Netiketa a bezpečnost na Internetu

Jiří Kratochvíl

Knihovna univerzitního kampusu
Masarykova univerzita 2013

Obsah

1 Úvod

Ve studijním materiálu o informační hygieně jsme již uvedli, že je internet nedílnou součástí našeho života, do něhož kromě řady pozitiv přináší i řadu negativních prvků. V předchozím dokumentu jsme se zaměřili především na eliminování těch jevů, které negativně působí na naše psychické, případně i fyzické zdraví. V následujícím textu rozšiřujeme tato preventivní opatření o další, a to konkrétní pravidla chování na internetu a při práci s počítačem, jež bývají souhrnně označována jako *netiketa*.

2 Netiketa

Tento pojem vznikl zkrácením slovního spojení Network Etiquette (Netiquette → Netiketa) a poprvé jej v roce 1995 použila Sally Hambridge ve své příručce popisující celou řadu pravidel netikety.[1] Nezávisle na této publikaci shrnula do desatera obdobná pravidla netikety také americká autorka Virginia Shea.[2]

1) **Remember the human (Mysli na druhé)**

   Tím, že s ostatními komunikujeme nepřímo prostřednictvím různých technologií, zapomínáme, že příjemcem našeho chování na internetu je stále člověk, a proto zde platí zlaté pravidlo: Nečiň druhým, co nechceš, aby oni činili tobě.

   Pod toto pravidlo můžeme včlenit nejrůznější dílčí pravidla, jako jsou:

   - Nerozesílej materiály, jejichž nejsi vlastníkem.
   - Nepřeposílej řetězové e-maily.

2) **Adhere to the same standards of behavior online (Na internetu se chovej, jako se chováš ve skutečném světě)**

   - Neuháněj druhé kvůli odpovědi na tvůj dotaz, mohou být zaneprázdněni jinou činností.
   - Před odhlášením z chatu/ICQ apod. se rozluč s ostatními.
   - Nechatuj s cizími lidmi
   - Počítej s tím, že zákony platné v reálném světě jsou platné i v tom virtuálním.

3) **Know where you are in cyberspace (Mysli na to, kde se právě v kyberprostoru pohybuješ)**

   - Před odesláním pošty se ujisti, není-li e-mailová adresa příjemce ve skutečnosti adresa skupiny osob pod přezdívkou.
   - Pamatuj na prostředí, z něhož adresát pochází, aby kvůli různým kulturám, jazykům, či smyslu pro humor nedošlo k nedorozumění.
   - V neformální komunikaci vyjádři tón hlasu příslušným smajlíkem, ale zároveň to s jejich množstvím nepřeháněj
   - Nepoužívej ve zprávě znaky, které nemusejí být čitelné v adresátově aplikaci.
   - Namísto zpráv s velkými přílohami pošlete adresátovi odkaz na soubor uložený v online úschovně (např. v IS MU, eDisk apod.); neznáte totiž kapacitu adresátovy schránky.

- Jste-li noví v určitém virtuálním prostředí (např. diskusní fórum, chat), nejdříve se porozhlédněte a seznamte s tamějšími zvyky a chováním a až pak se aktivně zapojujte.

4) **Respect other people's time and bandwidth (Respektuj čas a informační kapacitu ostatních)**

- Než odpovíš na e-mail, podívej se na ostatní doručenou poštu, jestli adresát již problém nevyřešil.
- Před odpovědí se ujisti, nejsi-li jen adresát v kopii a jestli tedy není zbytečné se do diskuse ostatních přidávat.
- Než někomu položíš dotaz, ujisti se, není-li již jinde zodpovězen a spadá-li skutečně do kompetencí zamýšleného adresáta.
- Než někoho požádáš o pomoc s nějakým problémem, zkus jej nejdříve vyřešit sám (např. podívat se do FAQ, přečíst si návod k přístroji apod.).
- Při příchodu do chatovací místnosti pozdrav jednou všechny a ne každého zvlášť.
- Pamatujte, že i ostatní mají své úkoly jako vy a nemohou se vám ihned věnovat.

5) **Make yourself look good online (Mysli na svou pověst v online prostředí)**

- Na konci zprávy vždy uváděj kontakt na sebe.
- Nemáte-li právě čas na delší odpověď odesílateli, napište mu krátce, kdy mu vše zodpovíte.
- Zjistíš-li ve svém příspěvku do diskusního fóra chybu, co nejdříve jej zruš nebo jej oprav.
- Chovej se na internetu stejně jako v reálném světě, dbej na svůj jazyk, kterým s ostatními komunikuješ, nenech se strhnout k pravopisným chybám nebo vulgarismům jen proto, že tak třeba komunikují ostatní.
- Vyjadřuj se k tomu, čemu skutečně rozumíš, a dbej na to, aby tvé vyjádření mělo logiku a bylo argumentačně silné.
- Vyvaruj se hrubostí a urážení ve svých vyjádřeních k ostatním.
- Když už se musíš hrubě vyjadřovat (např. jde o nějaký expresivní projev umění), čiň tak jen v příslušné diskusní skupině a vulgarismy raději nahraď eufemismy nebo nahrazením většiny znaků hvězdičkami (např. F*** off)

6) **Share expert knowledge (Poděl se s ostatními o své znalosti)**

- V diskusích o filmech nebo knihách vyznač, kde začíná a končí pasáž obsahující tzv. spoilery, které prozrazují vyústění zápletky.
- Znáš-li odpověď na otázku položenou ve virtuálním prostředí, zodpověz ji.
- Položíš-li otázku ve skupině, kterou pravidelně nenavštěvuješ, zaklikni si (je-li to možné) automatické upozornění na zodpovězení tvého dotazu.

