahraničí, zcela jistě znají platební metodu PayPal. PayPal není technicky vzato bankovní instituce, ale funguje velmi podobně. Umožňuje uživatelům snadno převádět peníze na jiný paypalový účet pouhým odesláním

emailové zprávy. V praxi působí tato služba bezpečněji, než na neznámých internetových stránkách zadávat údaje ke své platební kartě. A tam kde protékají peníze, samozřejmě musejí být i lidé, kteří tohoto chtějí zneužít.

Paypal má více než 202 milionů uživatelů operujících ve 190 zemích. Podvodníci tak phishingovou zprávu, SPAM, rozešlou do velkého množství emailových schránek, kdy je velká šance, že některé zprávy skutečně dorazí k uživatelům služeb PayPal.



Obrázek 6 Phishingový email vydávající se za EBAY[14]

3.7.3 Jak poznat phishingový podvod

Když víte na co se dívat, je snadnější podvod rozpoznat. Podvody prozradí poměrně široká škála vlastností. Patří k nim generické názvy, logo, které tak docela neodpovídá, špatná gramatika, požadavky na ověření a maskovaná webová adresa. U phishingových podvodů začíná SPAMový e-mail téměř vždy eufemismem v místě, kde by mělo být Vaše jméno. Takže například: „Vážený uživateli“, nebo „Vážený zákazníku“. Někdy volí podvodníci pozdrav, u kterého není jméno běžné, takže například „Zdravíme Vás!“ nebo „Vítejte!“.

[14] security.fnal.gov, 15. 12. 2013

Téměř každý pokus o phishing obsahuje požadavek, aby uživatel „ověřil svůj účet“ nebo potvrdil informace o svém účtu. Kvůli předpisům na ochranu soukromí, bezpečnostním potížím a zdravému selskému rozumu důvěryhodné společnosti nikdy nepožádají uživatele o potvrzení následujících informací:

- Kódy PIN
- Uživatelská jména
- Hesla
- Čísla bankovních účtů
- Čísla platebních karet[15]

3.7.4 Malware

Malware je obecný název pro škodlivý kód. Jedná se o programový kód speciálně vyvinutý k tomu, aby poškodil počítač nebo data v něm.

Existuje několik standardních typů malwarů, jsou to:

- Viry
- Červi
- Trojské koně
- Botnety
- Keyloggery
- Spyware
- Avare
- Shareware
- Ransomware

Právě poslední jmenovaný ransomware, chci popsat více, protože právě on zneužívá nevědomosti uživatelů k tomu, aby mu odevzdali své peníze.

[15] Buď pánem svého prostoru, Linda McCarthy, Denise Weldon-Siviy.

3.7.5 Ransomware

Ransomware neboli tzv. vyděračský malware. U ransomwaru drží pachatelé počítač jako rukojmí do doby než uživatel zaplatí výkupné (angl. ransom = výkupné). Pachatelé vyřadí uživatelův počítač z provozu a snaží se ho přimět zaplatit.

V současné době nejznámější a v České republice velice rozšířený je tzv. ransomware vydávající se za Policii České republiky. Tento ransomware se primárně vyskytuje na platformě Microsoft Windows. Tento malware po napadení cílového počítače zobrazí přes celou obrazovku zprávu Policie České republiky, ve které je uživatel předmětného počítače vyrozuměn o tom, že se dopustil trestného činu a jeho počítač byl zablokován. Dále je uživatel vyrozuměn o tom, jaká trestní sazba mu za tento čin hrozí, vždy nějaký trest odnětí svobody. Uživateli je ale ponechaná možnost do 48 hodin uhradit pokutu ve výši 2000 až 3000,- Kč pomocí kupónu PaySafe Card nebo Ukash a celá věc tak bude anulována a Policie ČR mu opět jeho počítač zpřístupní. K řádnému vystrašení uživatele ještě poslouží jeho fotografie, která byla pořízena prostřednictvím jeho webové kamery, jeho IP adresa a jeho geolokační údaje. Aplikace ransomware se spouští v celoobrazovkovém režimu a má nastavený atribut always-on-top, tedy vždy na vrchu. Neznalý uživatel tak nemá šanci činnost této aplikace ukončit.

Analýzou tohoto malware ze zajištěných počítačů bylo zjištěno, že se tento malware skládá ze dvou částí. Jednou částí je tzv. botnet klient. Pomocí tohoto botnet klienta je počítač uživatele zapojen do botnet sítě a připraven přijmout pokyny z CaC serveru. Druhou částí je aplikace zobrazující výzvu policie a vyžadující platbu. CaC server po té v napadeném počítači spustí na dálku ransomwarovou aplikaci, ale dokáže počítač ovládat a donutit ho tak i k jiným úkonům. K infikování počítače dochází tak že, majitelé ransomware infikují internetové stránky, speciálně stránky s pornografickým obsahem, nebo stránky nelegálně poskytující filmy a jiné soubory chráněné autorským zákonem. Při prvním přístupu počítače na infikované stránky dojde k přesměrování na stránky obsahující exploit umožňující získat přístup do systému. Malware, který se dostane do počítače, se zde usídlí a vyčkává na pokyny z botnetu.

U tohoto způsobu je možné vypozorovat použití sociálního inženýrství zejména ve výběru infikovaných stránek. Systém se navíc zaměřuje na infikování počítačů, které na určité stránky vstupují poprvé, toto se snaží detekovat pomocí cookies souborů. Uživatel počítače tak řeší určité dilema, zda vyhledat pomoc či kontaktovat policii a svěřit se tak s tím, že navštívil stránky s pornografickým obsahem.

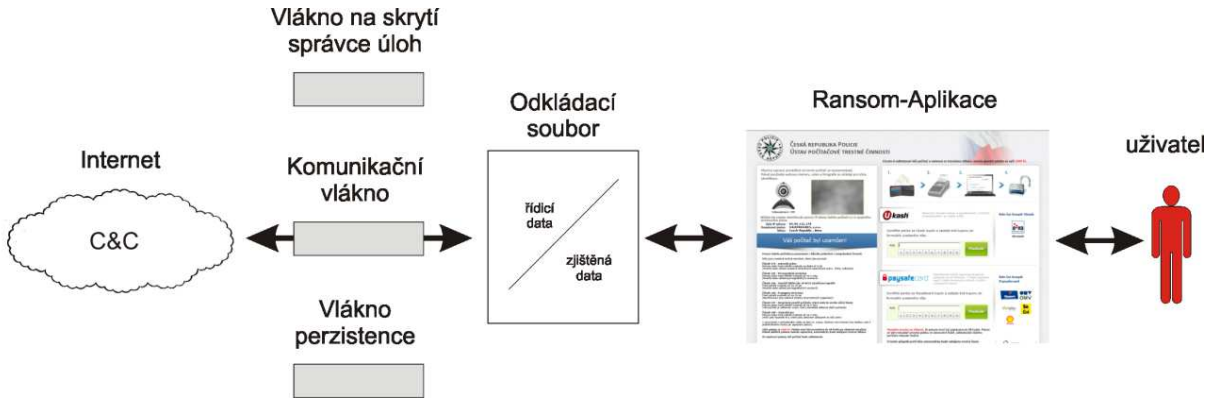
Aby tento malware nebyl ihned detekován a odstraněn používá na svoji obranu blokování správce úloh, za každou méně než sekundu zkontroloval, zda je okno s výzvou policie zobrazeno a pokud tomu tak bylo, vždy správce úloh ukončil. Dále také za méně jak sekundu obnovoval svůj zápis v registrových klíčích a tím se bránil proti vymazání. Svoji knihovnu tento malware v počítači zakódovává tak, aby nebyl detekován běžným antivirovým testem. Protože je tento malware závislý na komunikaci se svým CaC serverem, je nutné, aby komunikace mezi nimi probíhala skrytě a nebyla ihned odhalena. Ransomware tak vloží svůj vlastní kód do internetového prohlížeče, dosud byla zjištěna jeho komunikace přes prohlížeče Explorer, Mozzila Firefox, Google Chrome a Opera. Malware má v sobě umístěnu jednu IP adresu CaC serveru a doménové jméno, což mu zaručuje flexibilní přístup, pokud by došlo ke změně v DNS. Malware se tak nejdříve pokouší spojit se svým velitelským centrem prostřednictvím IP adresy a pokud by tato již nebyla aktuální, využije doménové jméno.

Jak je tedy tento způsob vylákání peněz z lidí účinný? Z pohledu sociálního inženýrství je nutné uznat, že jeho přesvědčivá metoda je velice účinná. Uživatel, který je si vědom toho, že navštívil pornografické stránky, navíc vidí na obrazovce svoji fotografii a geolokační údaje vidí zaplacení pokuty ve výši 2000 – 3000,- Kč jako nejmenší zlo. Zaplacením pomocí platebních kupónů, které lze volně zakoupit například na benzinové pumpě, tak navíc umožňuje vyděračům anonymní převzetí finanční částky. Takto získané peníze pak provozovatelé tohoto vyděračského malwaru využijí například v internetových kasinech, kde je převedou na peníze legální.

Jak se proti tomuto malware ubránit po technické stránce? „Po nalezení prvních podezřelých souborů a persistence, lze dle času jejich modifikace dohledat další soubory, vytvořené činností malware. Dále je třeba v registrech a na disku vyhledat veškeré reference na nalezené podezřelé soubory. Poté už lze odstranit všechny odkazy v registru na tyto soubory i samotné binární soubory. Na závěr zbývá vymazat všechny dočasné složky a internetovou cache. V případě úspěchu bude po restartu a přihlášení normálně dostupná pracovní plocha a počítač se bude opět chovat normálně. V případě, že se malware nacházel výhradně v uživatelském profilu a uživateli přístupných složkách, lze postupovat následovně: vytvořit nového uživatele, přesunout uživatelská data a smazat původního uživatele. Následně by měla proběhnout hloubková kontrola PC antivirovým programem, nejlépe na jiném počítači, ke kterému je disk z napadeného počítače dočasně připojen.“ [16].

[16] www.root.cz/clanky/ransomware-policejni-virus-na-pitevnim-stole/

Další z možností pokud je počítač v nouzovém režimu či v režimu jiného uživatele volný, tedy již není blokován tzv. ransomwarovým oknem, které je vždy navrchu, lze na internetových stránkách http://www.f-secure.com/en/web/home_global/online-scanner využít přímo k tomuto určenou službu, která v počítači vyhledá a bezpečně odstraní veškeré soubory patřící k tomuto škodlivému souboru. Toto působí i jakási prevence, že v počítači nezůstal žádný ukrytý malware a počítač není nadále připojen do boletu a připraven kdykoliv opět poslouchat pokyny podvodníků.



Obrázek 7 schéma spojení obou částí klient - ransomware - botnet[17]

V lednu 2013 vydal Odbor bezpečnostní politiky Ministerstva vnitra situační zprávu, ve které mimo jiné uvedl, že v roce 2014 se očekává prudký nárůst počtu infikovaných zařízení tzv. ransomware, který nejprve zašifruje některé soubory na disku uživatele a následně za klíč k nim vyžaduje „výkupné“. V tomto případě je vyhrožováno uživateli tím, že v případě neuhrazení požadované částky budou data zaslána na policii. Mimo Českou republiku se již tyto případy vyskytly v roce 2012, kdy bylo za odšifrování počítače požadováno až 3 tisíce dolarů. Vzhledem k tomu, že většina uživatelů nelegálně využívá určité druhy softwaru, jsou tyto výhružky mnohdy účinné.

Ve třetím čtvrtletí roku 2013 narostl počet zjištěných případů ransomware o 43%, což z něj v roce 2013 udělalo jeden z nejrychleji rostoucích větví kyberkriminality.

Z článku internetového portálu nakedsecurity.sophos.com vyplývá, že v únoru 2013 španělská policie s asistencí Interpolu a Europolu zatkla 10 podezřelých – 6 občanů z Ruska, dva Ukrajince a dva Řeky, kteří si vydělávali právě prostřednictvím ransomwaru. Španělská policie uvedla, že tato skupina si prostřednictvím této trestné činnosti vydělala více jak 1

[17] www.root.cz/clanky/ransomware-policejni-virus/ , 20. 2. 2014

milion euro ročně. Šéfem této skupiny byl 27 letý Rus, který byl později zatčen v Dubaji ve Spojených arabských emirátech.[18] Ačkoliv tento gang byl i s jeho šéfem Španělskou policií zatčen, vyděračský malware se šíří mezi počítači dál, což nasvědčuje tomu, že know how o tomto vyděračském škodlivém kódu již bylo nejspíše prodáno dalším skupinám osob, kdy těchto gangů může být po celém světě několik a jejich zastavení je tak pro policii velice obtížné. Nejlepší obranou tak zůstává kvalitní antivirový systém a hlavně dobrá informovanost veřejnosti, aby se nenechala podvodníky tak snadno oklamat.

Tomu, že ve světě řádí těchto vyděračských skupin více, nasvědčuje i čtvrtletní zpráva společnosti AVG, která oznámila, že nejméně jeden kolující ransomware tohoto typu byl vyvinut v České republice.[19]

Obrázek 8 Vzhled ransomwarového okna[20]

[18] http://nakedsecurity.sophos.com/2013/02/14/reveton-ransomware-gang-arrested-by-spanish-police/
[19] http://mediacenter.avg.com/en/press-tools/avg-threat-reports/avg-community-powered-threat-report-q3-2012.html
[20] Vlastní zdroj

Ačkoliv celý tento „trik“ působí lacině a průhledně, přesto se najdou uživatelé, kteří pokutu zaplatí. Tyto uživatele v posílání svých peněz neznámo kam nezastaví, ani fakt, že nápis „Česká republika Policie“ je nesmyslný, neboť správně by mělo být uvedeno Policie České republiky. Dále název „Ústav počítačové trestné činnosti“ v České republice neexistuje. Jedním z trestných činů, kterého se mohl uživatel dopustit a který prostřednictvím tohoto zobrazovaného okna mu je kladen za vinu je „hráli jste hazardní hry, které jsou zákonem zakázány ve Vaší zemi“, takto formulovaný trestný čin bychom v trestním zákoníku, asi těžko hledali. Dále je na první pohled podezřelé, že Policie České republiky by po zaplacení pokuty zastavila snahu o trestní stíhání poškozeného, zejména pokud se pokuta platí přes netransparentní platební systém Ukash či Paysafecard. Zde je ovšem nutné podotknout, že ne každý danou částku uhradil, se po té rozhodl celou věc nahlásit na policii. Po uhrazení této částky, totiž z většiny případů blokující podvodná stránka z obrazovky zmizí a „šťastný“ uživatel nevidí důvod, proč by měl celou věc policii hlásit. V praxi se dokonce objevily případy, kdy uživatel pokutu uhradil i dvakrát za sebou a bohužel nebylo to pouze v jednom případě. Po uhrazení první pokuty uživateli sice bylo z obrazovky odstraněno varovné okno požadující uhrazení pokuty, škodlivý malware ovšem v počítači zůstal a činnost uživatele sledoval. V momentě, kdy se uživatel po nějaké době opět přihlásil na určité stránky botnet opět vydal rozkaz „varovné okno“ spustit a opětovně vyžadovat pokutu, kterou uživatel samozřejmě opět rychle uhradil.

Společnost Symantec, která se tímto malwarem intenzivně zabývala, vypracovala odhady zisku. Podle společnosti Symantec si tak pachatelé mohli za 9 měsíců činnosti přijít na výdělek ve výši až 3,8 milionů EUR. Zde je ovšem nutno poznamenat, že se nejedná pouze o výdělek od obyvatel České republiky, ale z celého světa, neboť první známky tohoto viru jsou známy nejdříve z Německa, Velké Británie a Francie a teprve po té se tento virus dostal i do ostatních zemí včetně České republiky.

3.7.6 Podvodné elektronické obchody

Češi se k výhodám nakupování prostřednictvím internetu teprve postupně propracovávají, ale jejich zájem o tento druh nakupování rok od roku stoupá. Obrovský nárůst těchto obchodů je hlavně v předvánočním období. Dle Asociace pro elektronickou komerci nakupují po internetu nejčastěji studenti, podnikatelé a ženy na mateřské dovolené, obecně pak lidé s vyšším vzděláním, v předvánočním období se ovšem zvyšuje počet lidí i z ostatních kategorií. Tedy lidé, kteří nemají s nakupováním přes internet tolik zkušeností. V tomto

předvánočním období jsou Češi ochotni utratit prostřednictvím nákupu v elektronických obchodech vysoké částky. V roce 2011 v období od 12 do 21. prosince to bylo dle Asociace pro elektronickou komerci cca. 3,8 mld. Kč. Podvodníci se tak právě v tomto čase zaměřují na zakládání podvodných elektronických obchodů.

Policejní prezidium vydalo dne 30. 1. 2014 zprávu, ve které upozornilo na stále více narůstající počet internetových podvodů v rámci elektronických obchodů. Jako nejčastější příznaky podezřelého internetového obchodu dle Policejního prezidia jsou:

- Příliš nízké ceny zboží
- Nabídka zboží, které již není v prodeji
- Na stránkách obchodu chybí kontakty, je uveden pouze kontaktní formulář
- Uvedený email, nebo telefonní číslo jsou nekontaktní
- Krátce registrovaná internetová doména a skryté údaje o vlastníkovi
- Požadavek na platbu předem, absence na zasílání na dobírku či osobní převzetí
- Zmatené, velmi často zkopírované obchodní podmínky
- Nevhodné sídlo firmy (nefunkční), v tomto případě je prospěšné zkusit si vyhledat zadanou adresu firmy prostřednictvím google maps – StreetView a zjistit tak, zda uvedená adresa existuje a zda na této adrese nestojí jen polorozpadlá budova.[21]

Provozovatelé internetových stránek www.lupa.cz na svých internetových stránkách http://www.lupa.cz/clanky/jak-poznat-podvodny-e-shop-tady-je-jedenact-priznaku-ktere-napovi/ k výše uvedeným znakům uvádí další, kterými jsou:

- Zmatená skladba sortimentu a nabízení hlavně aktuálního zboží. Většina podvodných eshopů byla charakteristická tím, že prodávaly vše možné i nemožné, jen aby pomocí širokého sortimentu nalákaly na své stránky další návštěvníky. Z tohoto důvodu do svého sortimentu dávaly zboží, které lidé nejvíce aktuálně vyhledávají na internetu.
- Vznik obchodu před několika dny či pár týdny. Toto se dá zjistit již přes registraci domény, ale firma, která je na stránkách elektronického obchodu se dá ověřit i na stránkách www.justice.cz. Na těchto stránkách se dá zjistit, zda není společnost nová či zda v blízké době nedošlo ke změně jejích vlastníků.

