Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Naše digitální stopa na počítači a na internetu

Jan Mládek

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jan Mládek

Informatika

Název práce

Naše digitální stopa na počítači a na Internetu

Název anglicky

Digital footprint on own computer and the Internet

Cíle práce

Hlavním cílem práce je charakterizovat jednotlivé typy digitálních stop a představit nejvýznamnější metody ochrany osobních dat. Dílčím cílem bakalářské práce je srovnání schopností a možností nástrojů k ochraně osobních dat na základě analýzy prostředí, infrastruktury, požadavků a možností navrhnout a implementovat vhodné řešení individuální ochrany dat.

Metodika

Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů, ale také na praktických zkušenostech s jednotlivými produkty. Pomocí této metodiky je navrhnuto a implementováno vhodné řešení ochrany digitální stopy. Na základě syntézy teoretických poznatků a přínosů vlastního řešení budou formulovány závěry bakalářské práce.

Doporučený rozsah práce

30-40 stran

Klíčová slova

digitální stopa, ochrana dat, hesla, cookies

Doporučené zdroje informací

ECKERTOVÁ, L., DOČEKAL, D. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. 1. vyd. Brno: Computer Press. 2013. 224 str. ISBN 978-80- 251-3804-5.

HOOG, A. Android Forensics. Waltham: Syngress Publishing. 2011. 432 str. ISBN 9781597496513.

LANGE, M. C. S., NIMSGER, K. M. Electronic evidence and discovery: What every lawyer should know now. Washington: American Bar Association. 2009. 429 pages. ISBN 9781604423822.

LARRY D., LARS D. Digital Forensics for Legal Professionals. 1ˆst edition. Waltham: Syngress Publishing. 2011. 368 pages. ISBN 9781597496438.

MATOUŠKOVÁ, M., HEJLÍK, L. Osobní údaje a jejich ochrana. 2. vydání. Praha: ASPI, Wolters Kluwer. 2008. 468 str. ISBN 978-80-7357-322-5.

PORADA, V. , RAK, R. Teorie digitálních stop a její aplikace v kriminalistice a forenzních vědách. Karlovarská právní revue 4/2006. ISSN 1801-2191.

Předběžný termín obhajoby

2016/17 LS – PEF

Vedoucí práce

Ing. Čestmír Halbich, CSc.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 21. 10. 2016

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 24. 10. 2016

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 05. 03. 2017

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Naše digitální stopa v počítači a na internetu" jsem vypracoval(a) samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor(ka) uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15. 3. 2017 _____

Poděkování

Rád(a) bych touto cestou poděkoval(a) Ing. Čestmíru Halbichovi, CSc. za jeho užitečné rady, trpělivost a vstřícnost při vedení mé práce.

Naše digitální stopa v počítači a na internetu

Souhrn

Tato práce je zaměřena na popis a přestavení množství digitálních stop a následné představení možných obranných prostředků.

V první části jsou představeny digitální stopy. Především jejich různé varianty a způsoby, jak nás ovlivňují v různých oblastech života jako například v práci nebo v běžném životě. Také jsou představeny nejhorší možná rizika spojená s odcizením osobních dat následovaná prostředky sloužícími pro ochranu digitální stopy zajištěním anonymity. Na závěr této kapitoly jsou představeni hackeři a jejich metody sloužící pro odcizení dat.

V praktické části jsou představeny některé antivirové programy, které poskytují ochranu před útoky hackerů na náš počítač, přičemž je brán ohled na schopnosti a efektivitu antivirů v odrážení hackerských útoků.

Klíčová slova: digitální stopa, ochrana dat, hesla, cookies, krádež identity, hackeři, phishing, počítačový virus, počítačový červ, antiviry,

Digital footprint on own computer and internet

Summary

This essay focused on description and introducing ways that digital footprints use, followed by introducing possible defences instruments.

In first part, will be introduced digital footprints. Especially their different variants and ways how it can affect our lives for example in work or in ordinary life. Also will be introduced possible risks associated with stealing private data followed by instruments serving for protection of digital footprint by providing anonymity. In the end of this chapter will be introduced hacking and methods serving for stealing data.

In practical part are introduced some antivirus programmes which provide protection from attacks from hackers. Antivirus programmes are judged by capability and efficiency of antiviruses in deflecting hacker attack.

Keywords: digital footprint, protection of data, passwords, cookies, identity theft, hackers, phishing, computer virus, computer worm, antiviruses,

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Za posledních několik let udělalo lidstvo v oblasti výpočetní techniky obrovské pokroky. Technika se stala kompatibilnější a z celé místnosti se stala malá krabice. Mluvím samozřejmě o osobním počítači. Více a více lidí si jej začalo pořizovat díky větší a větší dostupnosti. A jelikož pokrok je nezastavitelný začali se zařízení zmenšovat a vylepšovat. A přišli zařízení jako notebooky, netbooky, mobilní telefony a tablety.

Tím ale nekončíme. Jak už to, tak bývá, vojenská technologie se časem poskytne civilistům a nastává jeden z největších objevů 21. století – Internet.

Skoro každý má minimálně jedno zařízení, jež bylo zmíněno. Samozřejmě že se najdou i lidí, kteří mají i více těchto zařízení a jsou na nich stále připojení a projíždějí webové stránky, aniž by si uvědomovaly, co všechno o sobě mohou prozradit.

Internet připomíná džungli. Je tam sice krásně, ale cokoliv nás může ohrozit. Pro vlastní bezpečí se musíme naučit, jak se v této příslovečné „džungli“ orientovat, abychom nedošli k úhoně.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem práce je charakterizovat jednotlivé typy digitálních stop a představit nejvýznamnější metody ochrany osobních dat. Dílčím cílem bakalářské práce je srovnání schopností a možností nástrojů k ochraně osobních dat na základě analýzy prostředí, infrastruktury, požadavků a možností navrhnout a implementovat vhodné řešení individuální ochrany dat.

2.2 Metodika

Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů, ale také na praktických zkušenostech s jednotlivými produkty. Pomocí této metodiky je navrhnuto a implementováno vhodné řešení ochrany digitální stopy. Na základě syntézy teoretických poznatků a přínosů vlastního řešení budou formulovány závěry bakalářské práce.

3 Teoretická část

3.1 Digitální stopy

Digitální stopa je označení pro informace, které zůstávají v počítači po každém, kdo využívá digitální služby. Jakékoliv informace zanechané při pohybu po internetu můžeme zanechat vědomě či nevědomě.

Data zanechaná vědomě jsou nazývána Aktivní digitální stopou. Jsou to například příspěvky, fotky a profily, blogy, maily a sms. Všechny tyto informace o nás mohou vypovídat mnoho věcí. Sběr takovýchto dat většinou probíhá na sociálních sítích naší neopatrností. Situace, při které můžete takto přijít o data může vzniknout velice jednoduše. Pro lepší představu, jak snadno můžete poskytnout data si představte tuto situaci. Na sociální síti se chcete pochlubit novým bankovním účtem, a jelikož vám banka dala na kartu krásný obrázek vašeho auta vyfotíte zmíněnou kartu a poskytnete jí ke sdílení. Dále již jdou věci sami. Útočník uvidí fotografii, a tudíž ví číslo vašeho účtu, vaše jméno atd. Útočník má pak k dispozici mnoho nástrojů, kterými může z vašeho počítače ukrást hesla a tím se k vašemu účtu dostane a může vám z něj například odcizit peníze.

Data zanechávaná nevědomě jsou nazývána Pasivní digitální stopou. Jde o data, jež jsou sbírána bez vědomí uživatele. Mohou to být IP adresy, činnost na různých internetových stránkách nebo četnost návštěv webových stránek. Dále pak mezi tyto stopy patří i vyhledávání výrazů nebo lokace kde se právě nacházíte. Opět si to pro představu vysvětleme na následující situaci. Pasivní digitální stopu uživatelé zanechávají v podstatě jakýmkoliv pohybem po internetu. Surfujete po stránkách, které nemusí být úplně legální nebo je na nich nemorální obsah. Ať už jste na tyto stránky přišli schválně či jste jen omylem klikli na příslušný odkaz již je informace o vaší přítomnosti zaznamenána a ani o jejím vytvoření nemáte potuchy. Pokud někdo z vašeho okolí (ať schválně či náhodou) zjistí, že jste se pohybovali na nějakých neslušných stránkách v lepším případě budete „pouze“ svému okolí pro smích. V horším případě vám na dveře zaklepe Policie se zatykačem v ruce za přispívání nebo sdílení nelegálního či extremistického obsahu. [3]

Příklady, které byly zmíněny jsou možná trochu extrémní, ale opravdu se dějí. Vždyť internet sám je plný absurdních příběhů, které se opravdu staly. Dovolím si říci, že lidé dokáží sdílet mnohem citlivější data a neopatrně je poskytnou téměř komukoliv.