7) **Help keep flame wars under control (Vyvaruj se hrubého chování na internetu a nepodporujte ho)**

- Nepiš zprávu verzálkami, vypadá to tak, že adresátovi nadáváš.
- Na emoce vzbuzující informace reaguj později, až se zklidníš.

- Pokud skutečně potřebuješ zdůraznit své emoce, uvozuj příslušnou zprávu na začátku nápisem FLAME ON a na konci FLAME OFF (Pojmem flaming se označuje hrubá komunikace mezi uživateli internetu.).
- Při odpovědi ponechejme z předchozích zpráv jen nejnutnější informace pro pochopení kontextu komunikace.

8) **Respect other people's privacy (Respektuj soukromí druhých)**

- Bez souhlasu odesílatele nepřeposílej soukromou zprávu ostatním.
- Když na tebe dotyčný nereaguje ani po druhé tvé zprávě, nechej ho, nestojí o komunikaci.
- Nerozesílej komunikaci z privátních diskusních fór těm, kteří členy takové skupiny nejsou.
- Nevystavuj žádný svůj materiál ostatním v cizím úložišti.
- Neptej se ostatních na nic ohledně sexu, věku nebo místa pobytu, zvláště, když je neznáš a oni neznají tebe.
- Respektuj ostatní, používají-li přezdívky, a neprozrazuj jejich jména, i kdybys je osobně znal.
- Nepokoušej se přihlašovat k jakémukoliv cizímu účtu.

9) **Don't abuse your power (Nezneužívej svou sílu)**

- Jsi-li expertem v kyberprostoru (např. správce diskusního fóra, administrátor sítě apod.), nezneužívej své znalosti a práva například k čtení cizí pošty, mazání triviálních příspěvků od nováčků v tebou spravovaném systému, či nezdvořilému až arogantnímu upozorňování na chyby ostatních.

10) **Be forgiving of other people's mistakes (Odpouštěj druhým jejich chyby)**

- Každý jednou začínal, a proto buď shovívavý k ostatním, když udělají začátečnickou chybu.
- Rozmysli se, jestli je chyba toho druhého skutečně tak zásadní, že ji nelze přejít mlčením.
- Když už někoho na chybu upozorníš, buď zdvořilý.

3 Bezpečnost na internetu

Netiketa svou podstatou úzce souvisí s bezpečným chováním na internetu, zvláště pak v pravidlech týkajících se ochrany soukromí, nezneužívání znalostí virtuálního prostředí a správy systémů, či využívání elektronické pošty.

Internet zprostředkovává celou řadu funkcí, ať už se jedná o zábavu (hudba, film atd.), komerční obsah (reklamy, nakupování apod.), či další nejrůznější služby (elektronická pošta, elektronické bankovnictví, elektronické vyřizování úředních záležitostí atd.). [3(pp164–165)] Souběžně se vznikem a rozvojem internetu roste pochopitelně i riziko jeho zneužití v nejrůznějších formách. Tehdy hovoříme o tzv. počítačové nebo internetové kriminalitě, případně kybernalitě, [4(p19),5, 6(pp34–32)] která se může projevovat v nejrůznějších formách.

Kyberterorismus

Jednou z forem počítačové kriminality je kyberterorismus spočívající v útoku proti počítačům, počítačové síti s cílem proniknout k uloženým informacím.[5,7,8,9] Tomuto útoku jsou pochopitelně vystaveny i naše osobní počítače, proto si stručně shrňme nástroje, jimiž může k jejich ohrožení dojít, a doporučení, jak této hrozbě předejít.

V souvislosti s tím, kdo tyto útoky provádí, se můžeme setkat s pojmy *hacker* a *cracker*. Označují se tak právě ti, kteří se do počítačového systému snaží proniknout, přičemž zatímco hacker tak činí ze snahy prokázat své schopnosti prolomit se do systému a přitom žádná data nezcizit, cracker naopak tak činí s cílem poškodit systém a získaná data a informace ke svému prospěchu dále zneužít.[5,8,9]

Malware

Jednou z možností k proniknutí do cizího počítače je využit software poškozující po spuštění systém a v něm uložená data.[5,9, 10(p37)] Jedná se o nejrůznější aplikace, pro něž se používá zastřešující název malware a jimiž se především crackeři snaží dobít do systému počítače. Uveďme si alespoň několik těchto nástrojů, s nimiž se můžeme setkat i při používání osobního počítače.

Adware
: Ačkoliv po nainstalování se tento typ softwaru jeví neškodně tím, že umožní funkci vyskakovacích oken s reklamami, může ve skutečnosti sledovat, které stránky při surfování na internetu navštěvujete a jak se tedy chováte na internetu, a tyto získané informace odesílat původci příslušného adwaru.[5,8, 10(p248), 11(p3)]

Spyware
: Svým chováním má tak adware blízko spywaru, kterým se označují programy shromažďující nejrůznější údaje o chování uživatele počítače nebo počítačového systému (použité klávesy, obrázky, obsah adresářů apod.) a zasílající tyto informace původci dané aplikace.[5, 10(p233)]

Počítačové viry (viruses)
: Jedná se o škodlivý software snažící se kopírovat sebe sama v ostatních programech, čímž narušuje jejich fungování, zpomaluje jejich činnost nebo může poškodit i disk nebo disketu. V praxi se můžeme setkat s různými typů virů, jako jsou logické bomby (logic bomb) vyznačující se vytvořením nějaké logické chyby v programu, nebo časované bomby (time bomb) spouštějící se a ohrožující tak počítač v předem stanovený čas.[8, 10(pp37–38), 12(p71)]

Červ (worm)
: Pojmem se označují samostatné programy vytvářející kopie sebe sama a využívající bezpečnostní díry k proniknutí do dalšího počítačového systému.