[21] *mjr. Ing. Jana Macalíková, tisková mluvčí Policejní prezidium ČR, www. policie.cz*

- Žádné hodnocení či recenze od kupujících. Pokud předmětný elektronický obchod nemá zatím žádné hodnocení či jich má velice málo je taktéž zřejmé, že se jedná o obchod nově založený. Hodnocení obchodu je možno najít tak, že do kteréhokoliv vyhledávače uživatel zadá název obchodu, IČO, telefonní číslo nebo přímo internetovou doménu obchodu a za toto slovo napíše „hodnocení“. V tu chvíli dostane o předmětném eshopu již dostatek potřebných informací.

Rozpoznání podvodného eshopu není pro laika vůbec snadné. Podvodníci začali zneužívat i logo certifikovaných obchodů. Certifikace APEK při tom byla jedním z prvků umožňující odhalit podvodné či podezřelé eshopy. Pro získání certifikace je potřeba projít náročným testováním, které zahrnuje ověření nákupního procesu, ověření obchodu, obchodních podmínek, ale i mystery shopping. Mystery shopping je kvalitativní metoda výzkumu, která měří maloobchodní kvalitu. Při mystery shoppingu jsou data získávána pomocí fiktivního nakupujícího, který vystupuje jako běžný zákazník. Jeho úkolem je nákup výrobku, kladení dotazů, registrace stížnosti, sledování přístupu při vrácení zboží.

Asociace pro elektronickou komerci (APEK) v měsíci červenci roku 2013 upozornila na stále častější zneužívání jejich loga s tím, že každý měsíc prověřují několik eshopů, které na svých stránkách neoprávněně jejich logo zobrazují. Jako jeden z možných obranných postupů, kterým si lze ověřit, zda je logo APEK (obr. č. 9) na stránkách elektronického obchodu pravdivé, či zda se jedná pouze o jeho zneužití je ověřit si tuto skutečnost přímo na internetových stránkách Asociace pro elektronickou komerci, konkrétně na adrese http://www.apek.cz/certifikace-obchodu-hlavni/, kde lze do pole pro ověření zadat internetovou adresu obchodu a během několika vteřin dostane uživatel odpověď, zda je obchod skutečně oprávněně certifikován a je tedy pro nákup bezpečný.

Další logo, které je zneužíváno podvodnými elektronickými obchody je logo „ověřeno“ od provozovatelů internetových stránek www.heureka.cz (obr. č. 10). Zda je tato recenze na předmětný obchod skutečně platná je možno si ověřit na internetových stránkách http://overeno.heureka.cz/ .

Obrázek 9 Symbol APEK[22]

Obrázek 10 Symbol HEUREKA ověřeno zákazníky[23]

3.7.7 Správný postup při nakupování v elektronickém obchodě

Jak by tedy uživatel měl správně postupovat, chce-li svůj nákup uskutečnit prostřednictvím internetu? Pokud již v určitém elektronickém obchodě nakupoval v minulosti a je s jeho službami spokojen není potřeba podnikat žádné bezpečnostní kroky včetně toho, že v tomto případě bych i s klidným srdcem zvolila platbu předem na účet. Pozornost bych zvýšila pouze v případě, že by zboží, které si chci objednat, překročilo finanční částku, která by pro můj rozpočet už byla znatelná. V tomto případě bych vždy nejdříve překontrolovala, zda elektrický obchod, který pravidelně využívám, nezměnil od mé poslední objednávky své majitele a také zda na internetu v poslední době nepřibyly na tento obchod negativní reakce.

Jiný postup bych volila, pokud v obchodě objednávám poprvé. Jak jsem již uvedla v předchozí kapitole, některé z elektronických obchodů mají na svých stránkách značku doporučených obchodů (APEK a jiné). Zda předmětný obchod skutečně tento certifikát získal lze ověřit přímo na internetových stránkách poskytovatele tohoto certifikátu. Pokud se potvrdí, že předmětný obchod je certifikovaný, zbývá už jen zkontrolovat, zda předmětný obchod nezměnil v blízké době své majitele a lze si bezpečně zboží objednat.

[22] www.apek.cz, 20. 1. 2014
[23] www.heureka.cz, 20. 1. 2014

Ne všechny elektronické obchody ovšem certifikací prošly. Představme si tedy, že jsme na stránkách elektronického obchodu, s kterým nemáme dosud zkušenosti. Prvním krokem je ověření internetové domény. Tímto krokem zjistíme, majitele domény, tedy kdo si předmětnou doménu zaregistroval a dále kdy byla doména založena. Tedy zda se nejedná o nově založený elektronický obchod se stářím několika dnů či týdnů. Takto mladý elektronický obchod totiž ještě nebude mít na internetu negativní recenze od poškozených uživatelů a tak druhý krok, kterým je vyhledání recenzí na předmětný obchod prostřednictvím internetového vyhledávače či na adrese http://www.oversito.cz/pozor-na-ne/ by byl zbytečný. Prověření této domény je možné například na internetové adrese: http://www.regzone.cz/domena/whois/.

Pokud jsme zjistili, že předmětný elektronický obchod je založen již déle jak měsíc a nenalezli na něj žádné negativní reakce, můžeme si zboží objednat, přesto při první objednávce je vhodnější volit možnost platby na dobírku a uhradit tak zboží až při jeho obdržení. Elektronické obchody v případě zasílání zboží na dobírku úmyslně volí další finanční příplatek k celkové ceně. Argumentují tím, že klienti si často zboží objednají, ale již si ho nevyzvednou a obchodu tak vznikají neuhrazené výdaje na poštovné. Toto sice je pravdou, ale z praxe mohu říci, že za poslední dobu přibývá obchodů, které rozdíl mezi platbou předem a platbou na dobírku nedělají a svým klientům důvěřují, nebo ještě lépe procento těch, kteří si objednají a následně si zboží nevyzvednou je pro ně zanedbatelné.

Zvolili jsme platbu při převzetí zboží, obchod je starší více jak měsíc, negativní hodnocení obchodu jsme neobjevili, balík se zbožím jsme obdrželi, posledním bezpečnostním krokem by tak mělo být překontrolování poštovního balíku na poště či u dopravce, zdali zboží není poškozené a zda obsahem je skutečně to, co jsme si objednali.

Pokud jsme si zvolili při nákupu platbu za zboží prostřednictvím platební karty, protože v obchodě už nakupujeme delší dobu, anebo cena za zboží je pouze nepatrná, zboží nám v pořádku dorazilo a s obchodem nemáme nejmenší problémy, doporučuji i přesto si v průběhu dalších měsíců kontrolovat výpis z bankovního účtu, neboť již se stalo a ne ojediněle, že poškozeným následně z účtu začaly s měsíční pravidelností odcházet nízké částky ve výši několika desítek korun. Takto nízké částky jsou v celkovém účtu téměř neviditelné a jejich měsíční opakování z nich pro poškozené na první pohled dělá legální poplatky za blíže nespecifikovanou službu. Až později klient banky zjistí, že to, co mu odchází z účtu, nejsou poplatky za legální služby, ale potají zcizené peníze od podvodníků, kteří získali přístupové údaje k platební kartě.

3.7.8 Podvodné inzeráty na internetu

Podvody způsobené prostřednictvím internetu mívají určité znaky. Podvody v nižších finančních částkách se zaměřují především na poptávku. Reagovat na poptávkový inzerát je výhodnější než si sám vystavit inzerát nabídky. Výhodou tohoto je, že podvodník se nemusí nikde registrovat. Nemusí čekat, až se ozve někdo, kdo bude mít o jím nabízené zboží zájem. Naopak vzhledem k tomu, že budoucí poškozený si založil inzerát s poptávkou, je zřejmé, že jím požadované zboží je těžko k dostání a tak jeho reakce na možný obchod bude pozitivní. Podvodník může určit nízkou cenu, čímž vytvoří pro budoucího poškozeného zboží neodolatelné. Kdyby podvodník vystavil sám inzerát se zbožím s podezřele nízkou cenou, vyvolalo by to u některých uživatelů pozornost a ti by mohli předmětný inzerát nahlásit provozovateli stránek. Podvodník dokonce v tomto případě může nechat navrhnout cenu kupujícím s tím, že požadovaný předmět nepoužívá, nepotřebuje ho a o cenu mu ani tak moc nejde.

Jak by si měl tedy kupující ověřit, že nabízené zboží není jen podvod. Jedním z kroků je nechat si zaslat fotografii tohoto zboží. Podvodník v tomto případě většinou využije fotografii, kterou nalezne někde na internetu. Ověření této fotografie je potom možné například přes google vyhledávač, zde lze fotografii v kategorii „obrázky“ nahrát a dát vyhledat *(viz obr. 11).* Vyhledávač už se pak pokusí zjistit, kde se stejná (podobná) fotografie nachází, tedy zda podvodník nemohl použít cizí fotografii zveřejněnou na internetu.

Obrázek 11- vyhledávání obrázků - vyhledávač google[24]

[24] www.google.com 2. 2. 2014

Pokud nám podvodník pošle fotografii a my ji nikde jinde na internetu neobjevíme, pořád ještě bychom měli zvolit druhý krok a tím je požádat potencionálního prodejce, aby zboží vyfotil ještě jednou, tentokrát například s metrem či propiskou vedle požadovaného předmětu. Argumentovat můžeme tím, že si chceme ověřit velikost předmětu, nebo přímo na rovinu říct, že si chceme ověřit, že prodejce předmětné zboží skutečně má. V této fázi, pokud je prodejce skutečně podvodník začne fáze výmluv či hrané rozčilení, že kupující prodejci nedůvěřuje. Obojí je pouze signálem k tomu, že se jedná o skutečného podvodníka.

Dalšími znaky vyvolávajícími podezření je, že podvodník odmítá zboží zaslat na dobírku a požaduje platbu předem a zároveň také odmítá osobní převzetí. Vymlouvá se většinou na to, že bydlí na druhém konci republiky. Zde se vyplatí zkusit trik, že kupující má známého i v blízkosti bydliště prodejce a ten může zboží vyzvednout. Jedná se o cílené blafování, ale není zde co ztratit, pokud prodejce přistoupí na osobní předání zboží má kupující alespoň jistotu, že by se nemělo jednat o podvodníka. V tomto případě lze včas před předáním prodejci napsat, že známý nakonec zboží z nějakého důvodu vyzvednout nemůže a my přeci jenom zvolíme možnost zaslání zboží na naši adresu.

Pokud si tedy poškozený objednává zboží svoji adresu a podvodník trvá na platbě předem, může kupující navrhnout, že uhradí pouze cenu poštovného a zbytek až při převzetí zboží. Tak bude mít prodejce jistotu, že v případě nevyzvednutí mu nevznikne žádná škoda. Prodejce stejně tak nemusí požadovat uhrazení částky na číslo účtu, které není tak transparentní, ale lze peníze poslat poštovní poukázkou na jméno a adresu. Pokud by si podvodník chtěl peníze vyzvednout, musel by na poště prokázat svoji totožnost.

Pokud je balík zasílán prostřednictvím České pošty nelze sice již převzatý balík po rozbalení na poště vrátit zpět, protože Česká pošta vrácení již převzatého balíku neumožňuje, ale je povinna před převzetím sdělit váhu poštovního balíku. Pokud si objednává kupující určitou věc, může prostřednictvím internetu zjistit, kolik prodávaná věc přibližně váží a na poště po té tyto údaje porovnat. Pokud by váha balíku byla zjevně odlišná, neměl by zboží převzít anebo požádat poštovního doručovatele, aby v dané věci figuroval jako svědek a sledoval otevření balíku a překontrolování jeho obsahu. Tento svědek se bude po té hodit, pokud se poškozený rozhodne celou věc nahlásit policii. Podvodníci totiž spoléhají na to, že poškozený v době rozbalování u sebe žádného svědka nemá, anebo se jedná o svědky rodinné, a tedy ne moc důvěryhodné. V dané věci je po té obtížné prokázat, zda v poštovním balíku bylo skutečně zakoupené zboží či nikoliv.

3.7.9 Podvodné inzeráty s ojetými auty

Identifikace podvodné nabídky s automobily:

- Cena novější „lepší“ značky vozu se pohybuje zhruba na polovině ceny automobilu stejného druhu a roku výroby – překontrolovat si toto můžete, pokud zadáte do filtru pro vyhledávání například na stránkách sauto.cz stejnou značku vozu, model a rok výroby.
- Telefonní číslo – s běžnou nepodezřelou emailovou adresou je používáno i telefonní číslo, které se opakuje u více inzerátů, po vytočení tohoto čísla telefon nikdo nebere, nebo je nastavena hlasová schránka.
- Pokud potencionální kupující zareaguje na podvodný inzerát, obdrží většinou od kupujícího krkolomný česko-anglický text.

Příklad jednoho z mnoha podvodných dopisů

„Ahoj,

Jsem velmi rád, že máte zájem o koupi auta.

Ceny a informace jsou správné, jsem prodat Skoda Superb 2.0 TDI , z roku 2010 s cenou 150.000, - Kc. Jsem první majitel, auto bylo nikdy zapojeny do jakékoliv nehody, motor beží perfektne

Auto je v perfektním stavu, poslední služby, které asi pred dvema mesíci, když jsem menil olej, nejsou tam žádné velké problémy. Všechny dokumenty jsou k dispozici, jsem si všechny výživné na autorizovaného servisu, mám servisní knížka, auto mít skutecné Km.

Máte-li zájem prosím odpovezte mi, abych mohla dát více informací o transakci, prosím odpovezte pokud možno v anglictine, rychle reagovat“

Pokud kupující na tuto zprávu odpoví, obdrží většinou odpověď o tom, aby uhradil zálohu za vozidlo na účet v zahraničí. Nejčastěji to bývá polovina prodejní ceny vozidla. [25]

Provozovatelé inzertního portálu sauto.cz se pokoušejí tyto inzeráty detekovat a zneplatňovat. K tomuto účelu provozovatelé zřídili u každého inzerátu tlačítko, prostřednictvím kterého je možné nahlásit podezřelý inzerát.

Dalšími znaky podvodného inzerátu jsou:

- Auto se zpravidla nachází v zahraničí

[25] http://www.sauto.cz/auto-moto-clanky/upozornujeme-sautocz-varuje-pred-podvodnymi-nabidkami/4450

- Jedná se o pozůstalost nebo prodejce pracoval v České republice a v nedávné době se odstěhoval do jiné země
- Přepravu vozidla zajistí již předem najatá zahraniční společnost

3.7.10 Scam (419)

Scam 419 je v České republice spíše znám pod názvem „Nigerijský dopis“. Jedná se o druh podvodů, které existovaly již v minulosti ve formě dopisu. Rozvojem internetu a emailové pošty se tyto podvody rapidně rozšířily do celého světa. Varianty těchto dopisů se postupem času liší, ale jejich princip zůstává stejný. Uživateli internetu přijde do jeho schránky elektronická zpráva většinou v anglickém jazyce. V této zprávě se představuje neznámý člověk většinou jako správce několika milionového majetku osoby, která zemřela a nemá žádné dědice a on by potřeboval toto vysoké dědictví převést tajně do jiné země a protože uživatelovo příjmení se má údajně shodovat s příjmením zemřelého milionáře, udělá z něj tento správce jeho oficiálního dědice. Za výpomoc nabízí odměnu ve výši několika milionů dolarů. Pokud naivní uživatel internetu svolí ke spolupráci v naději, že získá několik milionů dolarů, sdělí mu tato osoba další postup. Tím je zřízení si nového účtu v cizině kam budou peníze převedeny, kdy k tomuto účtu bude mít výhradní přístup právě uživatel. Uživatel tak sdělí podvodníkům své osobní údaje. Následně je mu zaslán elektronický kontakt na bankovní instituci, kde si může uživatel ověřit, že mu byl účet zřízen a později, že na něj byly převedeny peníze. Jedná se samozřejmě o fiktivně vytvořené internetové stránky bankovní instituce. A zde začíná finální manipulace, jejímž účelem je vytáhnout z oznamovatele co nejvíce peněz. Uživatel potěšen již téměř nabytým pohádkovým majetkem je osloven bankou k uhrazení poplatku za zřízení účtu a převedení určité částky na tento účet, aby mohl být potvrzen jako skutečná osoba a ne jako podvodník. Tato částka se pohybuje ve výši několika tisíc až desítek tisíc. Po uhrazení těchto peněz získá uživatel plný přístup ke svému účtu, nevědomky, že je účet fiktivní a peníze na něm také zadá platební příkaz, kterým se pokusí převést peníze na svůj reálný účet. Zde mu fiktivní banka vyhoví ovšem pod podmínkou, že bude uhrazen poplatek buď za osvobození od daně, nebo za převod, či jakkoliv jinak nazvaný. Tento poplatek už je ovšem podstatně vyšší, mnohdy ve výši statisíců českých korun. Uživatel, se většinou zdráhá tak vysokou částku uhradit, mnohdy ji ani nemá. Ovšem při myšlence, že peníze ve výši několika milionů dolarů jiným způsobem na svůj účet nedostane a nedostal by zpět ani již odeslané peníze, se rozhodne i takto vysokou částku uhradit, případně si ji i vypůjčit pokud ji nemá. A tímto způsobem celá věc pokračuje dál, po

podvedeném uživateli jsou požadovány další a další nesmyslné poplatky až do doby, kdy mu dojde, že žádné peníze nikdy nedostane.

Že se nejedná o malé částky, které jsou podvedení schopni s vidinou náhlého zbohatnutí podvodníkům zaplatit, dokladuje například případ, který prošetřovala policie z Jindřichova Hradce:

Chtěla být fiktivní dědičkou a přišla o 617.571 korun.

Jindřichův Hradec – Podvodné vylákání peněz přes internet.

Mladá žena z Jindřichova Hradce chtěla rychle zbohatnout bez jakékoliv vynaloženého úsilí a práce. Místo „ zaručeného dědictví" však přišla prostřednictvím internetu o celoživotní úspory. Fiktivní zpráva, kterou emailem obdržela zněla velmi lákavě.

V měsíci květnu roku 2009 odeslal dosud neznámý pachatel ze svého e-mailového účtu patchanprivacy004@yahoo.com pošk. zprávu, ve které se představil jako Patrik Chan a uvedl, že je zaměstnancem banky v Hongkongu, měl bohatého klienta Musa Omara Numana, který před šesti lety zemřel v Iráku při výbuchu bomby a na jeho účtu, vedeném právě u banky v Hongkongu, u které je Patrik Chan zaměstnán po něm zůstala finanční částka 22.500.000,-USD. Vzhledem k tomu, že se bance nepodařilo zjistit žádnou osobu v příbuzenském vztahu k zemřelému Musa Omarovi Numarovi, požádal Patrik Chan poškozenou , zda by se nevydávala za jeho příbuznou, Patrik Chan by vyřídil veškeré formality s tím spojené včetně dědického řízení, zajistil by převedení výše uvedených finančních prostředků na účet a ona mu následně zašle 70 % z této částky. Poté odkázal poškozenou na osobu Pietera Rodolfa, který dle jeho tvrzení pracuje v bankovním ústavu v Nizozemí a tento jí zajistí založení účtu u této banky , který je nutný pro převod peněz.