3.2 Vznik a důležitost digitálních stop

Digitální stopy přitom nevznikají nijak složitě. Vznikají běžnou uživatelskou aktivitou jako je brouzdání po internetu. Ať už si čtete nějaký článek o globálním oteplování, prohlížíte obrázky na Googlu nebo jste na sociálních sítích. Uživatelé si ani neuvědomují, jak snadno zanechávají stopy, které by mohli někoho zajímat. [2]

Bohužel díky sociálním sítím je vznik a ukládání digitální stop v dnešní době velice problematický. Veškerý obsah, který jste prohlíželi nebo fotografie, které jste přidali nemusí být pouze na jednom místě. Je tomu tak proto, že každá služba, jež využíváme je někým poskytnutá a tento poskytovatel nemusí mít vámi uložené obrázky na jednom místě, ale i na více úložištích (serverech). Tato metoda se nazývá cloud computing. Tato metoda byla myšlena jako bezpečnostní pojistka proti ztrátě dat. Vždy se totiž může stát, že server selže a veškerá data na něm mohou být zničena. Pokud by se toto stalo poskytovatel, který vám data uschovával by měl nejspíš veliké problémy obzvláště pokud by data, jež jste ztratily na jeho serveru, pro vás byla životně důležitá. Proto pokud uložíte jakýkoliv dokument či obrázek na internet pravděpodobně bude tento dokument již existovat napořád. [1]

Dále se digitální stopy rozlišují podle důležitosti. Priority informací se u každého jedince mohou různit, ale přesto různá citlivá data jsou roztříděna podle obecné důležitosti.

Nejdůležitější data jsou označena jako kategorie Červená. Tato data jsou považována za nejdůležitější data pro každého jedince. Jedná se o data, která souvisí s identifikací občanů jako například rodné číslo, čísla účtů, informace o zdravotním stavu. Jsou to údaje, které mohou být použity k tzv. Krádeži identity (o tomto klíčovém slovu viz. níže).

Kategorie žlutá je označení pro data, která jsou stále citlivá, ale jejich ztráta již není tak bolestná. Mezi tyto data se řadí například adresa vašeho bydliště, vaše vzdělání nebo minulá zaměstnání a datum narození. Dále pak osobní kontakty jako telefonní číslo, emailová adresa a na konec internetové stránky, které jsme v minulosti navštívily.

Poslední kategorie je označena zelenou barvou. Tato kategorie zahrnuje marginální data, která vaši osobnost nijak neohrožují, pokud nejsou tyto informace spojena s některou s předchozích skupin. Mezi tyto informace patří věk nebo výše výplaty.

3.3 Digitální stopa v běžném životě

Digitální stopa nás v běžném životě ovlivňuje více než tušíme. Tedy ne až tak nás jako spíš naši budoucnost. V dnešní době, pokud o někom chcete něco zjistit první věc co uděláte je, že se podíváte, jestli náhodou nemá profil na sociálních sítích a pokud jeho profil najdete, zjišťujete, co všechno sdílel nebo co bylo přidáno přáteli dotyčného.

Stejně tak to dělají i personalisté ve firmách. Pokud ve firmě probíhá výběrové řízení na nějakou důležitou pozici, určitě nechcete zaměstnat nekompetentní či nezodpovědnou osobu. Proto personalisté kromě životopisu kontrolují i vaše digitální stopy. Zjišťují, jaké názory zastáváte, kde jste byl a co jste dělal v minulosti nebo podle příspěvků, které jste sdíleli, zjišťují, jak jste na tom s gramatikou.

Útěchou však je, že sociální sítě však neslouží jako úplný pohled na charakter člověka. Nesmíme totiž zapomenout, že čím úspěšnější člověk je tím více lidí je co mu závidí a snaží se ho pošpinit pomluvami a sociální sítě jsou skvělým prostředkem jak roznést pomluvu s minimální námahou maximálnímu počtu lidí.

Taktéž v osobním životě vám může vaše digitální stopa uškodit. Například vašemu současnému partnerovy se úplně nemusí líbit fotky, které máte na svém profilu se svým bývalým partnerem. [1]

3.4 Digitální stopa v marketingu

Naše digitální stopy jsou též sledovány firmami zabývajícími se obchodem. Jejich účel je jasný docílit co nejvyšších tržeb. Hlavní aspektem je analyzování uživatelů. Analýza je tvořena tím kde se daný uživatel v poslední době nacházel, co vyhledával nebo jaká klíčová slova zadával do vyhledávače. Na základě těchto dat poté internetové obchody určují a zda je jejich internetová stránka dosti přehledná nebo zda by úpravou stránky nezvýšili pobyt uživatelů na stránce a tím by potenciálně mohli zvednou i své tržby.

Dalším aspektem internetového marketingu je cílená reklama. Jak jsem již zmínil výše náš pohyb je sledován a následně analyzován. Určitě sami znáte tu situaci, když se vám rozbily hodinky a vy úporně hledáte nové. Při druhém dni hledání najednou vidíte hodinky všude kam se podíváte. Dle našich návštěv a hesel zadávaných na síti je totiž tvořen seznam našich zájmů a podle tohoto seznamu jsou nám podsouvány reklamy na výrobky, které jsme v nedávné době hledali. [4]

3.5 Rizika zneužití digitálních stop

Jak jsem již dříve zmiňoval, existují dva typy digitálních stop. Aktivní a Pasivní. Pro lepší představu jsem vybral jednoho zástupce za každý typ digitální stopy, pomocí kterého lze nejsnáze představit nebezpečí spojené se ztrátou dat.

3.5.1 Krádež identity

Ukázkovým zástupcem Aktivní digitální stopy je Krádež identity. S krádeží identity se setkáváme od nepaměti. Lidí se již od pradávna vydávali za někoho jiného, aby trest za případné zločiny, které hodlají způsobit přešel na osobu, za kterou se vydávají. V současné době se změnila její podoba. Veškeré fyzické aspekty vydávání se za někoho jiného pomalu vymizeli a nahrazují je aspekty digitální. Je to jeden z nejhorších způsobů, jak vás někdo může poškodit. Pokud o vás útočník nasbírá dostatečné množství dat, může se za vás začít vydávat. Čím více dat o vás bude útočník mít tím autentičtěji bude působit jako vy. [2]

Důvodů, proč jsou identity kradeny je spousta, a ne vždycky je identita kradena za účelem přímo poškodit originálního majitele identity. Prvním důvodem je samozřejmě finanční obohacení. Útočník chce vaši identitu, aby si na vás mohl půjčit peníze, ukrást peníze z vašeho účtu nebo využít služeb, které jsou přístupny pouze s vaším jménem. Dalším možným způsobem, proč krást identitu je použít ji pro kriminální činnost a tím převést vinu na někoho jiného. Jinou variantou může být ukrást data za účelem ukrýt svou pravou identitu. Jde o tzv. klonování identity a používá se například pro ukrytí ilegálních uprchlíků nebo dokonce k teroristickým činům. Méně závažné důvody krádeže identity může být ukrýt se před věřiteli či ukrýt se před jinými osobami, které nás eventuálně ohrožují. V tomto případě je samozřejmě lepší zvážit obrátit se na policii, protože v opačném případě ona osoba sama riskuje trestní stíhání za krádež identity. [5]

Proces krádeže identity má dvě fáze. První fází je získání identity. Jde o krádež jména, příjmení, hesel, přístupových údajů a rodného čísla. Útočník má spoustu možností a metod, jak se k těmto údajům dostat, ať už je uživatel nešťastně zanechá na sociální síti nebo je útočník dostane přímo z jeho počítače. Ale o těchto metodách se budu více zmiňovat v další kapitole. V druhé fázi pak pachatel využívá ukradenou identitu. [6]

3.5.2 Cookies

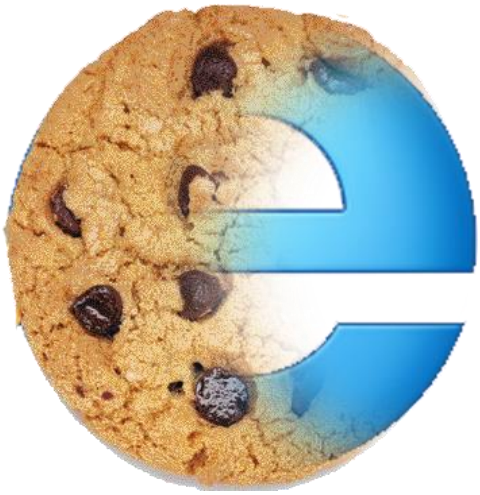
Příkladem Pasivní digitální stopy jsou Cookies. „Jsou to textové soubory, vytvářené webovým serverem a jsou uložené v počítači prostřednictvím prohlížeče.“ [7] Slouží k identifikaci uživatele za účelem zjednodušení pohybu po daném serveru. Název cookies vymyslel v roce 1994 programátor prohlížeče Netspace Lou Montulli. Cookie znamená v angličtině sušenka, a její název má symbolizovat její původní funkci. A to „nabídnout návštěvníkům sušenku“, čili soubor s daty o uživateli, aby byl uživatel rychleji a lépe identifikován.

Cookies se v zásadě dělí na dva typy. Session cookie (přechodná) a Persistent cookie (permanentní). Session cookies je pouze dočasná a maže se při odchodu z webového prohlížeče. Tento typ cookies nesbírá přímo informace o vaší identitě, ale spíše o tom, jak probíhal pohyb po stránce. Persistent cookie sbíra informace o vás a je

ukládána ve vašem počítači. Zanikne buď tím, že ji smaže uživatel nebo ji vyprší čas života. Slouží pro majitele webu, aby mohl stránku lépe přizpůsobit potřebám svých návštěvníků.