  Nejedná se o počítačový vir, neboť zatímco vir se musí připojit k nějakému programu a do počítačového systému se obvykle dostává prostřednictvím e-mailové pošty, nosiče médií apod., červ funguje zcela samostatně a sám nalézá bezpečnostní díry a proniká jimi do hostitelské počítačové sítě. V nich slouží k vyhledávání citlivých informací, jako jsou hesla, čísla kreditních karet apod., ale i vojenská data či další bankovní údaje.[5, 10(pp99–100), 12(pp71–72),13]

Trojský kůň (Trojan Horse)
: Je programem vloženým do počítačového systému bez vědomí uživatele například při stažení nějakého programu z internetu, instalaci aplikace z pochybných zdarma dostupných CD-ROMů apod.

Na rozdíl od virů a červů trojský kůň nekopíruje sebe sama, ale umožňuje průnik svému původci do počítačového systému hostitele a sleduje uživatelovo chování. Zvláště zaznamenává, které klávesy uživatel stiskl při zadávání hesla, jaké webové stránky si prohlížel apod.[5, 10(pp123–126), 12(p72)]

Zadní vrátka (Back doors)
Aplikace (popř. vlastnost programu) omezující ochranu počítačové systému s cílem umožnit do něj přístup z jiného počítače. Tento průnik může sloužit jak hackerovi dostat se k našim datům, tak i osobám zajišťujícím servisní služby k počítačové síti (např. IT specialisté určitého pracoviště, programátoři operačního systému Windows apod.).[5,13, 14(p24)]

Prevence

K obraně před útoky crackerů a hackerů je třeba provádět vícero opatření.

Antivirové programy

V současnosti je zcela nezbytné mít na počítači nainstalovaný antivirový program a pravidelně jej aktualizovat. Při koupi nového počítače si před jeho připojením k internetu nainstalujeme antivirový program, po připojení ihned stáhneme jeho aktualizace a až poté pokračujme s instalací dalších programů. V současnosti existuje celá řada antivirových programů, mezi nimiž jsou i produkty dostupné jednotlivci bez poplatku. Je třeba si vždy na webové stránce konkrétního programu přečíst, zdali je produkt k užívání zdarma, a pokud ano, v jakém rozsahu zabezpečí počítač. V současnosti patří mezi nejrozšířenější antivirové programy Avast!, AVG, Norton, Kaspersky, Microsoft Essential, NOD.

Firewall

Rovněž nesmíme zapomínat na zapnutí firewallu. Uživatelé operačního systému Windows si v nastavení zapnou fungování brány, případně mohou využít některý z dostupných firewallů (ZoneAlarm).

Aktualizace systémů a programů

Nezbytné je pravidelně aktualizovat operační systém i programy, které používáme (např. Windows si pravidelně stahují instalace, internetový prohlížeč je průběžně aktualizován formou nových verzí apod.).

Ochrana proti spywaru

Proti spywaru se lze chránit jak různými programy (Spybot Search & Destroy, AdAware SE, AVG Anti-Spyware, Spyware Doctor apod.), tak vlastním chováním, kdy neinstalujeme na počítač programy z neznámých zdrojů, nenavštěvujeme podezřelé a pochybné stránky (např. nabízející nelegální programy apod.).

Bezpečná hesla

Je zcela nezbytné používat dostatečně bezpečná hesla, přičemž každý uživatel počítače by měl mít vlastní zaheslovaný účet, heslo nesmí být jednoduše dostupné (např. umístěné na monitoru), heslo

nikomu jinému nesdělujeme a při běžné práci používáme počítač ve standardním režimu, nikoli jako administrátor.

Chceme-li vytvořit silné heslo, mělo by mít minimálně šest až osm znaků, mezi nimiž jsou velká i malá písmena, číslice a symboly (např. $@}&# apod.). V hesle bychom neměli používat jméno a příjmení nebo uživatelské jméno. Některý ze symbolů je vhodné umístit mezi druhým až šestým znakem.[15,16,17,18]

Jednou z možností, jak si vytvořit silné a zapamatovatelné heslo je použít první znaky z nějakého výroku, přičemž je však třeba takové heslo ještě náležitě upravit, aby bylo maximálně bezpečné. Zdůrazněme, že se musí jednat o výrok, který není obecně známý (např. nesmí jít o větu z knihy, filmu apod.)

Jak vytvořit bezpečné heslo

1.	Vymysli si svou vlastní jedinečnou větu o počtu slov, které má mít výsledné heslo.	V našem domě máme dva kanárky, jeden se jmenuje Honzík a druhý Pepík a oba mají zelenou barvu.
2.	Číslovky nahraď číslicemi.	V našem domě máme 2 kanárky, 1 se jmenuje Honzík a 2 Pepík a oba mají zelenou barvu.
3.	Použij první písmeno z každého slova.	vndm2k1sjha2paomzb
4.	Některá písmena napiš verzálkami (zde dodržíme pravopis).	**V**ndm2k1sj**H**a2**P**aomzb
5.	Nahraď některé písmena nebo číslice symbolem, např. s → $, c → (, i → ! apod. (zde nahradíme a → &, o → 0 a přidáme interpunkci jako ve větě).	Vndm2k**,**1sjH**&**2P**&**omzb.
6.	Nyní již máme dostatečně bezpečné heslo, jehož kvalitu můžeme i prověřit.	Vndm2k,1sjH&2P&omzb.