Mladá žena zřejmě pod vidinou „ závratného zisku" ztratila racionální uvažování a kontaktovala prostřednictvím e-mailu Pietera Rodolfa, který jí následně založil fiktivní účet u neexistující banky v Nizozemí a prostřednictvím za tímto účelem úmyslně založených webových stránek navodil v poškozené dojem, že má skutečně zřízen účet u banky v Nizozemí a prostřednictvím webové aplikace internet banking komunikuje s tímto účtem on-line.

Dále pod různými záminkami jako zřízení účtu v Nizozemí , jeho změna pro přijetí tak vysoké částky a podobně vylákal celkem na ziskuchtivé poškozené celkem 3.900 USD. A rozehrání šachové partie neznámého pachatele pokračovalo. E-mailem se ozval Patrik Chan, který mladé ženě sdělil, že zahájil převod výše uvedené částky 22.500.000 USD z banky v Hongkongu na tento její nově zřízený účet v Nizozemí. Poškozená si poté ověřila na tomto svém fiktivním účtu, že na něj byla částka skutečně připsána a P. Rodolf, který vystupoval jako zaměstnanec Post Bank jí následně sdělil, že pro převod takto vysoké částky do jiné banky, musí poškozená uhradit tzv. osvobození od daně ve výši 29.250 USD, což žena učinila a peníze dne 31. července 2009 odeslala na účet uvedený P. Rodolfem. Zhruba za tři týdny jí přišla od P. Rodolfa zpráva, že peníze byly v pořádku připsány na účet a byl jí zaslán číselný kód, který měla poškozená zadat do svého účtu u banky v Nizozemí a poté měla dát příkaz k převodu výše uvedené částky na její účet v České republice. To učinila, zadala číselný kód do svého fiktivního účtu, avšak následně byla webovou aplikací vyzvána k zadání dalšího číselného kódu. Poškozená se tedy obrátila opět na P. Rodolfa, který jí sdělil, že si musí zaplatit tzv. antiteroristický kód, neboť tento je nutný pro převod tak velké finanční částky do jiné banky. Za tento kód požadoval po poškozené finanční částku ve výši 49.550.60 USD, avšak tyto peníze již neodeslala.

Celkem tak žena z Jindřichova Hradce přišla o 617. 571 korun.

Policisté z kriminální služby a vyšetřování v Jindřichově Hradci dne 6. ledna 2010 ve věci zahájili úkony trestního řízení, požádali o spolupráci rovněž Europol a nadále budou pokračovat v prověřování tohoto případu.

Obrázek 12 Případ policie při řešení podvodného scamu 419[26]

Protože postupem času se Nigerijské dopisy dostaly do podvědomí hodně lidí a nabídka fiktivních dědictví v pohádkové výši již nebyla pro lidi dostatečným lákadlem, začali tito podvodníci cílit spíše než na touhu po zbohatnutí na touhu po lásce. Cílovou skupinou se tak staly hlavně ženy. Tyto ženy jsou vybírány na internetových seznamkách, následně jsou osloveny a je s nimi navázán vztah s fiktivním mužem. Tento muž jim pošle svoji fotografii,

[26] *http://www.policie.cz/clanek/chtela-byt-fiktivni-dedickou-a-prisla-o-617-571-korun.aspx, 10. 3. 2014*

pak další, na které již je se svým dítětem a po dobu několika týdnů si s obětí jen dopisuje, dokud si není jistý, že vztah byl již navázán. Fiktivní muž je vydáván za vojáka, nebo za obchodníka, který je v cizině a má u sebe majetek či zboží v hodnotě několika milionů. Na jeho cestě domů vzniknou komplikace a on by toto jmění potřeboval zaslat někam do bezpečí. V tuto chvíli požádá oběť, naivní ženu, o pomoc, zda by nemohl drahé zboží zaslat ji. Ona s tím pochopitelně souhlasí. Podvodník ji přes email zkontaktuje s fiktivní dopravní službou a následně se odmlčí. Fiktivní dopravní služba začne po adresátce požadovat různé poplatky za dopravu, nejdříve nižší, později se částky zvyšují na statisíce. Žena, protože se nemůže spojit se svým „vysněným mužem“ a dopravní služba při neuhrazení požadované částky vyhrožuje tím, že zboží do České republiky nedopraví, požadované peněžní částky začne zasílat. Osobně jsem se setkala s případem, kdy poškozené zaslala svému „fiktivnímu“ příteli přes jeden milion korun.

Další možností těchto scamů jsou tzv. podvodné loterie. Podvodné loterie jsou druhem podvodu, kdy jsou lidem rozeslány e-maily s oznámením o výhře vysoké částky v eurech, dolarech nebo v jiné zajímavé měně. V případě, že oslovený výherce kontaktuje provozovatele loterie, je mu sděleno, že výhra bude vyplacena, jakmile zaplatí manipulační poplatek ve výši v přepočtu až několika desítek tisíc korun, který samozřejmě není možné odečíst ze slíbené výhry. V případě, že uživatel poplatek zaplatí, je po něm obvykle požadován další, dokud je ochoten platit. Zaplacené peníze a slíbenou výhru už nikdy neuvidí. V některých případech jsou požadovány od „výherce“ důvěrné informace nebo přístupové údaje k účtům například pod záminkou problému s převodem slibované výhry. Někdy „výherce“ zašle i scan svého osobního dokladu. Tyto informace mohou pak podvodníci snadno využít.

Obrázek 13 Grafická podoba emailu podvodné loterie[27]

3.8 Založení fiktivního bankovního účtu a nábor bílých koní

Aby podvodníci mohli získané peníze dostat až do svých kapes a pro policii zůstali co nejvíce anonymní, musí k tomuto využít bankovní účty, které nejsou spojeny s jejich osobou. K tomuto účelu jsou využívány tzv. „bílé koně“.

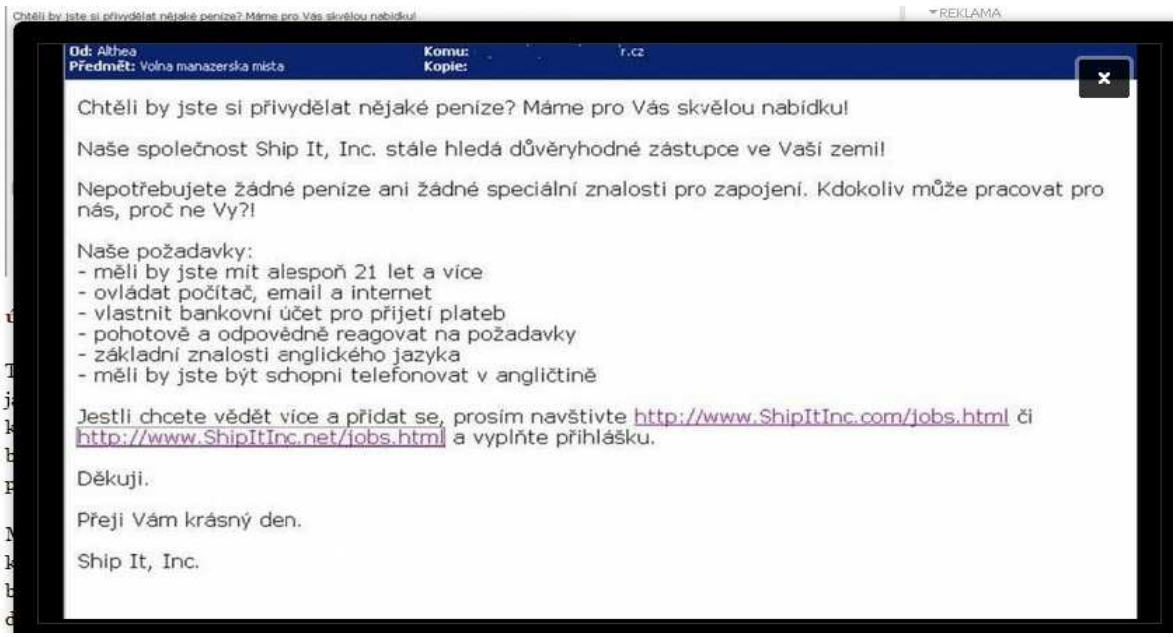
Jako bílý kůň se slangově označuje osoba, která je nastrčená k páchání trestné činnosti, aby zakryla skutečného pachatele nebo osobu, která má z této činnosti prospěch. Bílý kůň pak v daném případě figuruje jako pachatel i poškozený. K roli bílého koně bývá osoba často donucena vydíráním, může se ale také jednat o naivní nebo nevzdělanou osobu, která ani nemusí tušit, že se dopouští trestné činnosti. Zvláštním případem bílého koně jsou osoby, u

[27] *http://www.fightidentitytheft.com, 10. 12 .2013*

nichž se předpokládá, že vzhledem k jejich věku nebo duševnímu stavu bude soud jejich jednání posuzovat velmi mírně nebo od potrestání upustí. V některých případech bývají bílí koně nakonec zlikvidováni, aby se snížilo riziko prozrazení. [28]

Z osobních zkušeností při výkonu mé profese musím říct, že potrestání těchto bílých koní je v našem právním systému ojedinělé, neboť je velice těžké prokázat těmto osobám úmysl, to že věděli, že se dopouštějí protiprávního jednání.

Jak se takové bílé koně dají opatřit? Podvodníci si s tím, nedělají moc hlavu. Jednoduše si podají inzerát. Inzerát, ve kterém nabízejí práci za dobré finanční ohodnocení. Při zájmu o jimi inzerovanou práci, následně zájemci sdělí, že jsou ze zahraničí a aby si nemuseli v České republice zakládat účet, bude jeho činnost spočívat v tom, že mu na jeho účet budou zasílat peníze. On tyto peníze vždy vybere a následně je pošle přes jinou bankovní instituci na zahraniční účet. Z těchto peněz si bílý kůň může nechávat určité procento provize, nebo pobírá měsíční fixní plat. Osoba, která zde vystupuje v pozici bílého koně mnohdy ani netuší, že peníze, které jsou mu na účet posílány, pocházejí z trestné činnosti a pokud ano, je to velice těžké prokázat. Protože policie již takovéhle vystavené inzeráty monitoruje, nabízejí podvodníci možnost přivýdělku prostřednictvím elektronické pošty, kdy je v podobě spamu rozesílají do emailových schránek.



Obrázek 14 Email s nabídkou brigády pro získání bílých koní[29]

[28] http://cs.wikipedia.org/wiki/bílý_kůň
[29] Vlastní zdroj

Znění těchto inzerátů je vždy podobné. Podvodníci hledají osobu starší 18ti, někdy 21 let, která má v České republice založený svůj vlastní bankovní účet, z kterého může kdykoliv vybrat peníze a převést je do zahraničí. Při prostudování těchto emailových zpráv lze zjistit, že jsou rozesílány ze zahraničí. Šetření policie končí u těchto bílých koní a skuteční podvodníci zůstávají utajeni.

Pokud někteří podvodníci nechtějí dávat provizi bílému koni, nebo jim jeho použití přijde riskantní, použijí další možnost, kterou je založení si bankovního účtu na cizí jméno. Založení takového účtu není opět nijak složité. Na inzertním portálu zveřejní inzerát s nabídkou práce, tentokrát spíše běžné a nenápadné. Zájemci následně tomuto podvodníkovi zašlou na jeho žádost své životopisy. Po té obdrží email o tom, že byli vybráni do užšího výběru a jsou požádání o zaslání oskenovaného občanského průkazu, aby řádně prokázali svou totožnost a také o zaslání oskenovaného řidičského průkazu, aby doložili, že mají skutečně platný řidičský průkaz. Pro sjednání účtu v některých bankovních institucích postačí zadání telefonního čísla a dvou oskenovaných osobních dokladů, takto lze založit účet například u Airbank, ale tuto formu založení účtu poskytují už i jiné bankovní instituce.

3.9 Boj proti kyberkriminalitě

Prevence je v kyberkriminalitě důležitější a účinnější než následná represe. Protože vypátrat pachatele je v případě kyberkriminality zpravidla složitější. Zaměření se na prevenci v této oblasti je tedy stěžejní činnost k omezení páchání internetových podvodů. Prevenci bychom v tomto směru mohli rozlišit na technologickou a psychologickou.

Psychologická prevence spočívá ve zvýšení informovanosti společnosti o tom, jak se proti tomuto druhu kriminality účinně bránit, jak si ochránit svou identitu a nepřijít tak o své peníze či důležité informace.

Technologická prevence pak souvisí s technologickým zabezpečením, účinným šifrováním a jinými bezpečnostními prvky jako jsou například antivirové programy. Tato prevence ovšem není od běžného uživatele očekávána, tedy ne přímo. Většinou jsou mu tyto preventivní služby nabízeny za určitý finanční obnos a práce je pak přenechána profesionálům, tedy například zakoupení antivirového programu.

3.9.1 Technologická prevence

Do technologické prevence zařazujeme: antivirový program, firewall, kryptografické prostředky (šifrování), nástroje pro ověřování identity uživatelů.

Antivirový program je počítačový software sloužící k tomu, aby detekoval škodlivý software (malware) a bezpečně ho odstranil. Jedná se například o Norton AntiVirus, trend Micro, McAfee, Webroot, AVG a jiné. Antivirový program ovšem nemůže chránit počítač před všemi druhy útoků. Aby antivirový program rozeznal, zda se jedná o škodlivý software nebo software, který není uživateli počítače nebezpečný, používá k identifikaci těchto „virů“ jejich signaturu. Signatura je jedinečný bitový řetězec, který antivirový program používá k identifikaci viru.

Tyto škodlivé kódy jsou vyvíjeny po celém světě. Z historie počítačových virů bych ráda označila 5 neznámějších, kterými jsou:

- Brain vznikl v Pákistánu
- Černobyl, vnikl v Tchajwanu
- Michelangelo pochází ze Švédska, tento virus měl dne 6. 3. 1991 smazat z počítačů všechna data uživatelů. Ačkoliv se odhadovalo, že bude zasaženo více jak 5 milionů počítačů, díky včasném zásahu antivirových programů to bylo nakonec pouze okolo 10 000 počítačů.
- Tequilla vznikl ve Švýcarsku
- Yankee Doodle je z Ameriky, z roku 1989, tento virus se nechoval nijak škodlivě, pouze vždy v 5 hodin odpoledne přehrál na infikovaných počítačích část písničky „Yankee Doodle“.

K ochraně počítače proti škodlivému softwaru je potřeba několik bezpečnostních vrstev a antivirový program je jen jednou z nich. Dalším je již zmiňovaný firewall.

„Jako firewall označujeme zařízení či sadu opatření, která filtrují data přicházející do sítě (někdy i v opačném směru) a na základě určitých pravidel je propouští, nebo blokuje. Pomocí firewallů se na hranicích privátních sítí vytvářejí kontrolní body zabezpečení. Na těchto bodech jsou firewally a ty kontrolují všechny pakety, které mezi privátní sítí a internetem

procházejí a podle toho jak pakety splňují daná pravidla nastavená ve firewall, firewall určí, zda jednotlivé pakety propustit, nebo zablokovat.[30]

Pomocí šifrování je možno ochránit informace transportované z jednoho počítače do druhého. Šifrování je proces, kterým se informace (nešifrovaný text) za pomoci šifrovacího algoritmu transformuje na text zašifrovaný. K tomuto dochází pomocí matematické funkce a šifrovacího hesla. Dešifrování následně probíhá tak, že za pomocí speciálního hesla se šifrovaná informace opět dešifruje na srozumitelný text. Šifrování ovšem nezabrání ztrátě dat, jejich vymazání. Šifrovací klíč určuje šifrovacímu algoritmu jakým způsobem má data šifrovat a dešifrovat. Délka klíče musí být dostatečně dlouhá.

3.9.2 Smart-phony – chytré telefony

Chytré mobilní telefony jsou nejrychleji se rozrůstajícím komunikačním prostředkem, z kterého se lidé připojují k internetu. Podle Evropské agentury ENISA (European Network a Information Security Agency) překonají smart-phony v počtu zařízení denně se připojujících na internet poprvé klasické stolní počítače. Průzkumy poukazují na to, že většina uživatelů si stále neuvědomuje, že jejich chytré mobilní telefony jsou v důsledku technologického vývoje již na úrovni počítačů a přistupují k nim stále jako k analogovým mobilům z 90. let. Z výsledků ankety společností AVG a Ponemon Institute vyplývá, že pouze 29% vlastníků mobilních telefonů má na svém přístroji instalovaný antivirový program, anebo jeho instalaci alespoň zvažuje. Klasické osobní počítače mají nainstalovaný antivirový systém v celkovém počtu přes 80%. Tento poměr vychází ze zprávy McAfee, kdy dle jejich zjištění, mělo v roce 2012 antivirový program 83% osobních počítačů. V případě smart-phonů si většina lidí stále nezvykla používat určitou úroveň zabezpečení a proto se právě tyto chytré telefony stávají v poslední době stále častějším terčem útoku pachatelů. Nedostatek zabezpečení se netýká jen tabletů, ale také tabletů, u těch je úroveň zabezpečení podstatně nižší než u chytrých mobilních telefonů. Ze Situační zprávy II. pololetí 2013 Ministerstva vnitra České republiky vyplývá, že většina tvůrců počítačových virů se nově začne soustředit na chytré mobilní telefony a pro rok 2014 se všeobecně očekává exponenciální nárůst malwaru určeného právě pro tyto telefony.

Neznalost uživatelů je zde tedy zřejmá. Většina výrobců mobilních telefonů, tak již při prodeji vkládá do mobilního telefonu alespoň základní antivirový systém. Uživatelé ovšem i tak

[30] *Zemánek Jakub, Stavba a správa sítě, aneb cesta do hlubin internetu.*

umožní škodlivému malwaru přístup do jejich mobilního telefonu a tím i vlastně přístup k jejich citlivým údajům, jako je třeba přístup k bankovnímu účtu, či informace, které umožní podvodníkům připravit účinný phishingový útok za použití několika konkrétních pravdivých informací získaných právě z mobilního telefonu.