Cookies normálně nenarušují bezpečnost počítače, ale v současné době vzrůstá nový trend malicious (zlomyslné) cookies. Jejich cílem je shromáždit co nejvíce osobních údajů o vás a namapovat vaši historii sledování. Jakmile nasbírá dostatečné množství vašich osobních dat, je dost velká, že budou vaše data prodána reklamním společnostem, která tyto informace použijí proti vám posíláním cílených reklam a nabídek do vašeho počítače.

Nakonec je tu ještě jedno rozdělení cookies, a to na First-party a Third-party cookies. First-party cookies jsou cookies z internetové stránky, na které momentálně jste a obecně shromažďuje informace o preferovaných věcech na této stránce. Zatímco Third-party cookies slouží především pro sledování vašeho prohlížení pro marketingové účely. [8]



Obrázek 1:Cookie (ilustrace)

Zdroj: http://4.bp.blogspot.com/-IpjicHxMeq4/VPDr3jz-5FI/AAAAAAAAAIs/1qiiFliA8gI/s1600/iecookie.png [online] [26. 11. 2016]

3.6 Ochrana digitální stopy

Ochrana vlastních dat není vůbec jednoduchá činnost. Ať už se budete snažit sebevíce vždycky nějakou tu stopu zanecháte. Existují však prostředky, které mohou pomoci minimalizovat rizika spojená s používáním internetu.

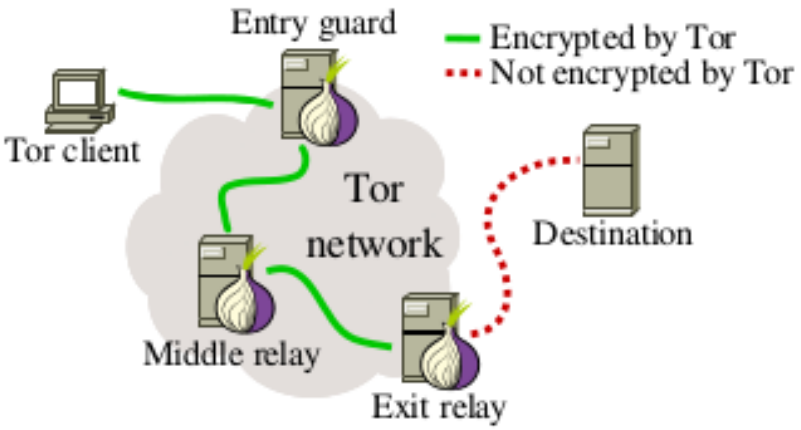
3.6.1 Metoda TOR

Jinak zvané The Onion Routing. Jedná se o software, který umožňuje anonymní přístup k internetu. Při použití této metody je velice obtížné, téměř nemožné, identifikovat jedince, který na stránku přistupuje.

K využití této metody je třeba nainstalovat si software a správně jej nakonfigurovat. Tor funguje tak, že komunikuje přes více TOR serverů zvané node. Pokud tedy využijete tuto metodu připojíte se k prvnímu TOR serveru, který jako jediný zná vaši skutečnou IP adresu. První node se připojí na druhý, ten se připojí na třetí, který stáhne vámi požadovaný obsah a pošle jej zpět k vám. Těchto serverů, které budou využity může být spousta minimálně však musí být využity tři. Hlavní výhoda spočívá v tom, že vaše IP adresa je téměř nevystopovatelná, a to proto, že jednotlivé servery jsou propojeny sériově a znají pouze adresu předchozího a následujícího serveru.

Zajištění anonymity však nestojí na pouhém využívání softwaru a serverů. TOR totiž zajišťuje anonymitu v rámci skupiny. Pokud žijete ve městě, kde každý uživatel používá TOR není možné vás vysledovat, protože i kdyby někdo našel výchozí uzel, ze jehož jste začali, nebude vědět který z počítačů, jež se na něj připojil, prováděl danou činnost, za níž je nyní stíhán.

Mezi nevýhody patří fakt, že serverů metody tor je málo a jsou rozmístěny po celém světě, a proto je rychlost této služby značně omezená. Proto se doporučuje ji používat pouze pokud je to potřebné. Hlavním problémem je však její zneužívání pro nelegální činnosti. [3, 9]



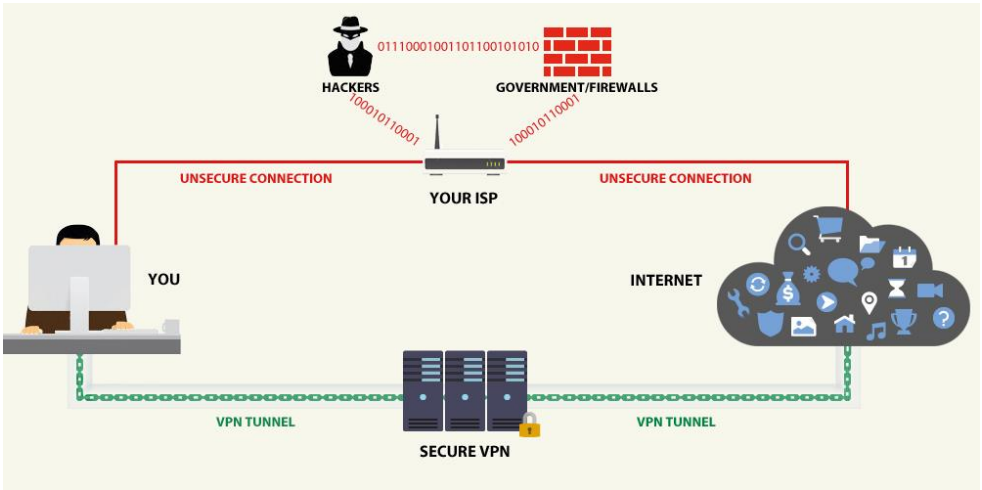
Obrázek 2: Metoda TOR

Zdroj: https://fossbytes.com/wp-content/uploads/2015/09/tor-working.png [online] [26. 11. 2016]

3.6.2 Virtual private network (VPN)

Virtuální privátní síť, jak už název vypovídá, je virtuální a privátní síť uživatele. Je to prostředí, které si uživatel sám vytvoří a může ho tedy považovat za své. Zároveň není skutečné, ale uměle vytvořené. Je to vlastně síť vytvořená v síti. Tvůrce této sítě si v ní může nastavit vlastní pravidla přístupu k internetu.

VPN je velice výhodná z několika důvodů. Prvním z nich je, že uživatel neřeší realizaci sítě, ale nechá jí čistě na poskytovateli. Na této síti si pak uživatel nastaví takové nástroje a technologie, které jemu vyhovují. [10]



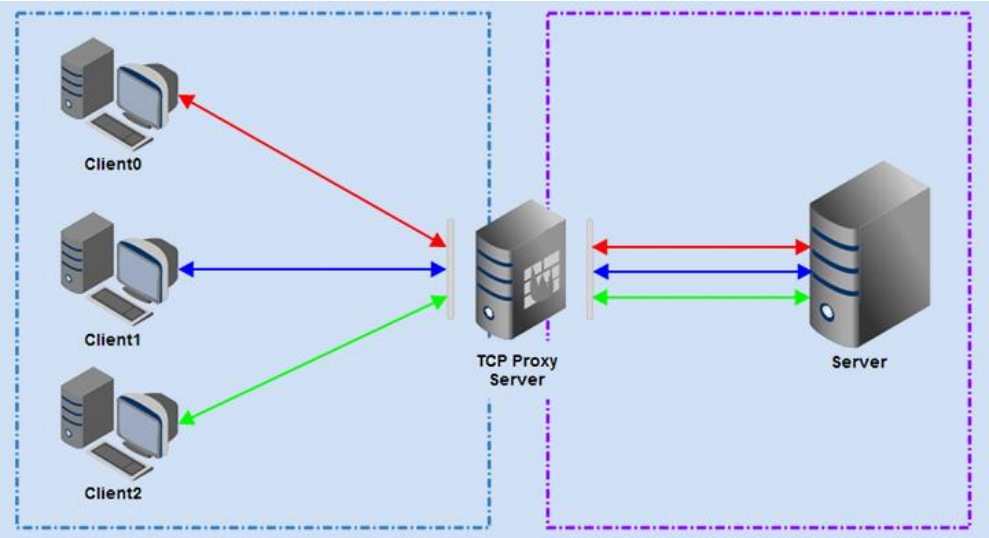
Obrázek 3: Metoda VPN

Zdroj: http://www.afgit.com/wp-content/uploads/2016/03/diagram.jpg [online] [26. 11. 2016]

3.6.3 Proxy server

Tento typ serveru vytváří prostředníka mezi klientským počítačem a cílovým webserverem. V případě připojení na jakoukoliv webovou stránku se pak nezobrazí vaše IP adresa, nýbrž adresa routeru nebo serveru, přes který se připojujete.