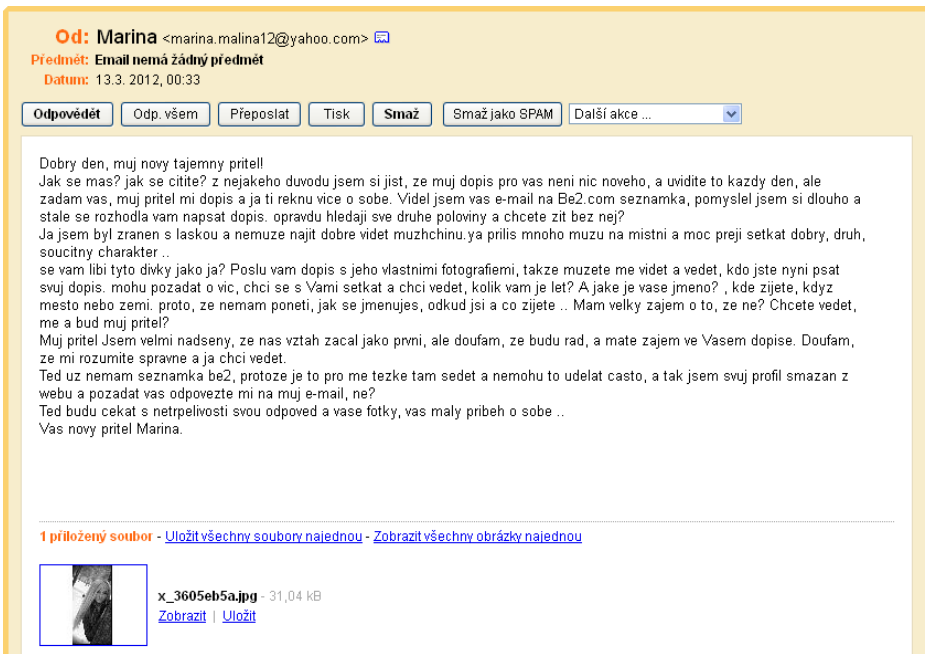
Sociální inženýrství

Zatímco výše uvedené metody proniknutí do počítačového systému souvisejí s jeho ohrožením prostřednictvím nějakého programu nebo nastavení počítače, existují i postupy, jak získat citlivé údaje přímo od konkrétního člověka díky jeho důvěřivosti. Tehdy hovoříme o tzv. **sociálním inženýrství**, [4(p112), 19(p69)] s nímž se v současnosti setkáváme velmi často zvláště v podobě spamu, hoaxu a phishingu.

Spam

Termínem *spam* se označuje zpráva hromadně rozesílaná a vnucovaná prostřednictvím elektronické pošty adresátům, kteří o ni ve skutečnosti nemají zájem. Tyto zprávy obvykle obsahují různá reklamní sdělení, návody na rychlé zbohatnutí a zázračné vyléčení, případně se jedná o řetězové zprávy.

Základním problémem spamu je zatěžování příjemce nechtěnou činností (označování spamů, jejich mazání apod.), finančními náklady na přenos spamů (platby za připojení k internetu, jehož prostřednictvím byl spam doručen), zaplněním poštovní schránky na úkor regulérních zpráv, ale i zbytečným přetěžováním sítí přenášejících data. [4(pp104–105),9, 12(pp64–66),20, 21(pp111–112)]

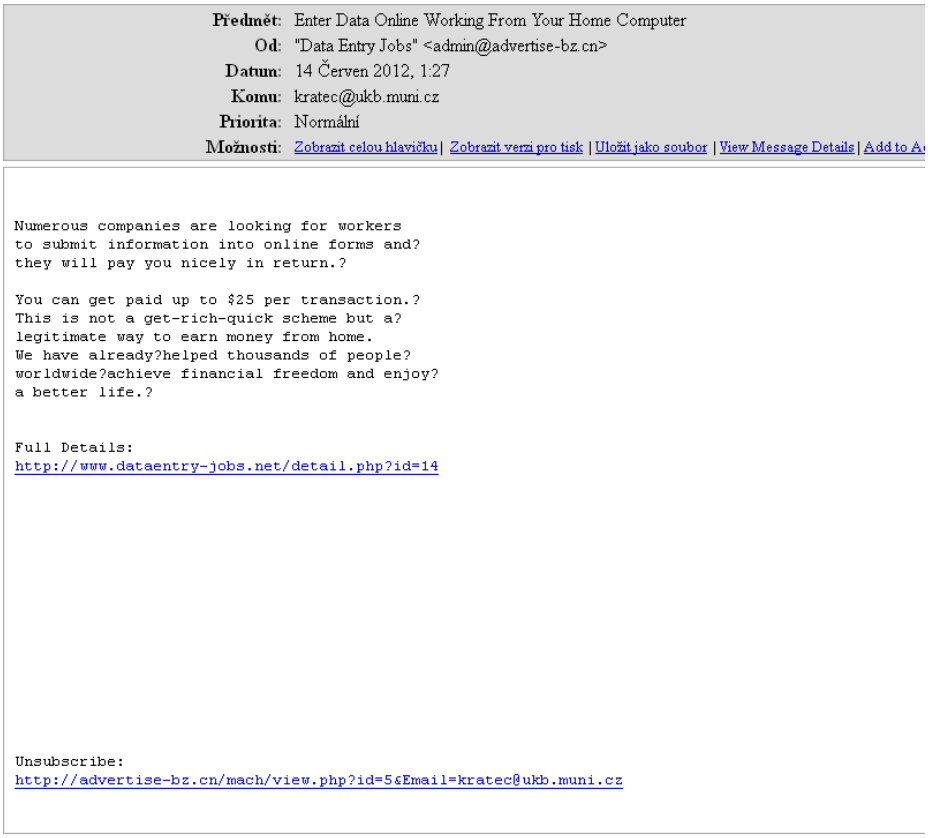


Obrázek 1: Ukázka spamu 1

Předmět: odpovezte
Od: "Dr Kleinwort Benson" <drbenk369@msn.com>
Datum: 11 Červen 2012, 8:18
Priorita: Normální
Možnosti: Zobrazit celou hlavičku | Zobrazit verzi pro tisk | Uložit jako soubor | View Message Details