Uživatelé umožní přístup škodlivým kódům do jejich mobilního telefonu například přijatou elektronickou poštou, nebo stáhnutím aplikace z neověřeného appstoru. Nepozorní uživatelé tak někdy stáhnou aplikaci místo z originálních stránek Google Play z fiktivních stránek Google Plays, své kopie má pochopitelně i obchod App Store. Mnohé škodlivé aplikace jsou ovšem umístěny i na oficiálních stránkách těchto App Storů. Podle průzkumu Kaspersky Lab přišlo o veškerá svá data uložená na mobilním telefonu či tabletu více než 13% českých uživatelů. Celosvětový průzkum společnosti TrustPort, který probíhal ve 30 zemích, ukázal, že uživatelé využívající různé aplikace se příliš nezabývají čtením licenčních podmínek a podepíší jakékoliv licenční podmínky, jen aby mohli danou aplikace využívat. V podstatě tak vlastně mnohdy dávají svolení autorům aplikace ke sdílení údajů s třetími stranami.

Jedním ze známých malware, který napadal mobilní telefony je tzv. diallerware. Ten bez vědomí uživatele píše a volá na zpoplatněná čísla, na tzv. prémiové sms. Uživatel při tom až do přečtení telefonního účtu nemá vůbec povědomí o tom, co se s jeho mobilním telefonem děje. Různé formy diallerware představovaly v roce 2012 až 40% celkového objemu malware v mobilních telefonech. V USA byl tento problém vyřešen tak, že v roce 2013 největší američtí telefonní operátoři se zavázali již služby prémiových sms až na určité výjimky neprovozovat. Těmito výjimkami jsou pouze charitativní sms zprávy a sms zprávy na podporu volebních průzkumů. V České republice ovšem telefonní operátoři se zastavením těchto služeb nepočítají. Tímto důvodem je zejména vysoký zisk, kdy z některých prémiových sms zpráv si telefonní operátoři berou až 50% z ceny. Málo uživatelů je obeznámeno s tím, že právě tyto placené služby je možné si u svého operátora zablokovat a tím předejít nežádané ztrátě peněz.

3.10 Horké linky

Kyberkriminalita se neustále vyvíjí. Držet s ní krok a účinně ji potírat vyžaduje velké úsilí jak ze strany státních institucí, tak i nestátních. K tomu, aby mohl být boj efektivnější a pachatelé neměli dostatek času na „zametení“ stop začaly tyto instituce zakládat tzv. horké linky. Jejich podstatou je, že se právě samotní uživatelé mohou podílet na boji proti kriminalitě a hlásit

vše, co jim v prostředí internetu přijde podezřelé. Využít horkou linku k nahlášení podezřelého chování v prostředí internetu může kdokoliv, kdykoliv. Horká linka je další formou prevence, a dá se říct, že formou účinnou.

3.10.1 INHOPE

Mám-li psát o horkých linkách, musím nejdříve zmínit mezinárodní síť horkých linek INHOPE. Inhope je síť aktivních a spolupracujících 49 horkých linek působících ve 43 zemích. V rámci Inhope vznikla nadace Inhope, která od roku 2010 pomáhá se založením nových horkých linek ve světě. V současné době se tato nadace podílí na založení horkých linek v Kolumbii, Kazachstánu a Thajsku.[31]

Provozování horké linky v České republice nestátními institucemi, pracovníci této horké linky nahlášený obsah prověří, a pokud se domnívají, že nahlášené jednání je protiprávní, oznámí toto jednání Policii České republiky.

Jednu z horkých linek nestátních institucí lze nalézt na internetových stránkách www.horkalinka.cz. Provozovatelem těchto webových stránek je CZI, s.r.o., v rámci projektu Národního centra bezpečnějšího internetu. Národní centrum bezpečnějšího internetu je neziskové nevládní sdružení, založené v roce 2006 jako Online Safety Institute. V lednu 2011 bylo sdružení přejmenováno na Národní centrum bezpečnějšího internetu (NCBI). Toto sdružení spolupracuje s mezinárodní sítí horkých linek INHOPE a horkou linku provozuje od roku 2009. Protože při výkonu své profese pracovníky této horké linky spolupracuji, mohu říci, že prioritním obsahem, který tato linka Policii České republiky zasílá, je trestná činnost s podezřením na šíření dětské pornografie. Výhodou této horké linky je její úzká spolupráce právě s dalšími zahraničními horkými linkami. Pokud tedy pracovníci horké linky zjistí, že nezákonná činnost pochází mimo území České republiky, kontaktují příslušnou horkou linku té dané zemi. Zefektivňují tak postup, neboť oznámení této věci Policii České republiky a její následné kontaktování policie země, ve které k nezákonnému jednání došlo je z důvodu zákonných postupů značně zdlouhavější a tedy méně účinné.

Další provozovanou horkou linkou byla ještě do konce roku 2012 linka nazvaná Internet hotline, na internetových stránkách www.internethotline.cz provozovaná Nadací Naše dítě. Tento projekt byl oficiálně zahájen dne 1. 1. 2007 a byl podporován grantem z fondů

[31] www.inhope.org

Evropské komise do roku 2008. Od roku 2009 byla tato horká linka provozována díky podpoře Nadace Naše dítě. Ke dni 31. 12. 2012 Nadace naše dítě ukončila provoz této horké linky převážně z důvodu vzniku horké linky provozované Policií české republiky.

Tato možnost hlášení kyberkriminality přímo Policii České republiky, tedy již ne přes prostředníka, byla spuštěna ke dni 1. 8. 2012 a funguje do současné doby. Umístěna je na stránkách www.policie.cz a obsluhují ji vyškolení policisté.

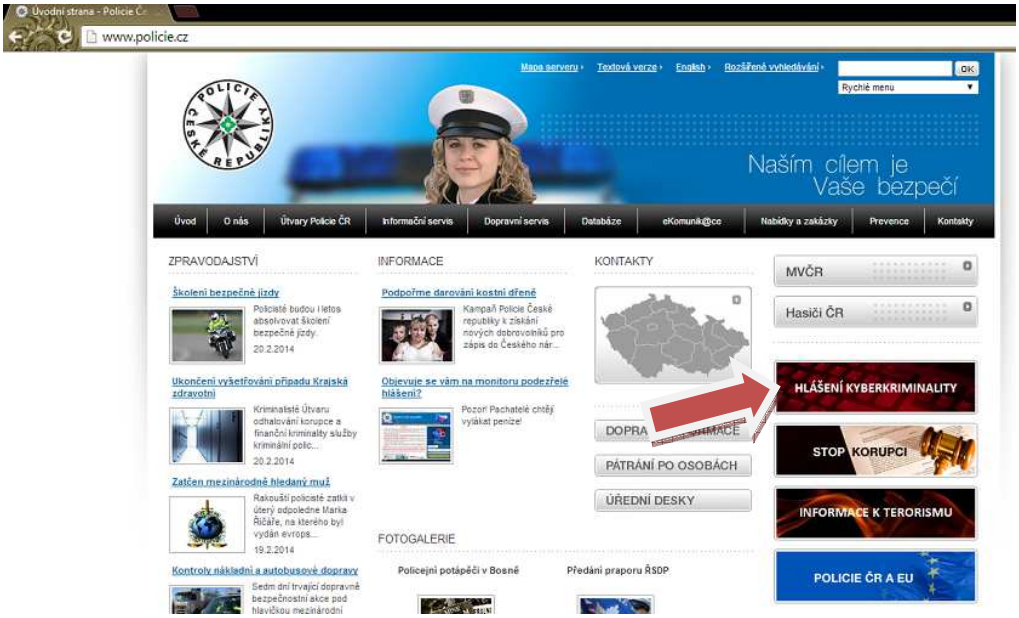
3.10.2 Policejní horká linka

Od 1. srpna roku 2012 vznikla v rámci informační kriminality v Policii České republiky horká linka, neboli tzv. „policejní hotline“. Cílem tohoto projektu je zefektivnění činnosti policie tím, že se tok informací potřebných k řádnému prověření podstatně zrychlí. Hlášení kyberkriminality se týká především případů dětské pornografie, extremistické propagandy, podvodů a neoprávněných přístupů k počítačovým systémům a nosičům informací.

Tím, že zaslané poznatky putují rovnou ke specializovaným policistům, mohou tito ihned reagovat a zajistit tak informace, které jsou na internetu mnohdy pouze dočasně. Hotline je dostupná na internetových stránkách www.policie.cz. Za rok 2012, tedy za období od srpna do prosince činil součet přijatých oznámení 1610, za rok 2013 bylo prostřednictvím tohoto internetového formuláře přijato 3 829 oznámení. Což je více jak dvojnásobek hlášení, která byla přijímána nestátními horkými linkami. Celkově bylo od prvního spuštění této horké linky ode dne 1. 8. 2012 do konce roku 2013 přijato 5 439 oznámení. Roční průměr za podání za rok 2013 činí 10,5 podání na den. Ovšem není výjimkou i přijetí přes 100 oznámení za jeden den. Z těchto přijatých oznámení bylo přes 300 oznámení týkající se malwaru vydávající se za Policii České republiky „ransomwaru“. Za rok 2013 bylo z celkových 3 829 oznámení oznámeno 564 podvodů, tedy 15% všech těchto oznámeních, v tomto čísle ovšem není započítáno podvodné vylákání peněz prostřednictvím právě zmiňovaného ransomwaru, neboť tento skutek je v celkové statistice zpracován pod trestným činem neoprávněný přístup k počítačovému systému a nosiči informací. Pokud bychom tato hlášení započítali k hlášením vyhodnoceným jako podvod, činil by poměr zastoupení těchto majetkových trestných činů přes 22%.

Jako jednu z hlavních výhod této horké linky vidím možnost rychlé komunikace s oznamovatelem. Pokud oznamovatel na sebe zanechá kontakt a ve svém oznámení se dotazuje na postup v případě, že se domnívá, že by se mohl stát obětí podvodu, může mu

policista ihned po přijetí a vyhodnocení přijatého oznámení odpovědět a zabránit tak podvodnému jednání. Jedním z příkladů je hlášení oznamovatelů o napadení ransomwaru. Ve větším množství případů se oznamovatelé dotazovali, zda výzva na jejich monitoru o uhrazení pokuty ve výši několika tisíců korun je reálná či nikoliv, v těchto případech byli vyrozuměni, aby předmětnou částku nehradili a bylo tak zabráněno způsobení škody.



Obrázek 15 Internetové stránky www.policie.cz odkaz na formulář hlášení kyberkriminality[32]

[32] www.policie.cz, 12. 12. 2013

4 Praktická část

4.1 Vyhodnocení zadaného dotazníku

Jako jednu z metod jak zjistit informovanost lidí při nakupování prostřednictvím internetu jsem zvolila dotazník (viz. příloha č. 1). V rámci dotazníkového šetření jsem vybrala 84 respondentů. Jako klíč při výběru těchto respondentů jsem zvolila dva hlavní atributy, a to pohlaví a věk. Mým cílem bylo, aby počet mužů a žen byl v dotazníkovém šetření zastoupen rovným dílem, tedy 42 a 42, což se také podařilo. Dále jsem zvolila rozdělení respondentů do věkových skupin. Celkem jsem respondenty rozdělila do 6 věkových skupin. Konkrétně se jedná o tyto skupiny: 16 – 25 let, 26 – 35 let, 36 – 45 let, 46 – 55 let, 56 – 65 let a 65 a více let. Každá z těchto skupin měla zastoupení 14 respondentů. Cílem tohoto rozdělení bylo zjistit, zda jsou v bezpečnosti při nakupování opatrnější a informovanější ženy nebo muži a dále zda má na tuto opatrnost a informovanost vliv věk dotazovaných, tedy zda se jednotlivé věkové generace liší. Prostřednictvím tohoto dotazníku jsem ověřovala svoji hypotézu, že není rozdíl mezi pohlavím či věkovými skupinami v opatrnosti a informovanosti při používání internetu, v tomto případě při nakupování prostřednictvím internetu.

U dotázaných respondentů jsem zároveň zjišťovala jejich nejvyšší dosažené vzdělání. Ze zjištěných informací tak vyplynulo, že můj dotazník vyplnil jeden člověk se základním vzděláním, 17 vyučených respondentů, 35 respondentů s maturitou, 21 lidí s dosaženým titulem Bc. Nebo DiS. a 10 vysokoškolsky vzdělaných s dosaženým titulem Mgr. a Ing. . Dotazníky byly předloženy v klubu důchodců, kam docházejí moji rodiče, dále byly předloženy mezi studenty na Univerzitě Karlově, fakultě farmacie a zbytek mezi mé známé a rodinu, aby mohly být dodrženy atributy výběru.

Složení respondentů je blíže znázorněno v tabulkách uvedených níže (tabulka č. 1, tabulka č. 2).

Tabulka 1 respondenti pohlaví x vzdělání

Tabulka 1	POČET
MUŽ ZŠ	0
ŽENA ZŠ	1
MUŽ vyučen	6
ŽENA vyučena	11
MUŽ SŠ maturita	19
ŽENA SŠ maturita	16
MUŽ Bc., DiS.	8
ŽENA Bc. DiS.	13
MUŽ Mgr., Ing.	9
ŽENA Mgr., Ing.	1
CELKEM	**84**

Tabulka 2 respondenti pohlaví x věk

Tabulka 2	POČET
MUŽ 16 - 25	9
ŽENA 16-25	5
MUŽ 26 - 35	7
ŽENA 26-35	7
MUŽ 36 - 45	10
ŽENA 36-45	4
MUŽ 46 - 55	8
ŽENA 46-55	6
MUŽ 56 - 65	4
ŽENA 56-65	10
MUŽ 65+	4
ŽENA 65+	10
CELKEM	**84**

Otázka č. 1

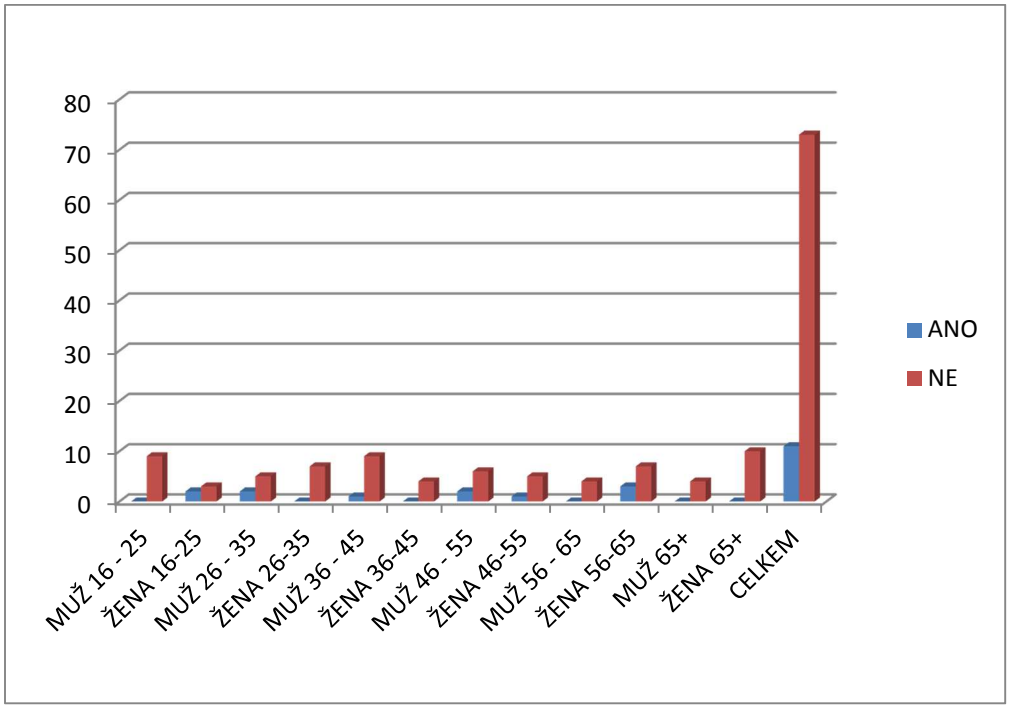
Byl/a jste někdy prostřednictvím internetu podveden/a? Pokud ano, jaká celková škoda Vám tím byla způsobena?

Na tuto otázku mi odpovědělo všech 84 respondentů. Z těchto 84 respondentů jich 11 uvedlo, že se stali obětí podvodu spáchaného prostřednictvím internetu. Jedná se tedy o 13% dotázaných. Z těchto 11 respondentů bylo 5 mužů a 6 žen. Tedy mezi podvedenými muži a ženami není jejich počtu zastoupení podstatný rozdíl. Tyto skupiny jsou téměř vyrovnané. Z hlediska věku po té byl nejmenší počet podvedených ve věku 65+, kdy v této věkové skupině nebyl podveden pouze žádný respondent. Nejvíce podvedených bylo ve věkových skupinách 46 – 55 a 56 – 65 let, kdy v každé této skupině byli podvedeni tři respondenti.

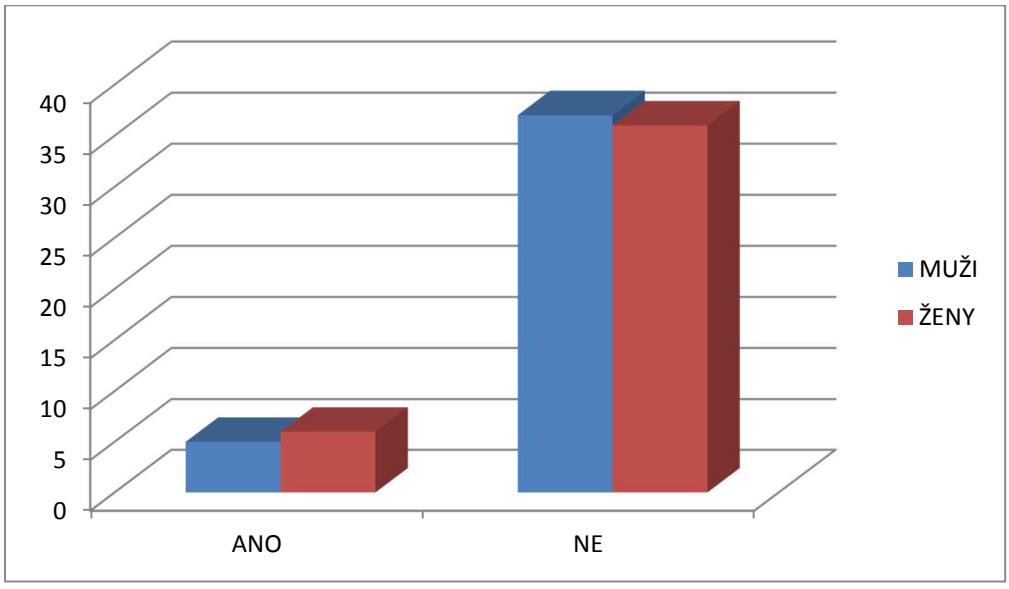
Podíváme-li se ovšem na výši způsobené škody z hlediska věkových skupin, zjistíme, že z celkové způsobené škody u 11 podvedených respondentů, která činila 136.280,- Kč, byla nejvyšší způsobená škoda ve výši 120.000,- Kč způsobena respondentovi z věkové skupiny 36 – 45 let. Tato skutečnost ovšem o ničem nevypovídá, neboť jde pouze o jednoho respondenta. Způsobená výše škody tedy nemá žádnou vypovídající hodnotu k potvrzení či vyvrácení stanovené hypotézy.