Jsou však dva typy proxy serverů. Proxy servery a webové proxy servery. Proxy servery váš počítač propojí s routerem, a při prohlížení webů se zobrazuje adresa právě routeru, jak jsem již zmínil dříve. Webové proxy servery mají dalšího prostředníka a tím je cílový server. Bezpečnost je téměř zaručena. Při brouzdání internetu se nezobrazuje ani vaše adresa, ani adresa vašeho routeru, ale právě adresa cílového serveru. Můžete tedy naprosto anonymně brouzdat internetem. [11]



Obrázek 4: Metoda Proxy server

Zdroj: http://www.partow.net/images/tcpproxy_server_diagram.png [online] [26. 11. 2016]

3.6.4 Základní obrana

Jak jsem již zmínil internet je nebezpečná místo, které monitoruje každý náš krok. Tomuto faktu se bohužel nevyhneme, ale můžeme se pokusit mu předejít. To, že nás monitoruje neznamená, že se nemůžeme bránit. A jak to udělat? Představme si situaci, že se někam máte přihlásit například na facebook. Použijete email a jako heslo kvůli lepšímu pamatování použijete stejné heslo jako máte pro email. A tady je ta chyba. Pokud si

zakládáte účty ať už na herních službách jako je steam nebo se registrujete na různá fóra měli byste volit různé přezdívky a různá hesla. To zajistí, že pokud už někdo odhalí vaše heslo, nemůže ho použít k přihlášení na ostatní vaše uživatelské účty.

Další věc, kterou můžete udělat pro ochranu svých dat, je pravidelná údržba. Tím je myšleno pravidelné instalování aktualizací, ať už operačního systému nebo antiviru, který používáte.

Další obrana je mazání cookies, jak jsem zmínil výše. Pokud je smažete budete sice muset pokaždé návštěvě zadávat hesla (budou-li to stránky vyžadovat jako například přihlašování na sociální sítě, přihlašování e-shopu atd.), ale je lepší zadávat hesla a znovu se stránce identifikovat jako nový uživatel než riskovat, že budou vaše data ukradena a zneužita nebo užita k nelegálním činnostem. [20]

3.7 Hackeři a hackování

V předchozích kapitolách jsem představil digitální stopy a způsob, jak nás ovlivňují. Také jsem představil, co se může stát, když o svá data přijdeme nebo je poskytneme nepovolaným osobám a pár metod, díky nimž se můžeme částečně vyhnout sledování. Taktéž jsem v předchozích kapitolách ve spojení s použitím digitální stopy proti nám používal slovo útočník. Pokud bychom však měli tomuto útočníkovi dát nějaké jméno pravděpodobně to bude Hacker. Pokud někdo použije slovo hacker spousta uživatelů si pod tímto termínem představí zlého člověka, co nás chce za každou cenu poškodit. Tak tomu však není. [12]

„Asi nejvýstižnější definice slova Hacking je: Činnost spočívající v hledání a využívání bezpečnostních děr v počítačových systémech. Motivace hackerů nemusí být finanční, jde také o reputaci, zábavu a překonávání výzev.“ [13]

Hackeři se dělí do mnoha skupin. Stejně tak jako není pouze černá a bílá barva ani hackeři nejsou pouze dobří či zlí. Jednou z prvních kategorií je White hat. Tito hackeři prolamují systémy za účelem zjištění jeho úrovně zabezpečení a v žádném případě jim

nejde o to někomu uškodit nebo se finančně obohatit. Black hat se dá označit jako „škodolibí“ hacker. Jdu mu o osobní obohacování a o poškozování uživatelů pro vlastní pobavení. Gray hat je označení pro člověka, který využívá hackování k informování uživatele, že byl jeho systém napaden, ale také po něm může chtít určitý poplatek za opravu chyby, kterou využil k útoku. Poslední skupinou jsou Blue hat. Blue hat je někdo, kdo se nechává najímat firmami pro ladění či testování softwaru před uvedením na trh. [14]

Kromě výše zmiňovaných kategorií se též hackeři dělí dle zkušeností na zkušené hackery (ať již „hodné“ či „zlé“) nebo úplné začátečníky. Dále se pak také dělí dle vlastních zkušeností (zda používají vlastní naprogramovaný soubor nebo skript, který vytvořil jiný uživatel).

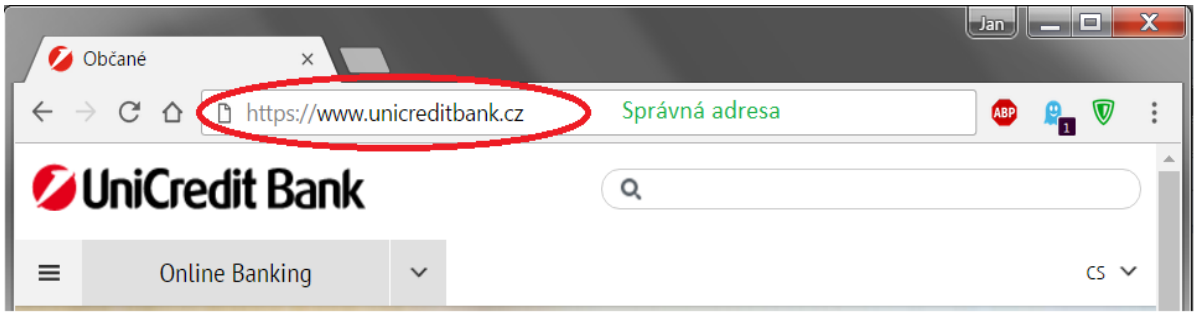
3.8 Nástroje hackerů

Existuje celá škála možností, pomocí kterých hackeři pronikají do našich počítačů. Jedná se převážně o programy nebo webové stránky, které nás mají oklamat tím, že se tváří neškodně nebo povědomě. V následující kapitole si představme několik prostředků, pomocí nichž hackeři pronikají do počítačů a kradou naše data.

3.8.1 Phishing

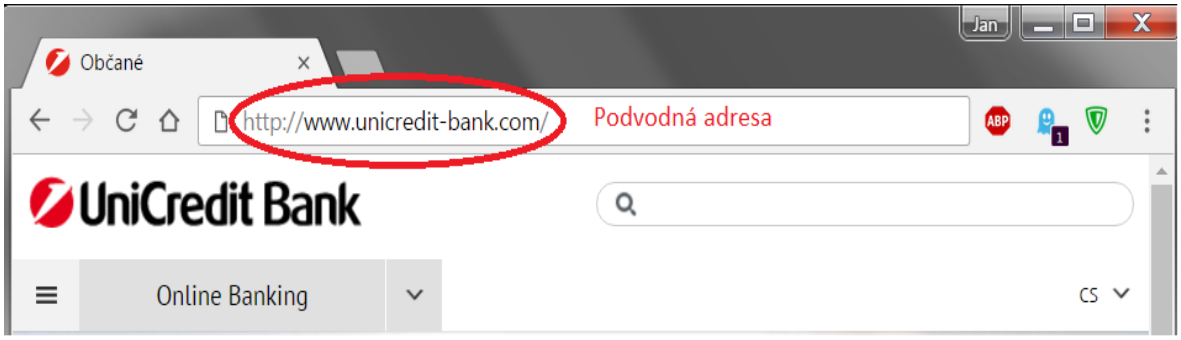
Jde o podvodné emailové zprávy, které vyvolávají dojem, že bylo odeslány od nějakého důvěryhodného zdroje. Slovo phishing se dá přeložit jako rybaření, a přesně tak i tato metoda funguje. Emaily se rozešlou stovkám uživatelů a pak se jen počká kdo se „chytí“. Postup je následující. Útočník vytvoří email nebo internetovou stránku, která vypadá přesně jako internetová stránka a email vaší banky. V emailu může být například napsáno, že pro zlepšení bezpečnosti vašeho účtu je třeba přihlásit se na váš účet a znovu vyplnit dotazník k registraci. Aby pro vás bylo vše jednodušší najdete odkaz na banku v tom samém emailu. Vše vyplníte a odešlete s tím, že nyní bude váš účet bezpečnější. Místo toho jste právě odeslali všechny své informace včetně hesel a rodného čísla zloději. Ale otázkou je, jak je možné, že vše vypadalo tak autenticky? [25]

Odpověď je, že ne vše bylo úplně dokonalé. Útočník zanechal malé nepatrné stopy. Samozřejmě je nezanechal úmyslně. Jedním z možných náznaků může být jiná adresa například místo standartního https://www.unicreditbank.cz/ může odkaz vypadat http://www.unicredit-bank.com/. [15]