Dr. Kleinwort Benson
Operace / Regionální manažer Egg Plc bankovnictví,
1Waterhouse námestí 138 až 142 Holborn
Londýn Velká Británie
Reknete: +44 703 188 8977
E-mail: drkleinwortbenson55@hotmail.com
Drahý príteli,
Mé jméno je dr Kleinwort Benson jsem z Harlesden North West England, formální vedoucí projektu a programátor manažer Deutsche Bank, duveryhodný poradce pro více než 20 let av soucasné dobe se provoz / Regionální manažer pobocky manažer Egg Bank London, tady v Anglii. Pracuji pro Nejnovejší ministru Bank v Londýne. Píši Vám po dohode v mé kancelári, která bude mít obrovský prínos pro nás oba. V mém oddelení, jako jsou operace / Regionální manažer pobocky manažer vejce bankovnictví Plc (1Waterhouse námestí 138 až 142 Holborn), jsem zjistil, opuštené cástku ve výši Kc 21,500,000,00 britské Pounds odst. dvacet jedna milionu pet set tisíc britských liber) na úctu , který patrí k jednomu z našich zahranicních zákazníku Pozdní David McDowell Brown americký obcan Arlington Virginie, který bohužel prišel o život pri prvním únoru 2003 pres jižní Spojených státu raketoplánu Columbia, zemrel jako jeden muž Volba Vás kontaktovat se vzbudila z geografické povahy, kde žijete, obzvlášte vzhledem k citlivosti na transakce a duvernost zde.
Nyní náš bankovní bylo cekání na nekterý z príbuzných prijde až k tvrzení, ale nikdo nemá delat. Osobne jsem byl neúspešný pri rozmistování príbuzným po dobu 5 let.
  I nyní usilovat o váš souhlas k vám jako další príbuzný / Bude príjemce, aby zemrelého tak, že výtežek z tohoto úctu ocenen na £ 21, 500, 000, 00 Britská libra muže být vyplacena na vás. To bude vyplacena, nebo sdílená v techto procent, 50% pro me a 40% na vás, zatímco 10% je pro všechny výdaje vzniklé v prubehu transakce, zatímco jsem zajištené veškeré nezbytné právní dokumenty, které mohou být použity pro zálohování toto tvrzení jsme tvorby. Všechno, co potrebujete, je vyplnit vaše jména na dokumenty a legalizovat to u soudu dokázat, jste zde jako oprávnený príjemce. Také jsem se vyžadují vaše uprímná Co-operace, duvernosti a absolutní duvera bezpochyby k tomu, aby nás videt tuto transakci prostrednictvím. Já vám zarucit, že to bude popraven za legitimní usporádání, které bude chránit vás z jakéhokoli porušení zákona. Prosím, uvedte mi následující, jak jsme 5 dní spustíme ji projít.
To je velmi URGENT PROSÍM.1. Celé jméno
2. Jsi Telefon
3. Jsi Kontaktní adresa.
4. PovoláníOdpovezte, prosím, tak i já posílám vás banka formulár k vyplnení okamžite.
S pozdravem,
Dr. Kleinwort
Tel. +44 703 188 8977 Zašlete vaše informace pouze soukromé MY EMAILEM [drkleinwortbenson55@hotmail.com]

Obrázek 2: Ukázka spamu 2



Předmět: Enter Data Online Working From Your Home Computer
Od: "Data Entry Jobs" <admin@advertise-bz.cn>
Datum: 14 Červen 2012, 1:27
Komu: kratec@ukb.muni.cz
Priorita: Normální
Možnosti: Zobrazit celou hlavičku | Zobrazit verzi pro tisk | Uložit jako soubor | View Message Details | Add to A

Numerous companies are looking for workers
to submit information into online forms and?
they will pay you nicely in return.?

You can get paid up to $25 per transaction.?
This is not a get-rich-quick scheme but a?
legitimate way to earn money from home.
We have already?helped thousands of people?
worldwide?achieve financial freedom and enjoy?
a better life.?

Full Details:
http://www.dataentry-jobs.net/detail.php?id=14

Unsubscribe:
http://advertise-bz.cn/mach/view.php?id=5&Email=kratec@ukb.muni.cz

Obrázek 3: Ukázka spamu 3

Preventivní opatření

Snížit riziko přijetí spamů můžeme několika způsoby:[12,20]

- Nezveřejňovat e-mailovou adresu volně na internetu a neregistrovat ji na neznámých a podezřelých stránkách.
- Potřebujete-li e-mailovou adresu na webu zveřejnit, vložte ji na web v podobě obrázku nebo v ní nahraďte symbol @ předložkou *at* (kratec@ukb.muni.cz → kratec [at] ukb.muni.cz).
- Je-li ve spamu tlačítko k odhlášení odběru zpráv (unsubscribe), pamatujte, že může jít o podvrh, kdy po kliknutí namísto odhlášení se přihlásíte k zasílání dalších spamů.
- Pravidelně si aktualizujte operační systém, antivirový program a firewall kvůli odhalení případného napadení virem sloužícímu k zasílání spamu.
- Využívejte e-mailovou poštu toho poskytovatele, který nabízí a pravidelně aktualizuje antispamové filtry.
- V poštovním klientovi označujte spamy, aby si aplikace zapamatovala adresu odesílatele, byla schopna rozpoznat spam na základě podobně znějícího obsahu apod.