Tabulka 3 Otázka č.1 respondenti pohlaví x věk

Otázka 1	ANO	NE	Výše škody
MUŽ 16 - 25	0	9	0
ŽENA 16-25	2	3	2400
MUŽ 26 - 35	2	5	3100
ŽENA 26-35	0	7	0
MUŽ 36 - 45	1	9	120000
ŽENA 36-45	0	4	0
MUŽ 46 - 55	2	6	8500
ŽENA 46-55	1	5	480
MUŽ 56 - 65	0	4	0
ŽENA 56-65	3	7	1800
MUŽ 65+	0	4	0
ŽENA 65+	0	10	0
CELKEM	11	73	136280



Graf 1 Otázka č. 1 respondenti pohlaví x věk



Graf 2 Otázka č.1 Respondenti pohlaví

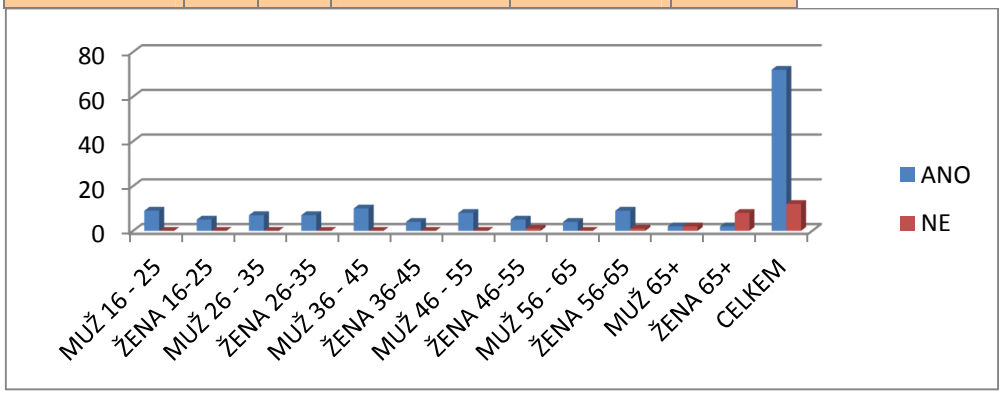
Otázka č. 2

Provedl jste někdy nákup zboží či služeb prostřednictvím internetu? A jak často?

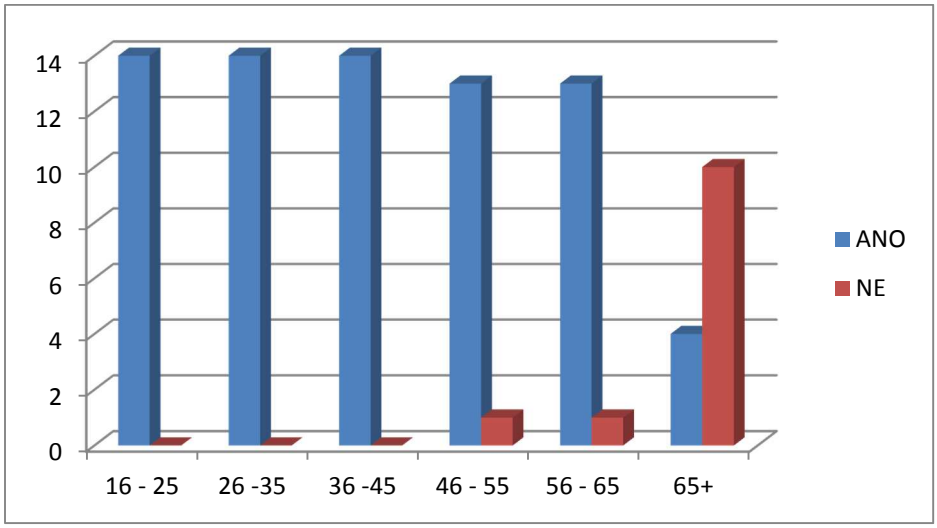
Otázka číslo 2 je otázkou rozřazující. Zodpovězení této otázky vymezilo 72 respondentů, kteří nakupují nebo v minulosti nakoupili zboží či službu prostřednictvím internetu. Z 84 dotázaných se tedy 72 lidí vyjádřilo, že prostřednictvím internetu již nakoupili či nakupují. Z těchto 72 lidí je 40 mužů a 32 žen. Nejmenší zkušenost s nákupy přes internet mají ženy starší 65 let. Součástí této otázky byla zároveň podotázka určená ke zjištění jak často dotázaní na internetu nakupují. Na vybranou měli jednu ze tří možností: 1x až 3x ročně, 4x až 12x ročně a více jak 12x ročně. Výsledkem bylo zjištění, že 16 respondentů využívá internet k nákupu jen zřídka maximálně 3x do roka. 45 respondentů tedy 62,5% využívá internet k nákupům v průměru maximálně jednou měsíčně a 11 respondentů využívá k nákupům internet často, více jak 12x za rok.

Tabulka 4 Otázka č. 2 respondenti pohlaví x věk

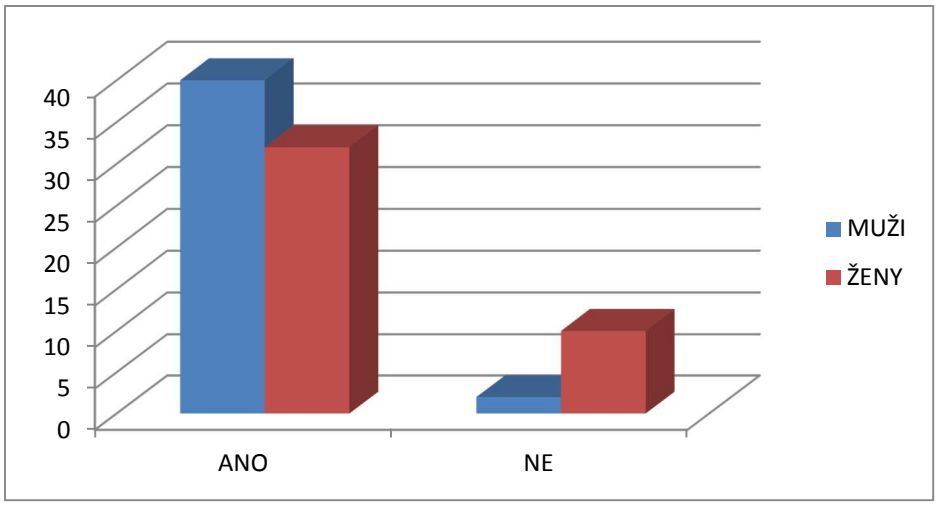
Otázka 2	ANO	NE	1x-3x/rok	4x-12x/rok	>12x/rok
MUŽ 16 - 25	9	0	0	9	0
ŽENA 16-25	5	0	2	3	0
MUŽ 26 - 35	7	0	0	5	2
ŽENA 26-35	7	0	0	2	5
MUŽ 36 - 45	10	0	0	6	4
ŽENA 36-45	4	0	0	4	0
MUŽ 46 - 55	8	0	1	7	0
ŽENA 46-55	5	1	0	5	0
MUŽ 56 - 65	4	0	3	1	0
ŽENA 56-65	9	1	6	3	0
MUŽ 65+	2	2	2	0	0
ŽENA 65+	2	8	2	0	0
CELKEM	72	12	16	45	11



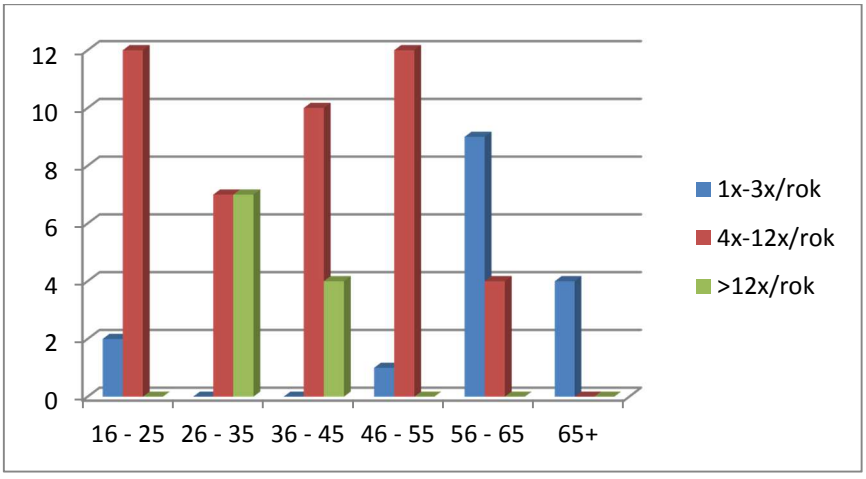
Graf 3 Otázka č. 2 respondenti pohlaví x věk



Graf 4 Otázka č. 2 Respondenti věkové skupiny



Graf 5 Otázka č. 2 Respondenti pohlaví



Graf 6 Otázka č. 2 Častost nákupů přes internet dle věkových skupin

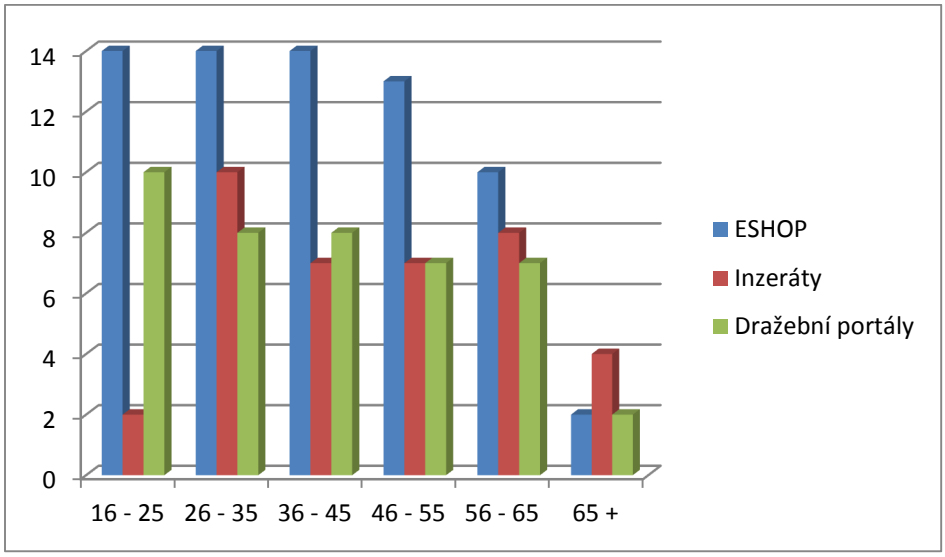
Otázka č. 3

Jakým způsobem na internetu nakupujete? Elektronický obchod (eshop), inzeráty, dražební portály (vyberte všechny možnosti, které používáte)

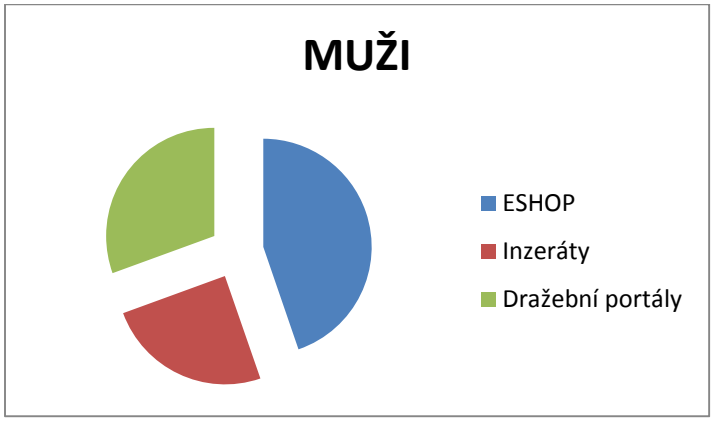
Tato otázka byla určena ke zjištění, jaký způsob nakupování prostřednictvím internetu respondenti nejvíce preferují a využívají. Ze získaných odpovědí vyplynulo, že nejčastějším způsobem respondenti nakupují prostřednictvím elektronických obchodů. Elektronický obchod využilo 67 dotázaných z celkových 72. 42 respondentů nakoupilo prostřednictvím dražebních portálů, kdy nejčastějšími využitými dražebními portály jsou Aukro, Mimibazar. Ve všech věkových skupinách s výjimkou věkové skupiny 65+ využívají respondenti nejvíce nakupování v elektronických obchodech. Věková skupina 65+ naopak více nakupuje zboží přes internet prostřednictvím zde zveřejněných inzerátů.

Tabulka 5 Otázka č. 3 Respondenti věk x pohlaví

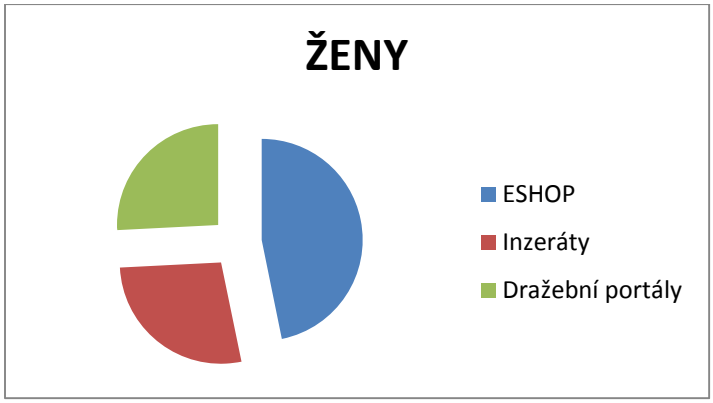
Otázka 3	ESHOP	Inzeráty	Dražební portály
MUŽ 16 - 25	9	2	8
ŽENA 16-25	5	0	2
MUŽ 26 - 35	7	5	5
ŽENA 26-35	7	5	3
MUŽ 36 - 45	10	5	8
ŽENA 36-45	4	2	0
MUŽ 46 - 55	8	3	3
ŽENA 46-55	5	4	4
MUŽ 56 - 65	4	4	2
ŽENA 56-65	6	4	5
MUŽ 65+	0	2	0
ŽENA 65+	2	2	2
CELKEM	67	38	42



Graf 7 Otázka č. 3 Respondenti věk x pohlaví



Graf 8 Otázka č. 3 Odpovědi muži



Graf 9 Otázka č. 3 Odpovědi ženy

Otázka č. 4

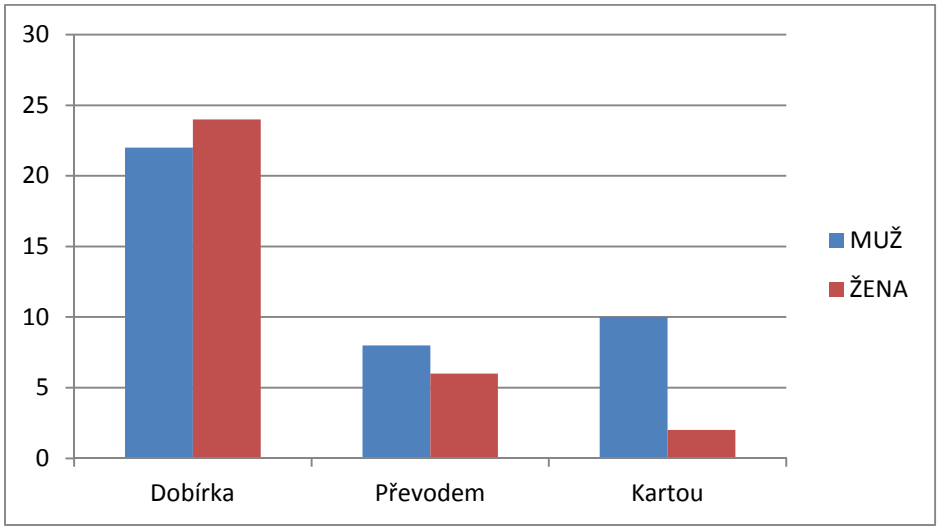
Jaký preferujete druh platby při nakupování přes internet?

Otázka číslo 4 byla položená za účelem zjištění, zda respondenti při nákupu přes internet volí raději platbu na dobírku nebo platbu předem a v případě platby předem, zda preferují platbu, při které předávají údaje ke své platební kartě, tedy platbu kreditní kartou. Ze 72 respondentů, jich 46 tedy více jak polovina preferuje bezpečnější platbu, tedy platbu na dobírku, tedy až po obdržení zboží. Naproti tomu 26 respondentů dává přednost platbě předem. Z toho 14 respondentů volí raději platbu převodem na účet nežli platbu prostřednictví platební karty.

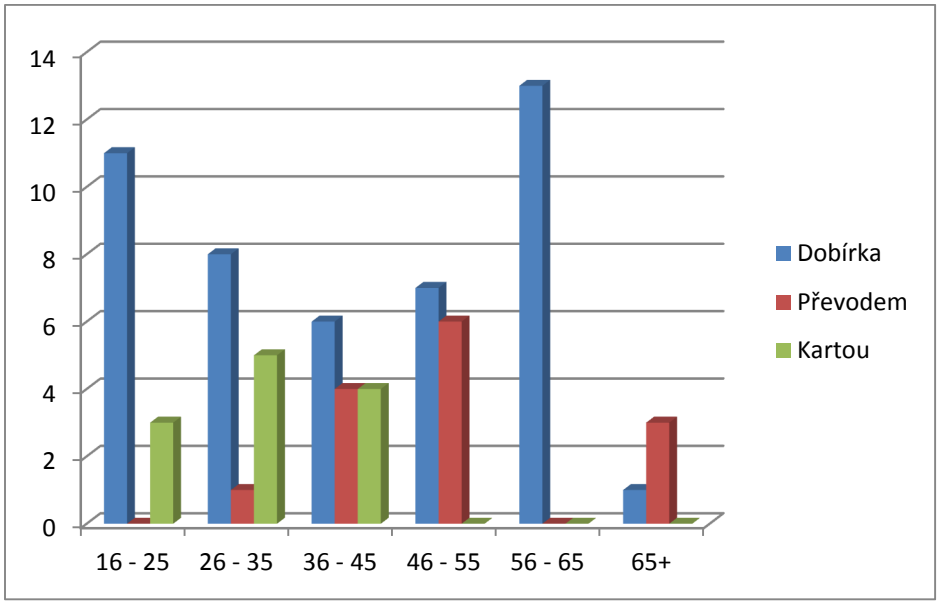
Podíváme-li se na výsledky z pohledu rozdílu mezi muži a ženami, tak zjistíme, že rozložení je následující 55% mužů a 75% žen volí bezpečnější možnost platbu za zboží na dobírku. Platbu předem převodem na účet volí 20% mužů a 19% žen, zde jsou poměry vyrovnané. Nejméně bezpečnou, avšak nejjednodušší a nejrychlejší možnost platby, platbu předem platební kartou preferuje 25% mužů a pouze 6% žen. Možnost placení platební kartou využívají nejčastěji muži od 16 do 45 let, starší muži již tuto možnost nevyužívají. Z výsledků vyplývá, že v případě způsobu platby jsou ženy opatrnější než muži a stejně tak i starší věkové skupiny jsou při volbě způsobu uhrazení ceny zboží opatrnější než mladší. Věkové skupiny od 46 let výše odpověděly, že nevyužívají k platbě přes internet platební kartu vůbec.