Obrázek 5: Správná adresa

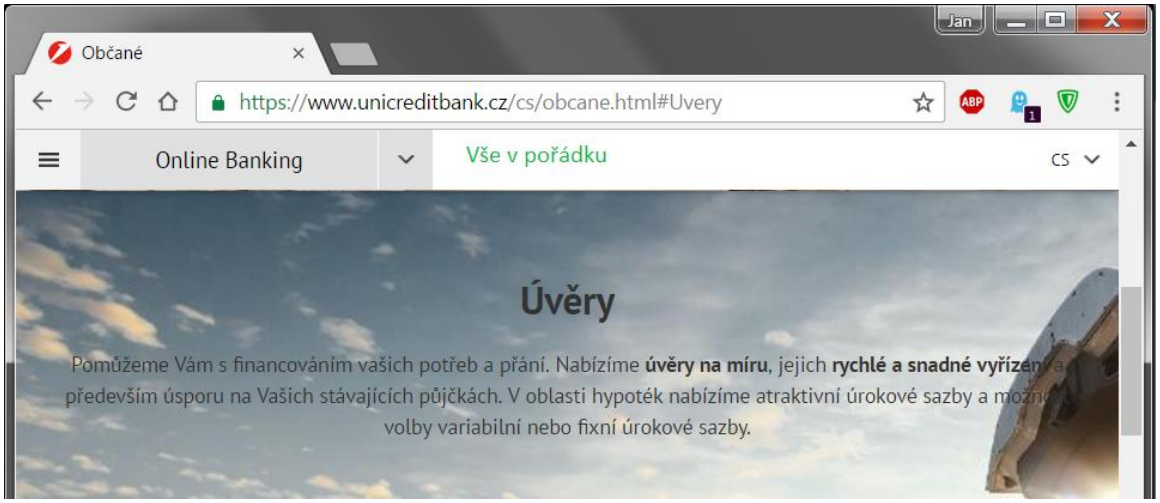
Zdroj: vlastní tvorba



Obrázek 6: Podvodná adresa

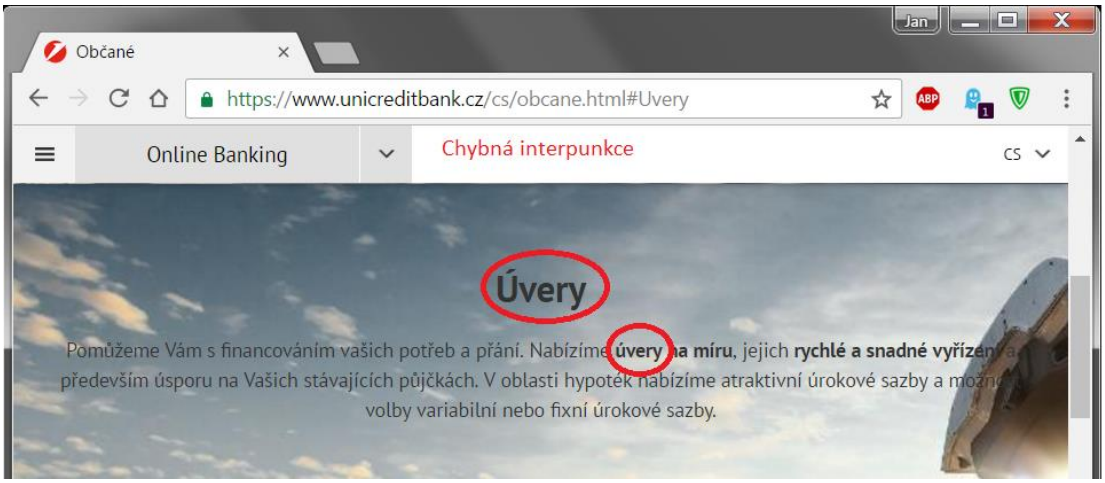
Zdroj: vlastní tvorba

Další náznakem mohou být například chyby v textu.



Obrázek 7: Bez chyb

Zdroj: vlastní tvorba



Obrázek 8: Chybná interpunkce

Zdroj: vlastní tvorba

3.8.2 Trojský kůň

Základním nástrojem hackerů bývá program zvaný trojský kůň. Trojský kůň pochází z příběhu o dobytí Troje, kdy právě tento kůň otevřel brány Troje. A tento program má stejný smysl jak jeho předloha, z níž vychází.

Tento typ viru se může dostat do systému v podobě neškodného programu jako například spořič obrazovky nebo program na likvidaci škodlivého softwaru. Může mít mnoho funkcí. Jednou ze zmiňovaných funkcí je tzv. Backdoor. To znamená, že hackerovi poskytne vzdálený přístup k vašemu počítači a může tak s ním manipulovat nebo hledat uvnitř vaše citlivá data. Další možností jsou destruktivní trojské koně, jejichž činností je likvidace dat.

Nejjednodušší, avšak neméně škodlivou verzí je trojský kůň typu Keylogger. Tento kůň má za cíl dostat se do uživatelova počítače a snímat znaky, jež uživatel zadává do své klávesnice. Tyto data pak odesílá hackerovi a on podle nich může poznat vaše nicky, hesla a emailové adresy. A jelikož Trojani běží na pozadí systému a maskují svou přítomnost ani si tohoto zákeřného viru nemusíte všimnout. [16, 17, 19]

3.8.3 Počítačový červ

Opět se jedná o počítačový program, který je schopen automatického rozesílání sebe sama. Jak již název programu vypovídá, červ se dostane do systému, začne se v něm množit a ovládat systém, buď za účelem získání dat či poškození uživatele. Jeho největší nebezpečí však přichází v jeho množení. Červ je totiž schopen kopírovat sám sebe, a též se samovolně šířit. Například pokud se dostane do vaší emailové pošty je schopen poslat svou kopii všem kontaktům ve vašem emailu. Tam červ nakazí počítač a udělá to samé s kontakty dalšího napadeného počítače. Tím vzniká dominový efekt, který může zapříčinit zpomalení celé sítě a hrozí její následné selhání.

Počítačový červ je velice nebezpečný, neboť jak bylo zmíněno výše může infikovat celou síť a následně ji zpomalit. Větší nebezpečí však přichází s možností červa zanášet do počítače trojské koně. Červ jako takový pouze slouží k zahlcení sítě a následného zpomalování programů v počítači. Ke svému šíření nepotřebuje být zaveden do krycího programu. [16, 17, 19]

3.8.4 Počítačový virus

Jak již název vypovídá virus má za úkol nakazit a poškodit napadený systém. Viry se na rozdíl od červů nedokážou šíři sami a potřebují soubor do kterého se vloží. Virus se však netváří jako užitečný program jako například trojské koně. Virus je vytvořen jako soubor, který je následně odeslán do počítače prostřednictvím emailu nebo jiného prostředku. Pokud je vir následně uživatelem spuštěn, probudí se a udělá, k čemu je naprogramován. Doba aktivace se může lišit. Může být naprogramován na konkrétní datum, může být spuštěn, až bude nakažen určitý počet zařízení či ihned po spuštění.

Viry mohou mít ničivé následky, které slouží k poškození uživatele nebo mohou být otravné, jež mají za cíl obtěžovat uživatele. Mohou taktéž obtěžovat uživatele už tím, že odebírají systému zdroje a zpomalují ho. Některé viry jsou tzv. polymorfní. To znamená, že mají stejný základ s jiným virem, ale úplně jinou funkci. [16, 17, 19]

3.9 Antivirové programy

Pokud mají hackeři zbraň v podobě virů a červů musí mít uživatelé nějaké možnosti obrany. Tedy antivirové programy. Tyto programy slouží k obraně počítače před škodlivým softwarem (viry) a tudíž před případnou ztrátou dat. Pracují na základě neustálého prohlížení dat na základním disku. Tyto kontroly se mohou provádět pravidelně či v případě podezření, že se systém nechová správně, lze sken systému vyžádat. Pokud narazí na virus ukrytý v souboru, okamžitě se ho snaží odstranit nebo přesunout do karantény, aby se vir dále nešířil. V případě menších hrozeb se pokusí antivirový programy soubor opravit, aniž by bylo poškozeny data. Antivirové programy zajišťují obranu pomocí dvou hlavních metod.

První z nich jsou virové databáze. Tyto databáze jsou vytvářeny tvůrci daných antivirů a slouží podobně jako policejní databáze. Jestliže se nějaký program nalezený v systému shoduje s nějakou položkou v databázi je považován za vir a je ihned formulován návrh řešení problému. V případě používání databáze je nutné sledovat a neustále aktualizovat tuto databáze, nýbrž hackeři vynalézají stále nové viry. Antivirové programy pracující na základě databází pouze neskenují data, ale také ihned kontrolují jakékoliv soubor, které jsou do systému stahovány. V takovémto případě lze vir odhalit ihned a může se tak předejít případným problémům předem.

Druhou metodou je pozorování běžících programů. Antivir pozoruje, zda se některé programy nepokoušejí například převzít kontrolu nad systémem nebo jestli neodesílají zprávy mimo počítač (Backdoor viz. výše). V případě nálezu viru vyzve uživatele k výběru dalšího postupu. Výhodou používání této metody je, že ačkoliv může být systém napaden novým virem, antivir rozpozná podezřelé a potenciálně nebezpečné chování. Metoda má bohužel i své nevýhody. Občas se stává, že antivirový program určí za vir program, který ve skutečnosti virem vůbec není. Těmto poplachům se říká Falešné poplachy. Hrozí tak odstranění důležitých dat, a právě díky této nevýhodě je tato metoda stále méně využívána. [18, 19]

Efektivnost jednotlivých antivirových programů je hodnocena nezávislými testovacími agenturami. Testování je prováděno na nejnovější verzi virové databáze. Test hodnotí několik aspektů virového programu. Za prvé počet neodhalených hrozeb, v případě neodhalené hrozby je zjišťováno proč antivir nevyhodnotil daný soubor (program) jako hrozbu. Dále pak počet falešných poplachů čili kolik souborů bylo označeno jako škodlivých, ač žádnou hrozbu nepředstavovali. I v tomto případě je zjišťováno proč k této situaci došlo.