Hoax

Rozšířeným prostředkem sociálního inženýrství je šíření tzv. *hoaxů*, jak jsou označovány řetězové zprávy (nejčastěji formou hromadného e-mailu) obsahující nejrůznější informace s cílem vyvolat v příjemci paniku, lítost s něčím osudem apod. Pro tyto zprávy je typické, že obsahují větu navozující dojem, jak je obsažená informace důležitá a že je třeba ji co nejrychlejší předat dalším příjemcům.[9, 12(p72),22]

Příklad hoaxu

```
PROSIM TĚ POMOZ MALÉMU MIMINKU!! A~POŠLI TENTO MAIL HODNĚ LIDEM!!
 Prosím přečti si to!! Neni to žádný otravnýřetězák!!
 A~pošli hodně ale opravdu hodně lidem!!
 Malá holčička na obrázku má rakovinu mozku.
 Společnost AOL za každý odeslaný e-mail daruje 5 centů
 na její operaci.Prosím, pomozte.
```

(převzato z portálu HO@X[23])

Preventivní opatření

- Podívat se na portále HO@X, je-li tam zpráva v doslovném nebo velmi podobném znění evidována. Případně můžeme zadat část zprávy do vyhledávače, např. Google, a budeme překvapeni, na kolika stránkách se již o dané zprávě jako o hoaxu hovoří.
- Kriticky posuzovat logičnost zprávy. Například v souvislosti s výše uvedeným příkladem vystává otázka, jak se společnost AOL dozví, že jsme zprávu poslali dál.
- Ignorovat jakékoliv zprávy vyzývající nás k jejich přeposlání dál a upozornit odesílatele, aby před odesláním podobných zpráv si prověřil jejich pravost a nikomu dál je nezasílal.

Pro zájemce o procvičení se v rozpoznání hoaxu je připraven tento krátký test.

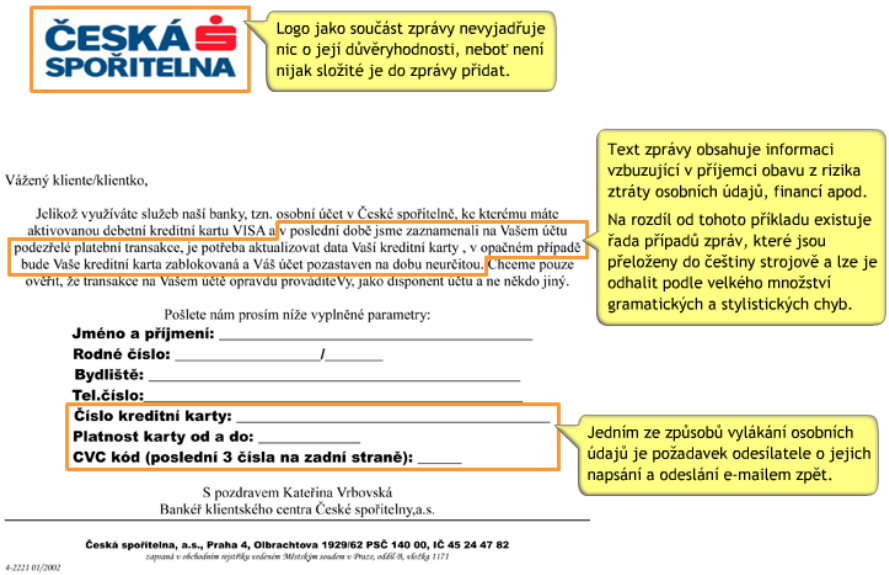
Phishing

V souvislosti s podvodnými zprávami se v současnosti často hovoří o tzv. *phishingu* (čti fišingu), kdy zprávy na rozdíl od hoaxu mají za cíl získat od adresáta nějaké cenné údaje, jako jsou např. heslo k e-mailu, bankovnímu účtu apod. Ať už jde o phishing formou e-mailu nebo podvodné webové stránky, vždy má jedno společné – snaží se v adresátovi vzbudit dojem, že namísto podvodné zprávy se jedná o skutečnou původní zprávu. Tohoto dojmu se dosahuje napodobením designu a obvykle užívaných větných formulací ve zprávách na webových stránkách, e-mailech apod. skutečné organizace. Obvykle tyto zprávy obsahují výzvu ke změně přihlašovacích údajů v důsledku aktualizace softwaru nebo hardwaru příslušné instituce a odkaz na webovou stránku, kde lze tuto změnu provést. [4(pp112–113),24, 25(p33)]

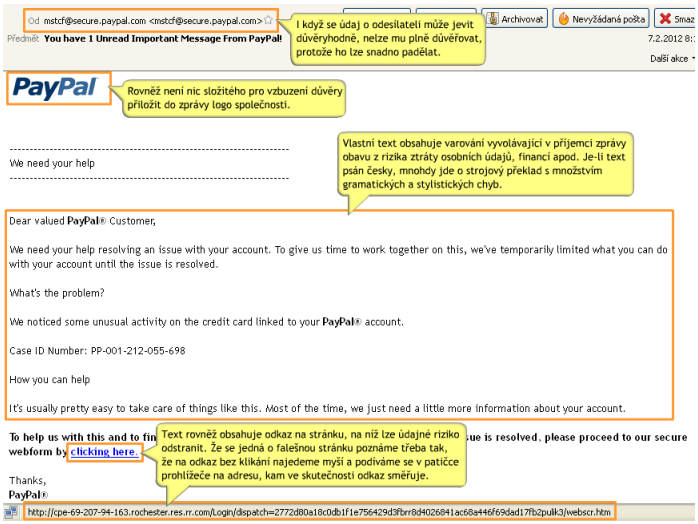
Preventivní opatření

Než si níže ukážeme na konkrétních příkladech phishingových zpráv konkrétní znaky, podle nichž lze odhalit jejich podvodnost, shrňme si základní pravidla prevence:

- Myslet na 3 NE – Nevyplňovat údaje, Neklikat na odkazy, Nestahovat soubory [24(p13)]
- Nikdy nikomu nesdělovat heslo k účtu, PIN platební karty, i kdyby to byl správce sítě.
- Nenechat se vystrašit hrozbami o zrušení účtu, deaktivaci karty apod., pokud nesdělíte ve zprávě požadované údaje.
- Pozorně si všímat formy textu, často se jedná o strojově přeložený text.
- Důkladně se podívat na webovou adresu zprávy, není-li nenápadně změněna, např. *www.amazon.com* → *www.annazon.com.*[26]



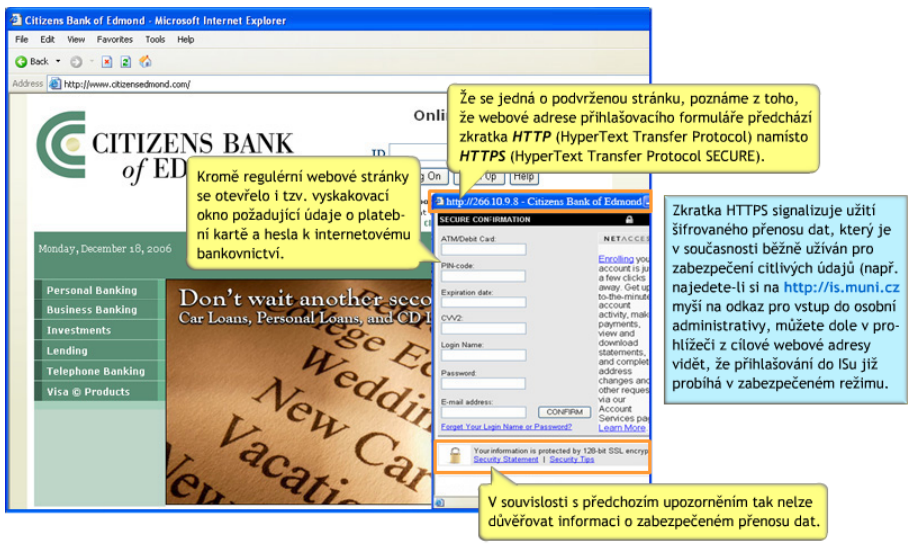
Obrázek 4: Ukázka phishingu 1



Obrázek 5: Ukázka phishingu 2

Pharming

Ještě nebezpečnějším způsobem, jak vylákat z uživatele internetu jeho osobní údaje, je *pharming* spočívající v útoku na DNS server, který překládá webové adresy na IP adresy (např. *www.novinky.cz* na *77.75.76.7*). Při napadení DNS serveru dochází k tomu, že po zadání hledané webové adresy dojde namísto k jejímu překladu na správnou IP adresu na IP adresu podvržené stránky, která svým vzhledem imituje požadovanou stránku nebo obsahuje nepatřičný prvek, jehož prostřednictvím se útočník dostane k osobním údajům uživatele. [4(p113),29]



Obrázek 6: Ukázka pharmingu

Ostatní internetová kriminalita

Kromě výše uvedených způsobů proniknutí do cizího počítačového systému existuje rovněž další druhy internetové kriminality, které mohou vyústit v mravnostní trestný čin, porušování autorského práva, finanční podvody apod. Níže uvádíme tři, s nimiž se může laická veřejnost nejčastěji setkat.

Porušování autorského práva

Snad nejrozšířenějším projevem internetové kriminality je porušování autorského práva, a to především u hudebních, filmových a softwarových produktů. Dochází k němu tehdy, jestliže uživatel internetu bez souhlasu původního autora nebo držitele autorských práv zpřístupnil produkt ostatním osobám. V případě softwaru je porušením autorského práva také prolomení jeho ochrany proti kopírování či úpravám zdrojového kódu. [4(p101), 25(pp41–45)]

Nejčastějším způsobem zpřístupňování uvedených produktů je prostřednictvím p2p (peer-to-peer) sítí a prostřednictvím nejrůznějších úložišť. V případě p2p sítí kromě uživatele sdílejícího soubory produktu, k němuž nevlastní autorská práva, může velice snadno porušovat autorská práva i příjemce souboru. Systém p2p totiž funguje na základě přijímání dat a jejich souběžného sdílení, takže i příjemce souboru se stává tím, kdo data sdílí dál a tedy porušuje autorský zákon. [4(p101), 25(pp43–45),31]

Odlišná situace je v případě FTP/WEB hostingů, kdy porušuje autorský zákon pouze ten, kdo na internetové stránce nebo v některém z úložišť typu *uloz.to*, *rapidshare.com* apod. zpřístupní soubory produktu, k němuž nevlastní autorská práva. [25(pp45–46)] Ačkoliv je představa přístupu ke zmíněným produktům zdarma lákavá, skýtá kromě trestního postihu i další riziko. Zvláště v případě softwaru riskuje uživatel instalací nelegálně získaného softwaru také spuštění některého z virových programů, nejčastěji trojského koně.