Tabulka 6 Otázka č. 4 Respondenti pohlaví x věk

Otázka číslo 4	Dobírka	převodem	platební kartou
MUŽ 16 - 25	6	0	3
ŽENA 16-25	5	0	0
MUŽ 26 - 35	3	1	3
ŽENA 26-35	5	0	2
MUŽ 36 - 45	4	2	4
ŽENA 36-45	2	2	0
MUŽ 46 - 55	4	4	0
ŽENA 46-55	3	2	0
MUŽ 56 - 65	4	0	0
ŽENA 56-65	9	0	0
MUŽ 65+	1	1	0
ŽENA 65+	0	2	0
CELKEM	46	14	12



Graf 10 Otázka č. 4 Odpovědi dle pohlaví



Graf 11 Otázka č. 4 Odpovědi dle věkových skupin

Otázka č. 5

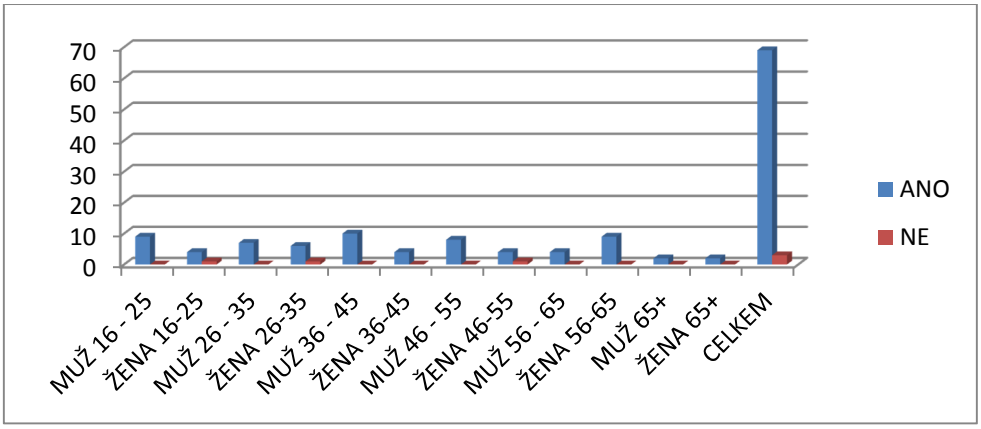
Představte si, že jste na internetu objevil Vám do této doby neznámý elektronický obchod s výhodnou cenou Vámi požadovaného výrobku a máte zájem si ho zakoupit. Ověřil byste si tento obchod před tím, než byste zde nakoupil?

Na tuto otázku odpovědělo 69 respondentů, že by si obchod ověřili před tím, než by zde nakoupili. Pouze tři lidé uvedli, že by si obchod neprověřovali. Všechny tři byly ženy, žádný z mužů nevybral variantu ne. Jelikož takto položená otázka je sugestivní a navádí respondenty ke zcela zřejmé odpovědi, což se projevilo i ve vyhodnocení této otázky. Byla u této otázky zároveň uvedena podotázka, která ty respondenty (69 dotázaných), kteří uvedli, že by si obchod prověřili, alespoň částečně zhodnotila tím, že byli vyzváni k uvedení konkrétních kroků, které by učinili při snaze elektronický obchod prověřit. Při této otázce nebyly dány možnosti k výběru, ale otázka byla volná. Odpovědi byly následně vyhodnoceny a rozřazeny do jednotlivých kategorií.

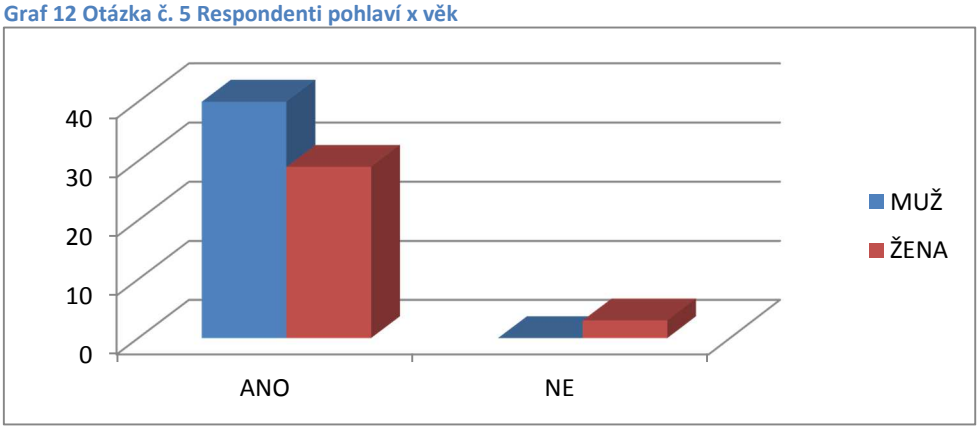
Z výsledku vyplynulo, že z 69 respondentů jich 5 neuvedlo žádný způsob prověření a políčko nechali prázdné. Jelikož respondenti vyplňovali dotazník samostatně bez asistence tazatele, nelze konstatovat, zda těchto 5 dotazovaných žádný způsob neznalo či jen necítili potřebu políčko vyplňovat a nad odpovědí přemýšlet. Přesto těchto 5 respondentů bych na základě toho, že nebyli schopni uvést nějaký způsob, zařadila mezi ty, kteří by si obchod nijak neprověřovali a celkový poměr by tak byl 64 ku 8 z dotázaných. Z 64 respondentů všichni uvedli, že by název obchodu zadali do vyhledávače (43 specifikovali vyhledávač na seznam.cz, google.com nebo heuréka.cz). U 40 dotázaných byl tento způsob jediný, který by k prověření obchodu použili. 10 dotázaných uvedlo jako další způsob ověření na internetových stránkách k tomu určených tedy www.podvodnici.cz a jiné. 8 respondentů uvedlo více jak dva způsoby prověření. 7 z nich uvedlo jako způsob ověření si identifikačního čísla obchodu a sídla obchodu v obchodním rejstříku či živnostenském rejstříku. 5 respondentů uvedlo, že by zkontrolovali datum založení internetových stránek elektronického obchodu. 4 respondenti uvedli, že v případě inzerátu by požadovali po prodejci zaslání více fotografií.

Tabulka 7 Otázka č. 5 Respondenti pohlaví X věk

Otázka 5	ANO	NE
MUŽ 16 - 25	9	0
ŽENA 16-25	4	1
MUŽ 26 - 35	7	0
ŽENA 26-35	6	1
MUŽ 36 - 45	10	0
ŽENA 36-45	4	0
MUŽ 46 - 55	8	0
ŽENA 46-55	4	1
MUŽ 56 - 65	4	0
ŽENA 56-65	9	0
MUŽ 65+	2	0
ŽENA 65+	2	0
CELKEM	69	3



Graf 12 Otázka č. 5 Respondenti pohlaví x věk



Graf 13 Otázka č. 5 Odpovědi dle pohlaví

Otázka č. 6

Pokud by v obchodě, kde nakupujete poprvé, byla v případě platby předem poskytnuta 20% sleva na zakoupené výrobky na rozdíl od plné ceny v případě zaslání na dobírku, zvolil byste tuto možnost platby (tedy platbu předem)?

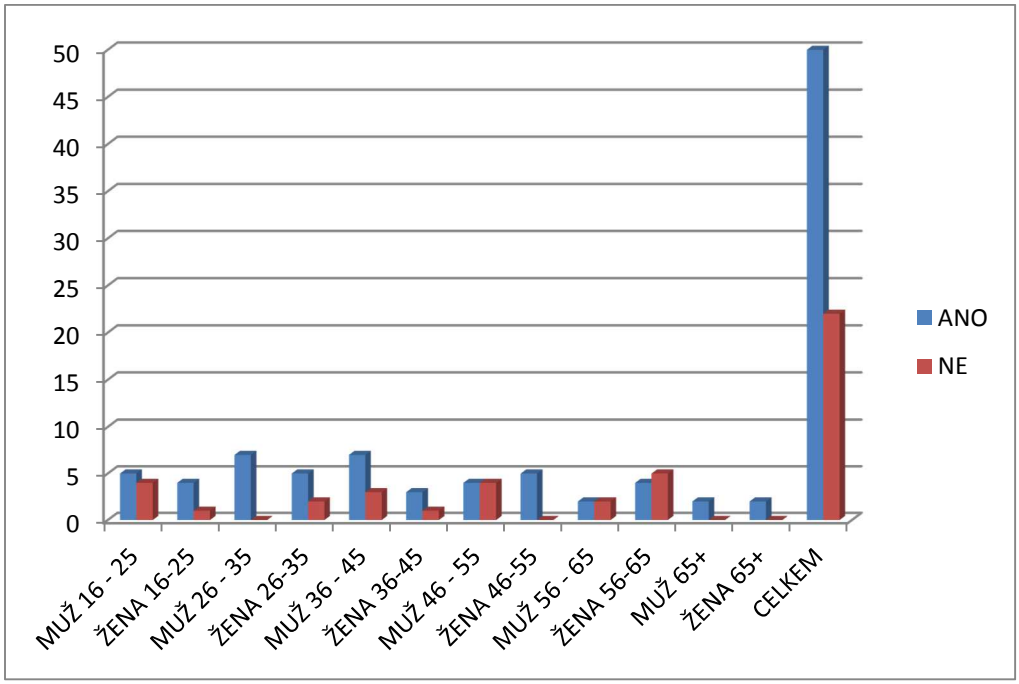
V odpovědích na tuto otázku se poměr respondentů, kteří by volili platbu předem, podstatně změnil oproti otázce číslo 4. V případě výhodnější ceny by uhradilo peníze za zboží předem 50 respondentů oproti 26 respondentům z otázky číslo 4. Taková to změna je podstatná, neboť podvodníci v úmyslu navést kupující k platbě předem volí jako přesvědčovací metodu právě výhodnější cenu za zboží, či výhodnější cenu za poštovné.

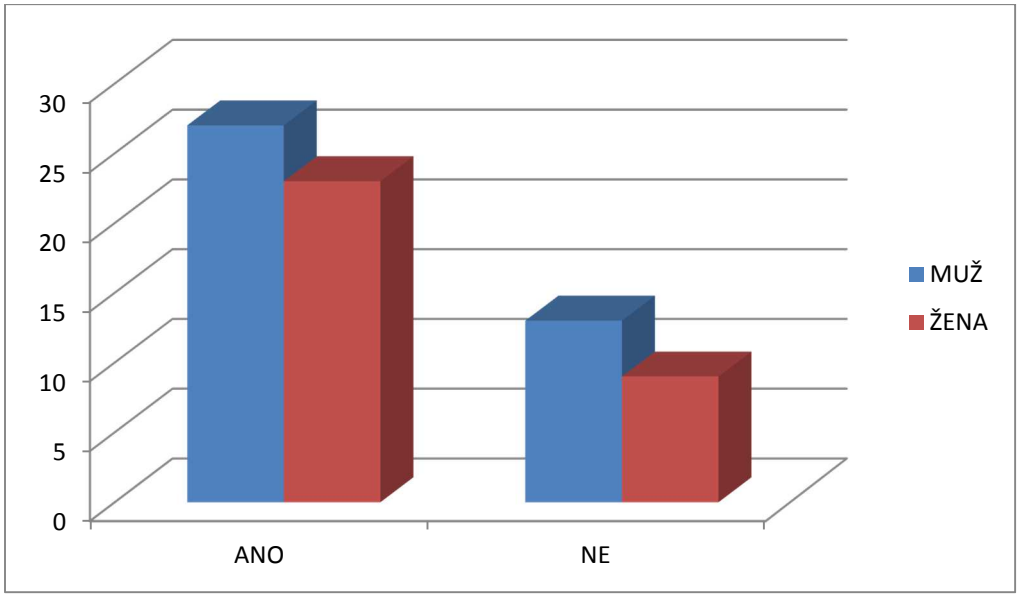
Platbu předem by zvolilo 27 mužů ze 40 dotázaných a 23 žen z celkového počtu 32. Tedy v případě mužů to je necelých 68%, v případě žen pak 72%. Obě tyto skupiny se tedy ve své odpovědi neliší. Z pohledu věku, jediná věková skupina 56 – 65 měla převahu svých odpovědí v možnosti NE, tedy, že by ani v případě lepší ceny platbu předem nezvolili. Konkrétně se v této skupině takto vyjádřilo 7 respondentů z celkových 13.

Tabulka 8 Otázka č. 6 Respondenti pohlaví x věk

Otázka 6	ANO	NE
MUŽ 16 - 25	5	4
ŽENA 16-25	4	1
MUŽ 26 - 35	7	0
ŽENA 26-35	5	2
MUŽ 36 - 45	7	3
ŽENA 36-45	3	1
MUŽ 46 - 55	4	4
ŽENA 46-55	5	0
MUŽ 56 - 65	2	2
ŽENA 56-65	4	5
MUŽ 65+	2	0
ŽENA 65+	2	0
CELKEM	50	22

Tabulka 9 Otázka č. 6 Respondenti pohlaví x věk





Graf 14 Otázka č. 6 Odpovědi dle pohlaví

Otázka č. 7

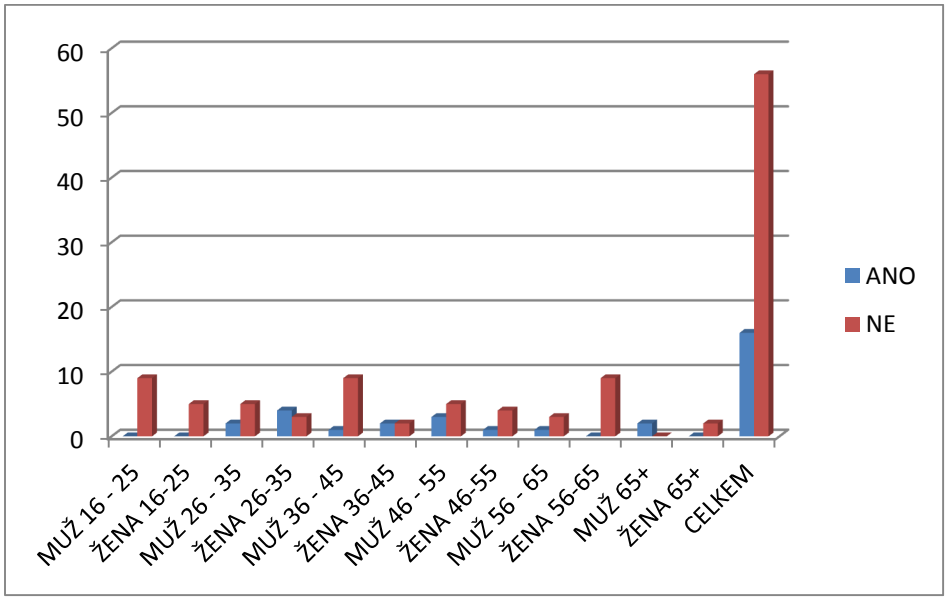
Pokud nakupujte zboží prostřednictvím elektronického obchodu, pročítáte si jeho obchodní podmínky?

Pročítání si obchodních podmínek je jedním ze základních kroků, které by měl kupující k ochraně svých peněz podniknout. Nejenže se dozví, jaké jsou například možnosti reklamace zakoupeného zboží, ale mnozí podvodních kopírují obchodní podmínky z jiných elektronických eshopů a tyto dále neupravují, při jejich pročtení může vyjít najevo, že obchodní podmínky se týkají úplně jiného elektronického obchodu.

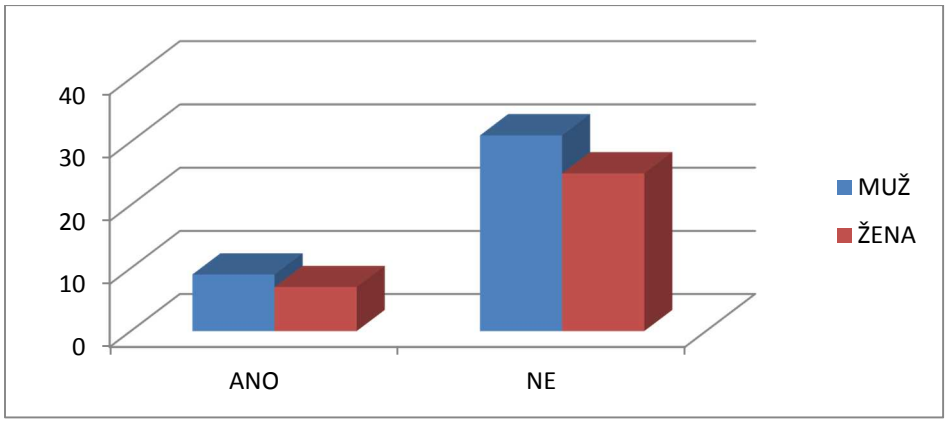
Výsledkem odpovědí na tuto otázku bylo zjištěno, že respondenti v převážné míře obchodní podmínky nepročítají. Respondenti tedy odpověděli v tomto poměru 56 z nich, tedy 78% si obchodní podmínky nepročítá oproti 16ti, kteří tak činí. Podíváme-li se opět na rozložení odpovědí mezi ženami a muži, zjistíme, že 78% žen a téměř 78% mužů obchodní podmínky nečte. Odpovědi mezi muži a ženami jsou tak opět vyrovnané. Rozdíl mezi věkovými skupinami taktéž není nijak významný.