Kromě efektivnosti ve vyhodnocování a odhalování hrozeb je též hodnocena náročnost na systém, tudíž kolik zdrojů antivir odebírá systému. Dalším důležitým aspektem je, jak často vycházejí aktualizace virových databází. V neposlední řadě je hodnocena uživatelská přívětivost. Tedy přehlednost systému. [20, 23]

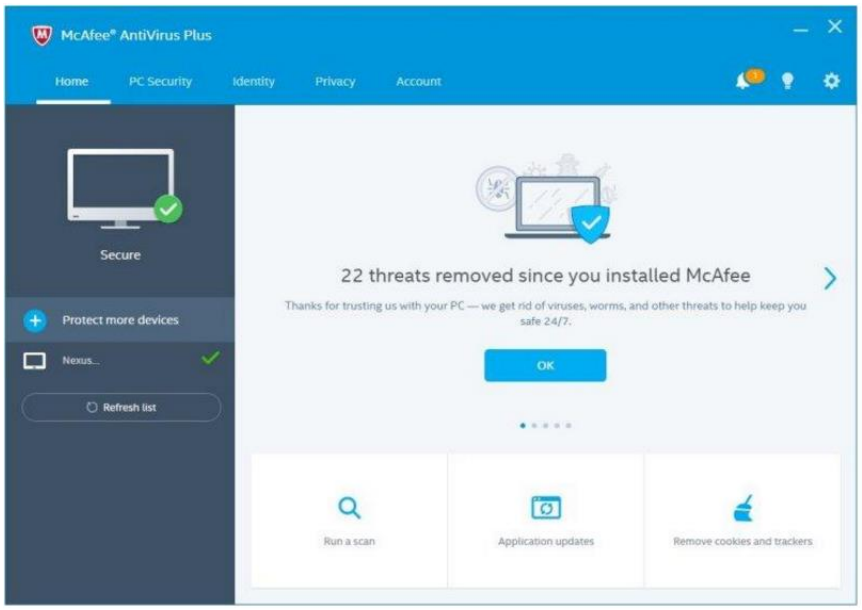
4 Praktická část

4.1 McAfee Antivirus Plus 2016

Antivirus, který lze použít na jakékoliv zařízení (počítač, telefon nebo tablet). To je McAfee plus. Tento placený antivirus poskytuje široké možnosti ochrany, přičemž nově poskytuje tzv. Virus protection pledge, což je slib daný společností, že v případě nálezu nebezpečného softwaru ve vašem zařízení udělají vše, co je v jejich silách, aby zajistili nápravu. V případě neúspěchu vám vrátí peníze. Co se týká ceny je zhruba o 450 korun dražší oproti jiným antivirovým programům, neboť za tuto cenu jej můžete neinstalovat na neomezené množství zařízení.

McAfee při obraně spoléhá na systém obrany Real protect. Tento typ ochrany pracuje na principu pozorování chování programů. V případě zaznamenání neobvyklého chování odešle data o tomto chování do cloudu (centrum McAfee) k analýze a nadále monitoruje chování programu. V případě, že bude program označen za škodlivý odešle zbylé informace o chování programu zpět do cloudu, kde je toto chování zařazeno do databáze pro případ podobných útoků. [21]

Při testování nezávislou společností AV test se McAfee ukázalo jako docela dobrý antivirus. Při testech ochrany proti virů zero-day (nejnovější viry, které byly vytvořeny nedávno) se ukázalo, že zachytává 97,9 % malwarů, čímž trochu zaostává za jinými antiviry. Překvapil však svojí „nenáročností“. Při kontrolování uživatelské aktivity (surfování po internetu, spouštění aplikací, kopírování souborů) nebere sytému tolik zdrojů kolik by se očekávalo. Taktéž při kontrole celého systému téměř vůbec nezatěžuje počítač. [22]



Obrázek 9: Uživatelské rozhraní McAfee

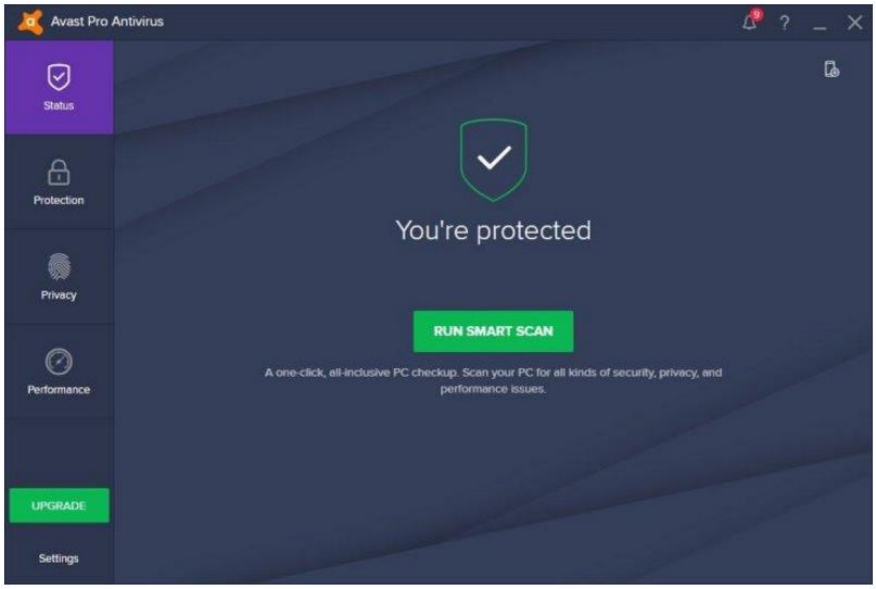
Zdroj: http://uk.pcmag.com/mcafee-antivirus-plus-2015/36055/review/mcafee-antivirus-plus-2017 [online] [25. 2. 2017]

4.2 Avast PRO Antivirus 2016

Avast je česká firma, která poskytuje velice rozsáhlé služby v oblasti antivirových programů a hlídání naší digitální stopy. Již jeho free verze obsahuje spoustu nástrojů, které bezpečně zajistí váš počítač. Avast PRO obsahuje ještě více nástrojů jako například wi-fi inspector (skenování sítě kvůli bezpečnostním důvodům) nebo možnost vytvořit bootovací záchranný disk, kterým je možná nastartovat počítač v případě že byl napaden agresivním malwarem, který systém blokuje v jeho úspěšném zapnutí.

Antivirus též nabízí možnosti virtuální privátní sítě či čistič počítače od zastaralých nebo zbytkových souborů. Oba tyto nástroje však vyžadují připlatit si je jako bonus navíc, což trochu ubírá na celkovém dojmu z jinak slibně vypadajícího a štědrého systému. Čím se však Avast PRO může pyšnit je nástroj sandbox. Tento nástroj slouží pro testování programů. Chová-li se nějaký program či soubor podezřele sandbox jej uzavře do virtuální schránky a nechá ho pracovat. Tím antivirus zjistí, jaké škody malware dokáže napáchat bez ohrožení systému. [21]

Testování odhalilo, že je schopen zachytit 98,8 % škodlivých souborů. I jeho běžné kontrolování systému je velice dobré a nenáročné pro chod celého počítače. Čím však Avast zaostává je jeho čerpání zdrojů při běžné uživatelské aktivitě, kde systém pobírá více zdrojů, než by se uživateli mohli líbit. [22]



Obrázek 10: Uživatelské rozhraní Avast

Zdroj: http://uk.pcmag.com/avast-pro-antivirus-2015/37302/review/avast-pro-antivirus-2017 [online] [25. 2. 2017]

4.3 Bitdefender Antivirus Plus 2017

Úkolem antivirových programů obecně je starat se, aby se do systému nedostal škodlivý soubor nebo program s úmyslem ukrást data z vašeho počítače. Birdefender však zajišťuje mnohem více než jen ochranu před malvary. Už při své instalaci Bitdefender skenuje systém pro přítomnost škodlivého softwaru, který by mohl přerušit instalaci.