Tabulka 10 Otázka č. 7 Respondenti pohlaví x věk

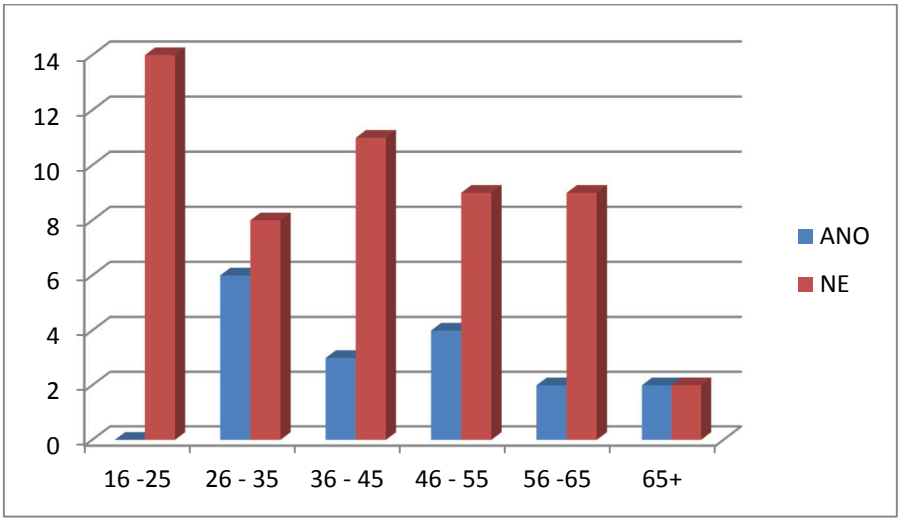
Otázka 7	ANO	NE
MUŽ 16 - 25	0	9
ŽENA 16-25	0	5
MUŽ 26 - 35	2	5
ŽENA 26-35	4	3
MUŽ 36 - 45	1	9
ŽENA 36-45	2	2
MUŽ 46 - 55	3	5
ŽENA 46-55	1	4
MUŽ 56 - 65	1	3
ŽENA 56-65	0	9
MUŽ 65+	2	0
ŽENA 65+	0	2
CELKEM	16	56



Graf 15 Otázka č. 6 Respondenti pohlaví x věk



Graf 16 Otázka č. 7 Odpovědi dle pohlaví



Graf 17 Otázka č. 7 Odpovědi dle věkových skupin

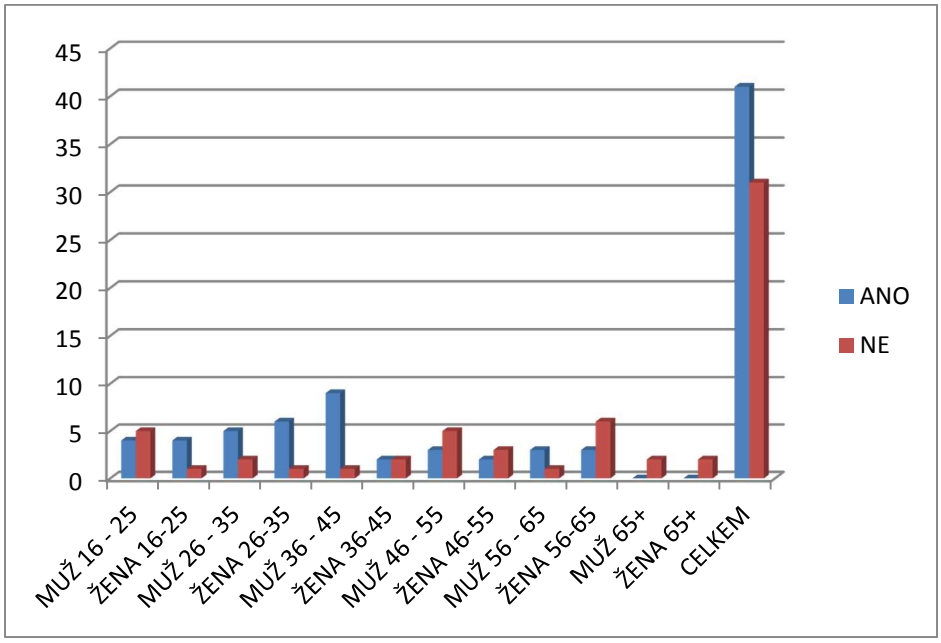
Otázka č. 8

Znáte certifikáty důvěryhodnosti elektronických obchodů, které jsou u některých elektronických obchodů uvedeny (např. APEK, HEUREKA)?

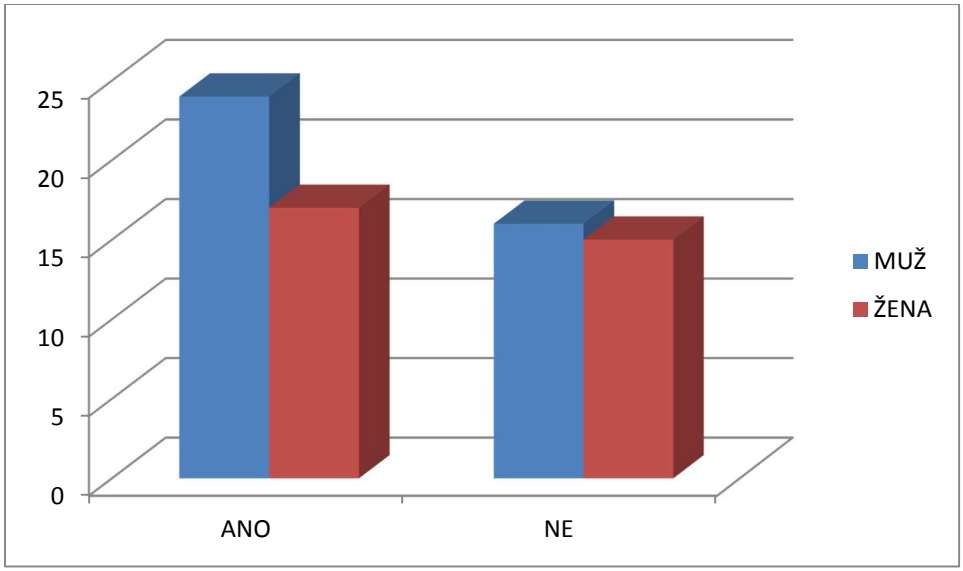
Tato otázka byla položena za účelem zjištění znalostí ohledně nakupování prostřednictvím internetu. Certifikáty důvěryhodnosti se nacházejí již u mnoha elektronických obchodů a mě tedy zajímalo, zdali si respondenti těchto certifikátů při nakupování po internetu všimli či zda mají povědomí, že nějaké takové hodnocení funguje. Z odpovědí vyplynulo, že 60% dotázaných mužů a 53% žen tyto certifikáty zná. Rozdíl mezi muži a ženami tak opět není nijak velký a jejich znalosti ohledně certifikátů důvěryhodnosti se neliší. Rozdíl je naopak vidět ve věkových skupinách. Zatímco mladší věkové skupiny tyto certifikáty z většiny znají, starší věkové skupiny ne.

Tabulka 11 Otázka č. 8 Respondenti pohlaví x věk

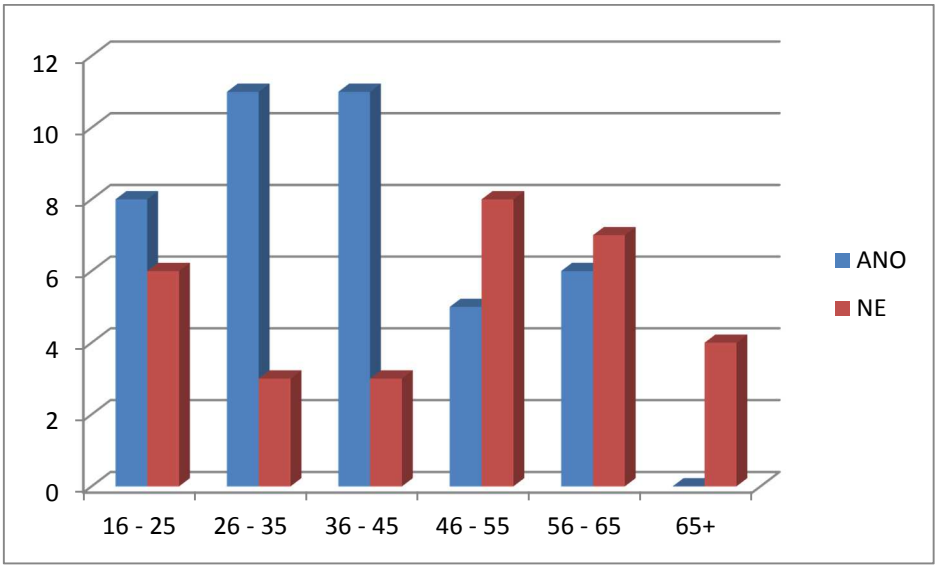
Otázka 8	ANO	NE
MUŽ 16 - 25	4	5
ŽENA 16-25	4	1
MUŽ 26 - 35	5	2
ŽENA 26-35	6	1
MUŽ 36 - 45	9	1
ŽENA 36-45	2	2
MUŽ 46 - 55	3	5
ŽENA 46-55	2	3
MUŽ 56 - 65	3	1
ŽENA 56-65	3	6
MUŽ 65+	0	2
ŽENA 65+	0	2
CELKEM	41	31



Graf 18 Otázka č. 8 Respondenti pohlaví x věk



Graf 19 Otázka č. 8 Odpovědi dle pohlaví



Graf 20 Otázka č. 8 Odpovědi dle věkových skupin

Celkové vyhodnocení dotazníku

Po celkovém vyhodnocení všech odpovědí na položené otázky nebyl zjištěn žádný podstatný rozdíl mezi muži a ženami ve vědomostech o bezpečném nakupování na internetu. Mnou stanovená hypotéza, že není rozdíl mezi muži a ženami ve znalostech bezpečného chování na internetu, zejména při nákupu zboží se potvrdila. V těchto znalostech však byl patrný rozdíl mezi jednotlivými věkovými skupinami. Z vyhodnocení odpovědí vyplývá, že mladší věkové skupiny jsou se znalostmi ohledně bezpečnějšího nakupování prostřednictvím internetu na vyšší úrovni než starší ročníky. Starší ročníky ovšem volí bezpečnější formy nakupování, například neplacení zakoupeného zboží platební kartou. Tato skutečnost je ovšem způsobena právě menšími zkušenostmi s nakupováním přes internet. Má druhá hypotéza, že není rozdíl ve znalostech bezpečného chování na internetu, zejména při nákupu zboží se tedy nepotvrdila. Z vyhodnocení jednotlivých odpovědí bych ještě vyzdvihla skutečnost, že respondenti, kteří uvedli, že nakupují prostřednictvím internetu více jak 12x do roka, jsou právě ti, kteří se chovají nejvíce rizikově, tedy platbu provádějí platební kartou a nečtou obchodní podmínky.

4.2 Analýza konkrétního případu

Jeden z respondentů, který v dotaznících uvedl, že již byl podveden při nákupu zboží přes internet a výše způsobené škody v dotaznících značně převyšovala škodu způsobenou ostatním respondentům, je můj příbuzný. Podveden byl v roce 2011 a byla mu způsobena škoda ve výši 120.000,- Kč. Ačkoliv se v praxi setkávám s případy podvedených lidí prostřednictvím internetu téměř denně a mohla bych zde analyzovat jakýkoli z těchto trestných činů, vybrala jsem si právě tento, neboť nijak nezasahoval do mé práce a já se s ním setkala pouze jako civilní osoba.

Vše začalo, když můj příbuzný, dále ho budu nazývat Pavel, se rozhodl zakoupit automobil. Jedná se o muže bydlícího na vesnici, povoláním je hasič. Jeho znalost bezpečného pohybu po internetu, bych ohodnotila na nižší úrovni. Protože má syna, který čerstvě vystudoval elektrotechnickou fakultu a věnuje se programování, bylo mu z jeho strany doporučeno, ať se poohlídne po nějakém vozidle na internetu, nejlépe na inzeráty na inzertním portále sauto.cz. Pavel tedy pročítal inzeráty na inzertním portále sauto.cz a protože byl řádně poučen svým synem, využíval k lepšímu vyhledávání možnost filtrování. Díky tomu nalezl nabídku prodeje automobilu, jehož cena byla podstatně nižší než cena ostatních automobilů stejného typu a značky uveřejněných na tomto portále. Cena byla natolik výhodná, že se Pavel rozhodl obchodníkovi ihned odepsat a zjistit, jak je možné, že je cena tak nízká. Odpověď obdržel během pár hodin, prodejce mu napsal emailovou zprávu, ve které nesrozumitelnou češtinou (text byl vložen do překladače a po té odeslán) uvedl, že je momentálně v Anglii, zde má i nabízené vozidlo. Vozidlo si zakoupil, když byl pracovně několik let v České republice. Když se vracel zpět do své rodné země, vzal si vozidlo sebou, zde ale narazil na problém, že volant je umístěn na opačné straně, neboť v Anglii jezdí auta vlevo.

Již zde pozbývá historka logiku, muž z Anglie vynaloží peníze na transport svého vozidla zpět do Anglie a neuvědomí si, že v Anglii se jezdí vlevo a proto volant umístěný na opačné straně by mohl být problém. Rozhodne se tedy, že auto prodá, ale chce ho prodat zpět do České republiky, a to samozřejmě zcela pod cenou, navíc vynaloží další finanční náklady na transport jen proto, aby vozidlo prodal v České republice. Nechám ale nelogičnost historky být a postoupím dál. Pavel prodejci odepíše, že by měl o auto zájem. Ale že by chtěl, alespoň jeho telefonní číslo, aby se mohli domluvit na prodeji. Toto byl jediný pokus Pavla o ověření si věrohodnosti prodejce. Den na to obdržel email s telefonním číslem. Počkal, až se vrátí jeho syn, který na rozdíl od Pavla hovořil anglicky a ten prodejci zavolal a společně se domluvili na podmínkách prodeje. Domluva nebyla jazykově náročná, prodejce při používání angličtiny

používal pouze pár známých frází a slov, mluvil pomalu a výslovnost měl podobnou jako Pavlův syn, tedy jako někdo, kdo angličtinu zase tak často nepoužívá. Telefonní číslo bylo platné, tedy již nic nestálo v cestě tomu obchod uskutečnit. Pavel tedy poslal zálohu na účet transportní firmy, na kterou mu prodejce zaslal odkaz. Záloha činila 50% z ceny, tedy v našem případě 55.000,- Kč. Vzápětí Pavel obdržel emailovou zprávu, ve které mu samozřejmě fiktivní dopravní firma potvrdila přijetí vozidla a jeho transport do České republiky. Při druhé emailové zprávě se dozvěděl, že auto je již v Německu a aby mohlo být předáno, je třeba uhradit zbylou část ceny, tedy dalších 55.000,- Kč. Transport byl rychlý a tak ani Pavel celou transakci nezdržoval a zbylých 55.0000,- Kč obratem zaslal na účet přepravní firmy. Podvodníci již dostali částku, kterou požadovali a mohli se odmlčet, ale když už se najde šikovná oběť, tak proč nezkusit štěstí dále. A tak Pavel obdržel třetí emailovou zprávu, týkala se uhrazení celního poplatku ve výši 10.000,- Kč jako nečekaný výdaj. S tímto už Pavel nepočítal, ale protože mu přepravní firma sdělila, že bez uhrazení by zůstalo auto v Německu, rozhodl se tuto částku zaplatit. Celkem tedy 120.000,- Kč odeslaných na účet podvodníků. Automobil samozřejmě Pavel neobdržel. Přepravní firma se odmlčela a telefonní číslo na prodejce již bylo nedostupné. Mimochodem k celkové částce 120.000,- Kč by si měl Pavel ještě přičíst cca. 500,- Kč za prvotní telefonát s prodejcem, neboť telefonní číslo bylo zahraniční. I Pavlovi již začalo docházet, že něco není v pořádku a se synem tak zadali název přepravní společnosti do vyhledávače google a nestačili se divit. Vzápětí bylo nalezeno několik stránek upozorňujících na podvod. Pavel vše nahlásil na policii, službě kriminální policie a vyšetřování, hospodářskému odboru z okraje České republiky. Vyšetřovatel neměl příliš velké zkušenosti s takovým to druhem podvodu, dokonce ani netušil, že by mohl využít zkušenosti policistů zabývající se kriminalitou páchanou přes internet a tak případ brzy odložil z důvodu neznámého pachatele. Na jeho obranu nutno říci, že šance dopadení pachatele by i tak byla velice nízká, přesto jak je vidět, ani všichni policisté nejsou řádně proškoleni v tom jak určité případy řešit a tím dostávají pachatelé další náskok. Pavel své peníze zpět nezískal a ani nezíská.

Pavel ve svém nakupování udělal spoustu chyb, ve zkratce nastíním, jak měl postupovat. Za prvé podezřele levný automobil již od pohledu nasvědčuje možnému podvodu a kupující by tak měl zpozornět. Druhá výstražná kontrolka by měla začít blikat v hlavě kupujícího v momentě, kdy prodejce je cizinec, který je mimo Českou republiku, ale inzeruje na českých stránkách a chce své zboží prodat zde. Vždy stojí za zamyšlení, proč by prodejce takhle uvažoval, co by tím získal. Pavel správně dospěl k názoru, že by si měl prodejce přeci jenom

prověřit, ale již zvolil nesprávný způsob. Komunikace telefonem stále ještě nepotvrzuje, že prodejce není podvodník, zvláště když rodilý Angličan nehovoří plynule anglicky. Na Pavlovo místě bych prodejce požádala o zaslání dalších fotek vozidla, tentokrát ale fotografií, abych si ověřila, že prodejce vozidlo skutečně má u sebe. Tedy požádala bych ho, ať automobil vyfotí a umístí na něj například cedulku s nápisem mého jména, samozřejmě dostatečně velkou a čitelnou. Fotografie, které byly v inzerátu, bych nejdříve použila ve vyhledávači google, jestli nejsou umístěny na internetu ještě někde jinde. V tomto případě by totiž Pavel zjistil, že fotografie byly použity z jednoho autobazaru v České republice, kde si je podvodníci pouze stáhli z jejich internetových stránek. Vyhledání si názvu transportní firmy, případně čísla účtu již nemusím uvádět. Jde o pár rychlých kroků, které nezaberou ani deset minut a Pavel mohl ušetřit 120.000,- Kč, ale neudělal to.

Proč jsem se rozhodla analyzovat zrovna tento případ? Chtěla jsem poukázat, že znalost bezpečného pohybu na internetu a ochránění svých peněz, nemá co dočinění ani s vysokoškolským vzděláním. Pavlovi po celou dobu obchodu asistoval jeho syn, který by vzhledem ke svému vzdělání a pracovní praxi měl mít v této oblasti dostatečné znalosti.