Jednou z nejužitečnějších funkcí je Autopilot. Pokud jede antivirus na autopilota a nalezne škodlivý software zlikviduje ho v tichosti a neobtěžuje uživatele výstrahami. Pokud však někdo chce vědět, že byl jeho systém napaden lze tuto funkci v nastavení vypnout a sám koordinovat co má antivir udělat s dotyčným malwarem. Bitdefender též obsahuje antiphishingovou obranu, jenž v případě rozpoznání podvodné stránky zabrání uživateli ve vstupu a upozorní ho na podezřelou stránku či email. Bitdefender obsahuje také sken zranitelnosti. Jde o sken, který vyhledává chybějící aktualizace například pro

zastaralé prohlížeče a další nástroje jako například Java. A v neposlední řadě chrání počítač před nezabezpečenými wi-fi pomocí nástroje Wi-fi Advisor. Tento nástroj hlídá, zda někdo na konkrétních wi-fi neodposlouchává komunikaci či nezískává vaše osobní data. [21]

Během testů se Bitdefender ukázal jako skvělý antivirus schopný odrazit drtivou většinu virů. Při testech dosahoval výsledku 99,8 % úspěšnosti v odstraňování hrozeb. Taktéž při testech zběžného kontrolování systému se ukázal jako velice efektivní a systém nezatěžující. Lehkou náročnost však vyžaduje při kontrolování běžné uživatelské činnosti, avšak nejde o žádnou výraznou odchylku oproti konkurenčním antivirům. [22]

Obrázek 11: Uživatelské rozhraní Bitdefender

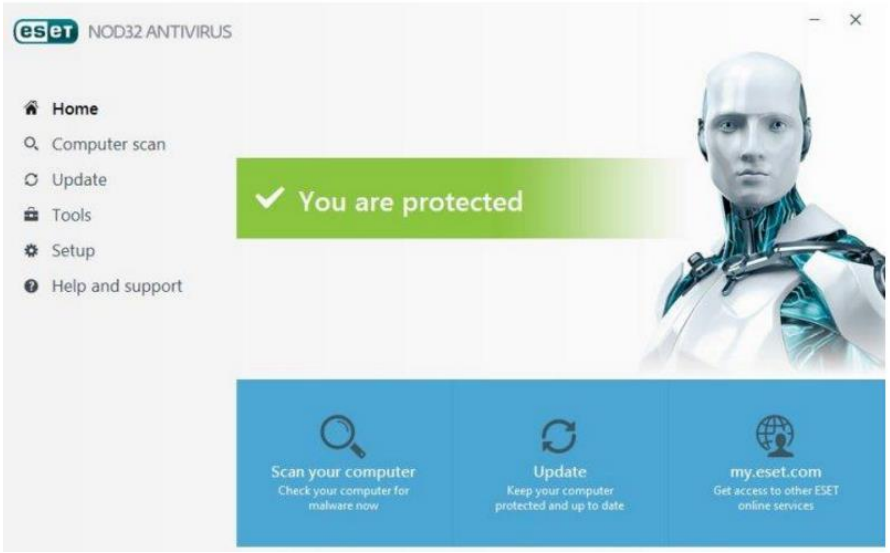
Zdroj: http://uk.pcmag.com/bitdefender-antivirus-plus-2015/34128/review/bitdefender-antivirus-plus-2017 [online] [25. 2. 2017]

4.4 ESET NOD32 Antivirus 2016

Za roční poplatek ESET automaticky nabízí 3 licence pro osobní počítače. Ihned při instalaci začal ESET kontrolovat systém a stahovat nejnovější aktualizace. Navíc se během instalace dotáže, zda máte zájem o program na detekci potenciálně nechtěných aplikací (mezi tyto aplikace patří programy obsahující reklamy, programy instalující nechtěné doplňky).

ESET disponuje rozsáhlými možnostmi co se týká skenování systému. Můžete si vybrat, který konkrétní disk, soubor nebo program chcete oskenovat. Rychlost skenování souborů je celkem obdivuhodná, neboť se jedná téměř o polovinu času, kterou potřebují ostatní antivirové programy pro skenování. Je to zapříčiněno i tím, že ESET neskenuje soubory, které již byly označeny za bezpečné. ESET se taktéž rychle zbavuje škodlivých souborů a jiného malwaru díky jeho real-time skeneru, který hlídá uživatele například při otevírání nových příchozích souborů. Co však ESETu chybí je lepší ochrana před phishingem, neboť jeho současná ochrana je v tomto ohledu nekompletní. Tento nedostatek však vynahrazuje správou externích zařízení. Uživatel má možnost si sám nastavit, jaká zařízení mají oprávnění spojit se s počítačem a jaká ne. Tímto způsobem se zamezuje především útokům směřujícím z externích zařízení, která mohou nést jak ničivé viry, tak viry sloužící k odposlouchávání uživatele. [21]

Při odrážení malwarových útoků si vedl ESET znamenitě. Jeho výsledky se pohybují okolo 99,8 % úspěšnosti v odstraňování virů. Jeho nevýhodou je kontrola uživatelské aktivity, při níž odebírá větší množství zdrojů, avšak toto čerpání zdrojů není tak velké jako u jiných méně úspěšných antivirů. Dalo by se označit za průměrné. [22]



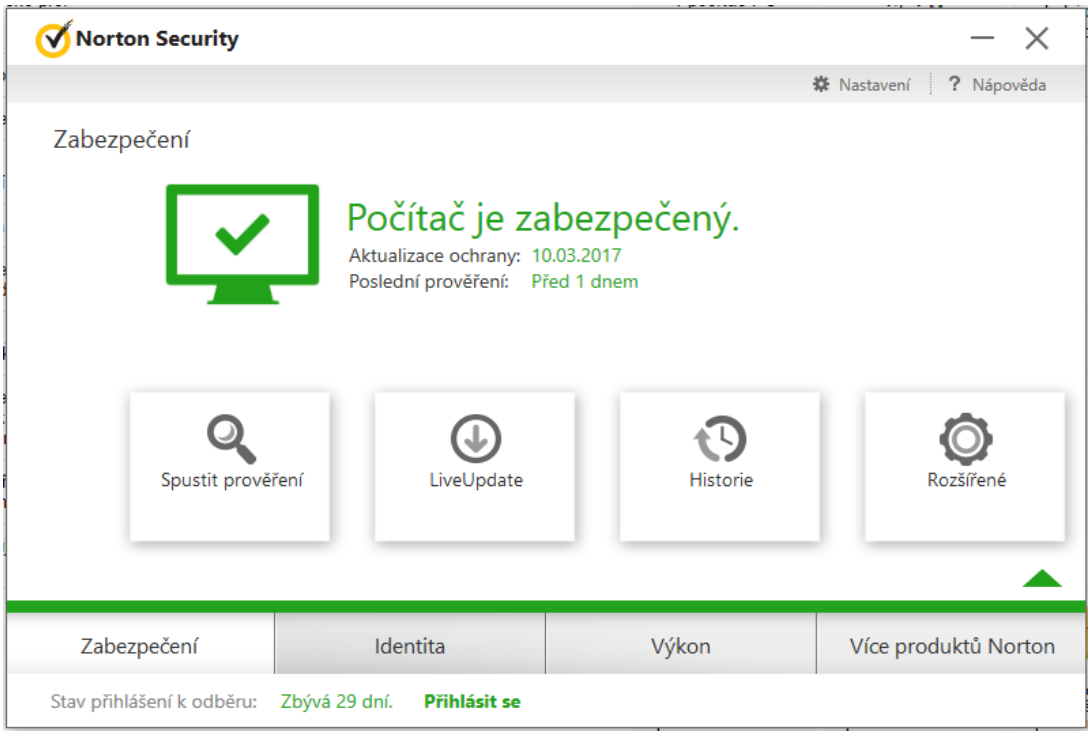
Obrázek 12: Uživatelské rozhraní ESET

Zdroj: http://uk.pcmag.com/eset-nod32-antivirus-8/36405/review/eset-nod32-antivirus-10 [online] [25. 2. 2017]

4.5 Norton Antivirus 2014

Antivirus vytvořený společností Symatec. Za přívětivou cenu nabízí 10 licencí pro osobní počítače. Při instalaci tohoto antiviru se okamžitě začnou stahovat nejnovější definice virů (aktualizace virové databáze), díky čemuž je ihned připraven bránit systém a není nutné čekat na aktualizaci. Běžný sken obvykle zanechá nějaké malwary v počítači. Norton je však vybaven agresivnějším skenovacím programem zvaným Norton Power Eraser, který odstraní většinu problémových programů. Norton také disponuje velice kvalitní obranou proti phishingu, a to především díky real-time ochraně. [21]

Stejně jako u předešlých testů (ač ne u všech byl tento fakt zmíněn) i zde byl proveden test ochrany nezávislou společností AV test. Díky jeho agresivnějšímu sken dokázal najít 99,5 % virů. Taktéž jeho kontrola běžné uživatelské činnosti je velice dobrá a dokáže chránit před malwary i phishingovými technikami. Co se kontrolování systému týče je Norton lehce náročnější, ale tato náročnost je v podstatě zanedbatelná. [22]



Obrázek 13: Norton uživatelské rozhraní

Zdroj: vlastní tvorba

4.6 Hodnocení antivirových programů

	Ochrana proti malwaru	Zatíženost systému při běžné aktivitě	Zatíženost systému při skenování
McAfee Antivirus Plus 2016	97,9%	5,5	6
Avast PRO Antivirus 2016	98,8%	3,5	6
Bitdefender Antivirus Plus 2016	99,8%	5,5	6
ESET NOD32 Antivirus 2016	99,8%	4,5	6
Norton Antivirus 2014	99,5%	5,5	5,5

Tabulka 1: Souhrn výsledků z testů společnosti AV test

Zdroj: vlastní tvorba

Hodnoty uvedené v tabulce jsou vyjmuty především z profesionálních testů společnosti AV test, která se na takovýmito hodnoceními zabývají.