4.3 Analýza současného stavu vzdělávání uživatelů v bezpečném užívání internetu

V rámci mé diplomové práce jsem se rozhodla analyzovat současný stav vzdělávání uživatelů v bezpečném chování na internetu. Pro tuto analýzu jsem si zvolila tři oblasti, kde se domnívám, že k tomuto vzdělávání mělo docházet. Těmito oblastmi jsou školské instituce – základní a střední školy, internet a televize.

Získat základní informace ohledně bezpečného pohybu na internetu by měli lidé získávat už ve škole. V dnešní době se k internetu připojují už i předškolní děti, z tohoto důvodu by měla tato osvěta probíhat již na základní škole. V nižších ročnících základní školy, by se děti měly seznamovat především s bezpečným užíváním sociálních sítí a být více obezřetné při seznamování se s cizími lidmi na internetu. Děti z vyšších ročníků už ovšem mají částečný přístup k penězům od svých rodičů a právě zde by již měly být obeznámeny s tím, jak si své peníze ochránit. V roce 2013 jsem se při výkonu své profese setkala s případem 13ti letého chlapce jehož počítač byl napaden ransomwarem a on ve strachu, aby rodiče nezjistili, na jakých stránkách se pohyboval, byl ochoten ze svého našetřeného kapesného zaplatit podvodnou pokutu ve výši 2.000,- Kč. Jedinou záchranou, že tehdy peníze neuhradil, byla

jeho neznalost platebního způsobu pomocí „Ukash“ karty. Tedy je zřejmé, že už v tomto věku by měly děti získávat informace o tom, jak podvodníkům na internetu nenaletět.

V souvislosti se získáním informací ohledně vzdělávání v dané problematice jsem oslovila tři žáky vyšších ročníků ze tří základních škol. Jednalo se o tyto instituce: Základní škola Březenecká v Chomutově, Základní škola Zahradní v Chomutově, Základní škola Mládežnická Litvínov a dále studenty ze tří středních škol Gymnázium Chomutov, Gymnázium T. G. M. v Litvínově a Gymnázium v Mostě. Jsme si vědoma toho, že tento průzkum pouze šesti institucí není dostatečně průkazný, ale mým cílem bylo pouhé nastínění situace za pomoci tohoto náhodného vzorku. Dva ze tří oslovených žáků základních škol uvedli, že byli ve škole poučeni o tom, že na internetu nemají posílat cizím lidem své fotografie, nemají o sobě prozrazovat důvěrné informace a sjednávat si schůzku s lidmi, které neznají osobně. Studenti ze středních škol uvedli, že byli ve škole seznámeni se základním fungováním internetu, se základy tvoření HTML stránek, nikoliv však již v souvislosti s tím, jak na internetu bezpečně nakoupit či nepodlehnout jinému druhu. Z dotazovaného vzorku tak vyplynulo, že ve školní instituci uživatel internetu potřebné znalosti k tomu, aby nepodlehl případnému podvodu, nezíská.

Na internetu je naopak informací o možných způsobech podvodů dostatek. Ať již zpravodajské stránky, které se věnují různým konkrétním případům společně s běžným zpravodajstvím, takovými to stránkami jsou například idnes.cz, aktualne.cz a jiné, nebo stránky přímo specializované na internetovou technologii a možné podvody na internetu jako jsou například stránky hoax.cz, lupa.cz, ale také třeba stránky policie.cz. Problémem těchto stránek je, že široká veřejnost je nenavštěvuje a tak paradoxně jsou tyto stránky navštěvovány pouze lidmi, kteří již znalosti o tom, jak podvodníkům na internetu nepodlehnout mají. Já sama jsem za tímto účelem zkusila vytvořit v měsíci listopadu 2013 internetové stránky pod názvem strazcenetu.cz s cílem zjistit, zda by lidé tyto internetové stránky navštívili a získávali tak z nich základní znalost o bezpečnosti na internetu. V měsíci listopadu 2013 jsem pouze nechala tyto stránky fungovat bez jakéhokoliv upozornění na jejich existenci. V měsíci prosinci 2013 jsem již umístila odkaz na tyto stránky v různých diskuzích mezi podvedenými na sociálním portále facebook. V měsíci lednu jsem ještě podpořila povědomí o těchto stránkách mezi respondenty, které jsem oslovila při vyplňování dotazníku určeného pro tuto diplomovou práci. Samozřejmě o existenci těchto stránek byli vyrozuměni až po vyplnění dotazníku, aby jejich znalosti nebyly nijak ovlivněny. Tímto pokusem bylo zjištěno, že zcela logicky tyto internetové stránky v měsíci listopadu neměly návštěvnost žádnou. V měsíci

prosinci tyto internetové stránky navštívilo 5 uživatelů. V měsíci lednu 2014 po té uživatelů 8. Pokus o vytvoření vzdělávacích internetových stránek tak z mé strany nevyšel a proto jsem tento pokus nakonec do své diplomové práce nezařadila a vyhodnotila ho jako nepovedený.

Ne všechny instituce ovšem opomíjejí vzdělávání uživatelů internetu, jedním z dobrých příkladů je zájmové sdružení právnických osob CZ NIC. Toto sdružení bylo založeno předními poskytovateli internetových služeb v roce 1998 a nyní má 112 členů. Jejich hlavní činností je provozování registrů doménových jmen „.cz“ a zabezpečování provozu domény nejvyšší úrovně „.cz“ a dále také osvěta v oblasti doménových jmen. V současné době je sdružení známé především s šířením služby mojeID. Sdružení taktéž provozuje interní bezpečnostní tým CZ NIC-CSIRT a od roku 2011 Národní CSIRT tým České republiky. Právě sdružení CZ NIC stojí za pro společnost nejznámější edukací v oblasti internetu, protože v souvislosti se vzděláváním společnosti se spojila s Českou televizí. Od 1 října roku 2012 tak Česká televize začala vysílat seriál osvětových videí nazvaných „Jak na internet“.[33] Tyto zhruba dvouminutové spoty jsou vysílány do dnešní doby a jedná se zatím o 85 dílů, které jsou kromě právě již zmiňované České televize dostupné i na internetových stránkách www.jaknainternet.cz.

Ondřej Filip výkonný ředitel CZ NIC k tomuto projektu uvedl: *„Internet je součástí každodenního života stále větší části české společnosti, ale obecná znalost o jeho fungování, možnostech využití či bezpečnostních rizicích se ukazuje spíše jako povrchní a mlhavá. Posláním našeho sdružení je kromě technického zajišťování chodu domény .CZ také osvěta v oblasti domén a Internetu jako takového. Proto jsme se rozhodli natočit seriál, který by co největšímu počtu diváků svět Internetu srozumitelně přiblížil a upozornil je na to, co od něj mohou čekat dobrého a na co si naopak dát pozor. Projekt Jak na Internet vhodně doplňuje naše stávající vzdělávací aktivity jako vydávání knih, pořádání konferencí nebo provozování našeho výukového centra Akademie CZ.NIC.“*[34]

Sdružení CZ NIC se opravdu snaží této osvětě věnovat. V současné době také provozuje dvouhodinové kurzy za symbolickou cenu 99,- Kč. Internetová komunikace s úřady, Internet a právo nebo hledání práce na Internetu a dalším tématům se nyní věnuje pražská pobočka Akademie CZ.NIC. Vzdělávací centrum provozované správcem české národní domény v současné době poskytuje 12 kurzů určených uživatelům s minimálními zkušenostmi,

[33] http://www.nic.cz/page/351/
[34] http://www.nic.cz/page/1177/televizni-spoty-podpori-znalosti-o-internetu/

například seniorům. Igor Kytka, koordinátor těchto vzdělávacích aktivit sdružení CZ.NIC k tomuto uvedl: *„Jedná se de facto o pilotní projekt, na jehož základě vzniknou balíčky vzdělávacích materiálů. Ty pak nabídneme dalším organizacím, které se zaměřují na vzdělávání laické veřejnosti v oblasti Internetu. V tomto pololetí bychom proto rádi od návštěvníků setkání získali zpětnou vazbu. Jejich poznatky následně využijeme pro finalizaci edukačních materiálů,“*

Tento pokus o edukaci společnosti ovšem stojí finance. Sdružení CZ.NIC tak například v poslední době oslovilo bankovní instituce, s cílem získat finanční podporu pro vzdělání klientů těchto bankovních institucí. Při rozhovoru s vedoucím pracovníkem majícím na starosti technologickou bezpečnost v jedné známé bankovní instituci, který si nepřál být jmenován, mi k tomuto následně uvedl, že bankovní instituce financování takových to aktivit nepodporují. Právě on musí vynaložit velké úsilí, aby každý rok přesvědčil vedení k financování technologického zabezpečení, a vždy musí prokázat, že vynaložení těchto peněz bude pro společnost výhodné a investice v tomto směru bude návratná. Vzhledem k jeho kontaktům na pracovníky v oblasti bezpečnosti v jiných bankovních institucích, uvedl, že se domnívá, že žádná z těchto institucí na projekty tohoto typu nepřispěje. Touto informací jsem jen chtěla poukázat na skutečnost, že instituce všeobecně raději vynaloží peníze na lepší a lepší technické zabezpečení než-li na samotné vzdělání uživatelů.

5 Závěr

Pro svou diplomovou práci jsem si zvolila trestný čin podvod páchaný prostřednictvím internetu. Svou diplomovou práci jsem nazvala Internet, rychlá a snadná cesta do Vaší peněženky. Tento název jsem zvolila, abych poukázala na to, že díky rozvoji internetu a službami, které poskytuje a které jsou využívány čím dál tím více uživateli, se cesta k penězům jiných pro podvodníky stává snazší.

Cílem mé diplomové práce bylo v teoretické části analýzou odborné literatury a získaných zkušeností při výkonu mé profese popsat podvody páchané prostřednictvím internetu. Poukázat na to, že internet a jeho možnosti se v průběhu let vyvíjí a lidé nejsou schopni s tímto vývojem držet krok. Popsáním jednotlivých způsobů podvodů páchaných přes internet jsem poukázala na to, že aby podvodníci byli úspěšní, stačí jim k tomu spíše sociální schopnosti než technické vědomosti. Ve své práci jsem ukázala, že ačkoliv počet spáchaných trestných činů podvodů v průběhu let klesá, počet podvodů páchaných přes internet naopak stoupá. Tento trend poukazuje na to, že podvodníci stále častěji využívají výhod internetu jako je anonymita a rychlé „zametání“ stop. Dalším cílem bylo, ukázat, že ačkoliv společnosti neustále vyvíjejí lepší technické zabezpečení, jakými jsou antivirové programy, firewally, kódování a jiné, nejslabším článkem je vždycky lidský faktor. Toto je způsobeno nedostatečnou informovaností lidí, která vede k nezodpovědnému chování na internetu. Uživatelé internetu tak dobrovolně odevzdávají své peníze podvodníkům.

Lidé si už zvykli instalovat do svých počítačů antivirové programy a volit jiná zabezpečení ale i přes ta nejlepší technická zabezpečení nakonec stejně přijdou o své peníze nedostatkem dostatečné informovanosti jak se v určitých situacích chovat. Tuto skutečnost bych přirovnala k situaci, kdy koupíte svým blízkým ty nejbezpečnější dveře na trhu s několika zámky, když na ně ale zaklepe podvodník, oni mu v dobré víře otevřou a pozvou ho dál. V této situaci je nejbezpečnější umístit zevnitř na tyto dveře návod, jak se chovat, stojí-li za dveřmi jim neznámá osoba. A právě tuto pomyslnou samolepku by měli mít před očima všichni lidé, kteří se chystají přes internet provádět nákupy či z jiného důvodu transferovat přes internet své peníze. Vybrané spolehlivé obchody sice mají na svých stránkách značku, která nasvědčuje tomu, že byli prověřeni například Asociací pro elektronickou komerci (APEK), ale to samo o sobě nedostatečně informovaným uživatelům nic neřekne. Navrhovala bych, aby elektronické obchody měly na svých stránkách viditelný návod, jak si ověřit, že tento obchod není podvodný. Inzertní portály se sice snaží vyhledávat podezřelé inzeráty a tyto odstraňují,

přesto jejich snaha není dostatečná a počet podvedených neustále stoupá. Tyto portály by měli taktéž na svých stránkách mít na viditelném místě umístěny postup, jak si ověřit pravost inzerátu. Umístění těchto „samolepek“ na co nejvíce míst by dle mého názoru snížilo počet podvodů spáchaných přes internet mnohem více než zvyšování technického zabezpečení.

V praktické části jsem si stanovila dvě hypotézy týkajících se nakupování zboží přes internet. První hypotéza byla, že neexistuje rozdíl mezi muži a ženami ve znalostech bezpečného chování při nakupování zboží přes internet. Druhou hypotézou bylo, že neexistuje rozdíl ve znalostech bezpečného chování při nakupování zboží přes internet. Tyto dvě hypotézy jsem si ověřila prostřednictvím dotazníku, který jsem předložila 84 respondentům. Výsledkem bylo potvrzení první hypotézy a zamítnutí hypotézy druhé. Znalosti mužů a žen v této oblasti nejsou rozdílné, ale znalosti věkových skupin již ano. Tento fakt je dle mého názoru způsoben rychlým vývojem internetu, jednotlivé věkové generace tak nestíhají na tento trend dostatečně reagovat.

Mým dalším cílem bylo analyzovat současnou situaci edukace uživatelů internetu v jeho bezpečném užívání. Při této analýze jsem zejména vyzdvihla aktivity sdružení právnických osob CZ.NIC, které ze zjištěných informací jako jediní volí dle mého názoru správnou cestu, jak uživatele internetu vzdělat v bezpečnosti jeho užívání.

Ve své diplomové práci jsem si stanovila cíle, které jsem naplnila. Jak v teoretické, tak v části praktické a mnou navrhovaný způsob řešení považuji jen jako tzv. „prototyp“ k zamyšlení a postupem času k jeho zdokonalení.

6 Seznam použitých zdrojů:

6.1 Seznam použité literatury

- SMEJKAL V., SOKOL T., VLČEK M., Počítačové právo, vyd. Praha: Beck, 1995, ISBN: 80-7179-009-5
- JIROVSKÝ V., Kybernetická krimalita, vyd. Praha: Grada Publishing, 2007, ISBN: 978-80-247-1561-2
- POŽÁR J., Základy teorie informační bezpečnosti, vyd. Praha: Policejní akademie ČR, 2007, ISBN: 978-80-7251-250-8
- McCARTHY L., WELDON-SIVIY D., Buď pánem svého prostoru, vyd. Praha: CZ.NIC, 2006, ISBN: 978-80-904248-6-9
- Council of Europe, Convention on Cybercrime, Budapest, 2001
- Council of Europe, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts a racist and xenophobic nature commited through komputer systems, Strasbourg, 2003
- POLČÁK R., Právo na internetu, vyd. Brno: Computer Press, a.s., 2007, ISBN: 978-80-251-1777-4
- POLČÁK R., Internet a proměny práva, vyd. Praha: Auditorium, 2012, ISBN: 978-80-87284-22-3
- LANCE J., Phishing bez záhad, vyd. Praha: Grada Publishing, a.s., 2007, ISBN: 978-80-247-1766
- ZEMÁNEK J., Stavba a správa sítě, aneb cesta do hlubin internetu, vyd.: Kralice na Hané: Computer Media s.r.o., 2004, ISBN 80-86686-26-4
- VÝBORNÝ Š., Nenávistný internet versus právo, vyd. Praha: Wolters Kluwer ČR, 2013, ISBN: 978-80-7357-766-7
- GLENNY M., Temný trh, vyd. Praha: Argo, 2013, ISBN: 978-80-257-0824-8

6.2 Seznam internetových stránek

- http://mercury.lcs.mit.edu/
- cs.wikipedia.org
- www.packet.cc
- www.homes.eff.org/
- security.fnal.gov
- http://www.f-secure.com
- www.root.cz/
- http://nakedsecurity.sophos.com/
- http://mediacenter.avg.com/en/press-tools/
- www.lupa.cz
- www.apek.cz
- www.heureka.cz
- http://www.sauto.cz/auto-moto-clanky/
- www.policie.cz
- http://www.fightidentitytheft.com
- www.inhope.org

6.3 Seznam obrázků

6.4 Seznam tabulek

6.5 Seznam grafů

6.6 Seznam příloh

Dotazník

(Prosím o vyplnění tohoto dotazníku, který vznikl za účelem zjištění aktuálního stavu vzdělanosti respondentů v bezpečném používání internetu, zejména při nakupování prostřednictvím internetu. Získaná data budou použita v mé diplomové práci. Děkuji. Kundrtová)

(Správnou variantu zakroužkujte)

MUŽ - ŽENA **Věk: _____** **Nejvyšší dosažené vzdělání (získaný titul):_____**

Otázka č. 1

Byl/a jste někdy prostřednictvím internetu podveden/a? Pokud ano, jaká celková škoda Vám tím byla způsobena?

(Správnou variantu zakroužkujte)

Ano – Ne **Výše způsobené škody: _____**

Otázka č. 2

Provedl jste někdy nákup zboží či služeb prostřednictvím internetu? A jak často?

(Správnou variantu zakroužkujte)

Ano – Ne **Častost:** **1x – 3x do roka**
4x – 12x do roka
Více jak 12x za rok

Otázka č. 3

Jakým způsobem na internetu nakupujete? Elektronický obchod (eshop), inzeráty, dražební portály (vyberte všechny možnosti, které používáte)

(Správnou variantu zakroužkujte)

- **ESHOP**
- **Inzeráty**
- **Dražební portály**

Otázka č. 4

Jaký preferujete druh platby při nakupování přes internet?

(Správnou variantu zakroužkujte)

- **Dobírka**
- **Platba převodem na účet**
- **Platba platební kartou**

Otázka č. 5

Představte si, že jste na internetu objevil Vám do této doby neznámý elektronický obchod s výhodnou cenou Vámi požadovaného výrobku a máte zájem si ho zakoupit. Ověřil byste si tento obchod před tím, než byste zde nakoupil?

(Správnou variantu zakroužkujte)

ANO – NE

Otázka č. 6

Pokud by v obchodě, kde nakupujete poprvé, byla v případě platby předem poskytnuta 20% sleva na zakoupené výrobky na rozdíl od plné ceny v případě zaslání na dobírku, zvolil byste tuto možnost platby (tedy platbu předem)?

(Správnou variantu zakroužkujte)

ANO – NE

Otázka č. 7

Pokud nakupujte zboží prostřednictvím elektronického obchodu, pročítáte si jeho obchodní podmínky?

(Správnou variantu zakroužkujte)

ANO – NE

Otázka č. 8

Znáte certifikáty důvěryhodnosti elektronických obchodů, které jsou u některých elektronických obchodů uvedeny (např. APEK, HEUREKA)?

(Správnou variantu zakroužkujte)

ANO – NE

Za vyplnění dotazníku Vám děkuji.