Použití bodovací metody	Ochrana proti malwaru	Zatíženost systému při běžné aktivitě	Zatíženost systému při skenování	Hodnocení
McAfee Antivirus Plus 2016	1	5	5	11
Avast PRO Antivirus 2016	2	1	5	8
Bitdefender Antivirus Plus 2016	5	5	5	15
ESET NOD32 Antivirus 2016	5	2	5	12
Norton Antivirus 2014	3	5	1	9

Tabulka 2: Vyhodnocení bodovací metodou

Zdroj: vlastní tvorba

Pomocí bodovací metody byl podle výsledku testů AV test vybrán antivirus Bitdefender.

4.7 Vlastní testování

	McAfee	Avast	Bitdefender	ESET	Norton
Výsledek 1	88%	96%	97%	85%	90%
Výsledek 2	91%	93%	92%	92%	92%
Výsledek 3	89%	97%	96%	98%	94%
Výsledek 4	92%	88%	98%	90%	97%
Výsledek 5	87%	90%	94%	94%	95%
Celkem	89%	93%	95%	92%	94%
AV test	97,9%	98,8%	99,8%	99,8%	99,5%

Tabulka 3: Vlastní hodnocení

Zdroj: vlastní tvorba

K testování bylo použito 100 různých malvarových souborů (například malvary s funkcí backdoor nebo keylogger). Při testech bylo zjištěno, že výsledky z nezávislé testovací společnosti Av test jsou velice podobné mým, až na výjimku Nortonu, který při vlastním testování svými výsledky překonal ESET oproti profesionálnímu testu.

5 Závěr

Od vzniku internetu se informační technologie ženou směrem ku předu a využívá je více a více lidí po celém světě. Digitální stopy jsou součástí našeho života, a právě díky internetu jsou tyto naše stopy sdíleny a ukládány. S tímto faktem souvisí i kradení a zneužívání těchto stop, čemuž se v dnešní době sítí už nevyhneme.

Hlavním cílem práce bylo představit nebezpečí spojené s digitálními stopami a dále představit možnosti efektivní obrany před případnými ztrátami dat. Kontrola našich digitálních stop je velice důležitá zvláště, pokud si hlídáme své soukromí. Avšak hlídání stopy v dnešní době se v podstatě rovná životu na příslovečném okraji společnosti, protože kdo nesdílí neexistuje. Přičemž si nikdo pořádně neuvědomuje rizika spojená s ukazováním svého osobního života veřejnosti. Hlídání digitální stopy je velice důležitá činnost, obzvláště pokud se chceme vyhnout případným problémům. Hlídání aktivní digitální stopy je jednoduší, protože my sami můžeme snadno ovlivnit co sdílíme nebo posíláme, ale vezmeme-li do úvahy sociální sítě je uhlídání aktivní stopy možné pouze zrušením všech účtů, neboť vaše data mohou být sdílena někým jiným.

Co se pasivních digitálních stop týká je to o dost složitější. K ochraně této stopy je třeba software, který vás dostane do anonymity. Další aspektem jsou samozřejmě hackeři, kteří útočí na náš počítač viry. V takovém případě je třeba se uchýlit k ochranným softwarům jako jsou antivirové programy. Jak jsme si mohli všimnout, všechny vykazují vysoké výsledky při zachytávání hrozeb. Ne všechny jsou si však rovny a hlavní rozdíl tak spočívá v náročnosti na systém a funkcích, které poskytují navíc ke svým běžným funkcím.

Digitální stopy se zkrátka staly součástí našeho života a musíme se s nimi naučit žít. Je však spousta prostředků, jak se efektivně bránit a je třeba je aktivně využívat, abychom to nebyli právě my, kdo doplatí na nedostatek ochranných prostředků.

6 Seznam použitých zdrojů

1. Kysela, Radek. Digitální stopy zanechávané na internetu [online]. c 2011 [cit. 26. 11. 2016] Dostupný na World Wide Web: <http://www.kysela.info/digitalni-stopy.html>

2. Černý, Michal. Digitální stopy a digitální identita [online]. c 2011 [cit. 26. 11. 2016] Dostupný na World Wide Web: <http://clanky.rvp.cz/clanek/k/g/12943/DIGITALNI-STOPY-A-DIGITALNI-IDENTITA.html/>

3. Digitální stopy [online]. c 2013 [cit. 26. 11. 2016] Dostupný na World Wide Web: <https://wikisofia.cz/wiki/Digit%C3%A1ln%C3%AD_stopa> ISSN: 2336-5897

4. Behaviorální marketing [online]. c 2017 [cit. 26. 11. 2016] Dostupný na World Wide Web: <https://www.mediaguru.cz/medialni-slovnik/behavioralni-marketing/>

5. Krádež identity a jak se jí bránit [online]. [cit. 26. 11. 2016] Dostupný na World Wide Web: <http://www.bezpecnyinternet.cz/pokrocily/ochrana-prav/kradez-identity.aspx>

6. Merritt, Marian. Úvod do krádeže identity [online]. c 1995-2016 [cit. 27. 2. 2017] Dostupný na World Wide Web: <https://cz.norton.com/identity-theft-primer/article>

7. Co jsou to cookies [online]. c 2005-2017 [cit. 26. 11. 2016] Dostupný na World Wide web: <http://www.adaptic.cz/znalosti/slovnicek/cookies/>

8. What are Cookies and what do cookies do? [online]. c 2017 [cit. 26. 11. 2016] Dostupný na World Wide Web: <http://www.webopedia.com/DidYouKnow/Internet/all_about_cookies.asp>

9. Jak funguje TOR [online]. c 2016 [cit. 26. 11. 2016] Dostupný na World Wide Web: <http://timehosting.cz/jak-funguje-tor/>

10. Co je to virtuální a privátní síť (VPN) a k čemu se hodí? [online]. c 1999-2017, poslední revize 2. prosince 2003 [cit. 26. 11. 2016] Dostupný na World Wide Web: <http://technet.idnes.cz/co-to-je-virtualni-privatni-sit-vpn-a-k-cemu-se-hodi-fw6-/sw_internet.aspx?c=A031201_5247613_sw_internet>

11. Vrba, Marek. Proxy servery: Jak se falšuje návštěvnost [online]. c 1998-2017, poslední revize 26. ledna 2005 [cit. 26. 11. 2016] Dostupný na World Wide Web: <http://www.lupa.cz/clanky/proxy-servery-jak-se-falsuje-navstevnost/>

12. What is hacking? [online]. c 2000-2017 [cit. 11. 2. 2017] Dostupný na World Wide Web: <http://whatismyipaddress.com/hacking> stejné jako u antivirů

13. Hacking [online]. c 2017 [cit. 11. 2. 2017] Dostupný na World Wide Web: <http://www.zive.cz/hacking/sc-381/default.aspx> ISSN 1213-8991

14. Kovacs, Nadia. What is the difference between black, white and grey hat hackers? [online]. c 1995-2017, poslední úprava 17. dubna 2015 [cit. 11. 2. 2017] Dostupný na World Wide Web: <https://community.norton.com/en/blogs/norton-protection-blog/what-difference-between-black-white-and-grey-hat-hackers>

15. Džubák, Josef. Co je to phishing [online]. c 2000-2017 [cit. 11. 2. 2017] Dostupný na World Wide Web: <http://www.hoax.cz/phishing/co-je-to-phishing>

16. Co je to virus, červ a trojský kůň? [online]. c 2011 [cit. 11. 2. 2017] Dostupný na World Wide Web: <http://www.srpenec.cz/internet/bezpecnost/co-je-to-virus-cerv-a-trojsky-kun>

17. Mikláš, Michal. Počítačový virus obecně [online]. [cit. 11. 2. 2017] Dostupný na World Wide Web: <http://www.gjszlin.cz/ivt/esf/ostatni-sin/pocitacove-viry.php>

18. Gardner, Mark. Antivirová ochrana [online]. c 2017 [cit. 11. 2. 2017] Dostupný na World Wide Web: <http://gvpdoc.comehere.cz/doku.php?id=wiki:informatika:antiviry>
19.
20. Gardner, Mark. Viry a antiviry [online]. c 1999-2017 [cit. 18. 2. 2017] Dostupný na World Wide Web: <http://marecek.blog.idnes.cz/blog.aspx?c=106382>

21. KRÁL, M. Bezpečný internet – Chraňte sebe i svůj počítač 184 str. ISBN: 978-80-247-5453-6 [cit. 18. 2. 2017]

22. Rubenking, Neil. The Best Antivirus Protection of 2017[online]. c 2017, poslední úprava 21. února 2017 [cit. 18. 2. 2017] Dostupný na World Wide Web:<http://uk.pcmag.com/antivirus-reviews/8141/guide/the-best-antivirus-protection-of-2017>

23. The best antivirus software for Windows Home User[online]. c 2017 [cit. 18. 2. 2017] Dostupný na World Wide Web:<https://www.av-test.org/en/antivirus/home-windows/windows-10/>

24. LOHINSKÝ, J., KOCMAN, R. Jak se bránit virům, spamu a spyware 152 str. EAN: 9788025107935 [cit. 18. 2. 2017]

25. Lance, James. Phishing bez záhad 281 str. ISBN: 80-247-1766-2 EAN: 9788024717661 [cit. 18. 2. 2017]