V oblasti softwaru existuje v současnosti řada alternativních programů zdarma vůči placeným aplikacím typu Microsoft Office, Adobe Photoshop apod., které představujeme v tutoriálu *GNU licence a software*. V neposlední řadě pro studenty existují různé slevové programy, v rámci nichž lze levněji než v obchodech pořídit i zmíněné programy, např. http://www.studentskelicence.cz a http://www.digitalmedia.cz/licence/adobe/edu/student.aspx.

Doménové pirátství

K internetové kriminalitě patří tzv. *cybersquatting*, jak se označuje postup spekulantů, kteří si zaregistrují doménu (webovou adresu) znějící podobně jako již existující zavedená doména nebo doménu, u níž původní majitel zapomněl zajistit její prodloužení. Cílem tohoto jejich jednání je obohatit se na úkor zavedených firem buď ziskem z reklam umístěných na stránkách s podobnou adresou, které uživatel internetu navštíví při nechtěném překlepu v adrese nebo prodejem registrace adresy oné zavedené společnosti. [4(p107), 25(pp39–41)]

V minulosti se odehrála řada případů, kdy zmínění spekulanti se na prodeji zaregistrované lukrativní domény obohatili o částky v řádech statisíců korun i dolarů.

Například České dráhy zaplatili 175 000 Kč za doménu *cd.cz*, doména *fish.com* byla prodána za 1 020 000 dolarů, *earth.com* za 800 000 dolarů apod.[32]

O závažnosti této trestné činnosti svědčí i řada soudních sporů, které se v minulosti uskutečnily v tuzemsku i zahraničí.

V českém prostředí je známý například spor České pojišťovny, ve kterém se soud přiklonil na stranu žalobce zvláště po zjištění, že spekulant si zaregistroval doménu *www.ceskapojistovna.cz*, aniž by na ní provozoval internetové stránky.[33]

Řada soudních sporů je vedena i v zahraničí, o řadě z nich se lze dočíst na webu http://www.traverselegal.com.

Kyberšikana

Obecně se za *šikanu* považuje jakékoliv chování vedoucí k *„ubližování někomu, kdo se nemůže nebo nedovede bránit.“* [34(p21)] Hlavní rozdíl mezi šikanou a kyberšikanou spočívá ve vztahu mezi agresorem a obětí, kdy při šikaně je mezi nimi *„osobní asymetrický vztah moci“* spočívající v tom, že oba účastníci šikany se vzájemně znají, [34(p21),35] zatímco při kyberšikaně tento vztah obvykle chybí. [34(p24),35, 36(p5)] Při kyberšikaně tak nemusí docházet k nadřazenému vztahu agresora vůči šikanovanému, na němž si *„demonstruje svou moc a převahu“*, [34(p24)] neboť agresor může zůstat skryt a šikanovat jinou osobu na dálku, a to prostřednictvím komunikačních technologií. [34(p24),35, 36(p3), 37(p67)]

Ve svých důsledcích je kyberšikana o to nebezpečnější, že internet skýtá agresorovi nejen anonymitu, ale bezkontaktním vztahem s šikanovaným mu ubírá na zábranách, které by jinak měl při pozorování reakce ublížené osoby. V neposlední řadě nebezpečí kybešikany spočívá i v tom, že agresorem zveřejněná informace je zpřístupněna (a může být dlouhodobě zpřístupněna) prostřednictvím internetu velkému množství ostatních osob. [37(p64)]

Projevy kyberšikany mohou být nejrůznější a patří mezi ně: [36(pp15–20),38, 39(pp41–42),35]

- zasílání výhružných a ponižujících textových či audiovizuálních informací prostřednictvím SMS, MMS a e-mailu,
- zveřejnění výše uvedených informací na webové stránce, blogu, Facebooku apod.,
- zasílání zpráv obsahujících některý z typů mallwaru oběti,
- zneužití osobních údajů oběti (např. i přihlašovací údaje k internetovým komunikačním kanálům) s cílem ji poškodit, zesměšnit apod.,
- vyvěšení upravených fotografií (např. přidání obličeje oběti na pornografický obrázek),
- zveřejnění konverzace bez souhlasu komunikujících,
- fotografování a nahrávání oběti s cílem poškodit oběť rozšířením pořízených záběrů,
- opakované obtěžování oběti telefonáty, e-maily apod.,
- vyloučení oběti z virtuální komunity.

Z uvedených projevů kyberšikany vyplývá, že velmi snadno se můžeme stát tím, kdo se na kyberšikaně podílí. V běžném životě si mnohdy neuvědomujeme, že vyfotografováním někoho a vyvěšením takové fotografie např. na Facebooku s ponižujícím komentářem, můžeme dotyčné osobě ublížit.

V nedávné minulosti se odehrála řada případů, kdy v souvislosti s kyberšikanou oběti došli nejen psychické, ale i zdravotní újmě včetně úmrtí.

Například v roce 2003 se Patrick Ryan Halligan, 14letý americký školák, oběsil poté, co jej spolužáci nejdříve ve škole šikanovali rozšiřováním lživé zprávy o jeho homosexuální orientaci, aby jej s pomocí jedné spolužačky přiměli v online komunikaci prozradit jí intimní informace, které pak šířili mezi ostatní studenty. [36(pp28–31)]

O tři roky později byla podobné šikaně vystavena i Megan Taylor Meierová, rovněž 14letá školačka, která se doma ve skříni oběsila poté, co jí na zeď sociální sítě MySpace.com začaly její bývalá kamarádka se svou matkou vkládat urážlivé výroky k její postavě a nenávistné zprávy. [36(pp34–36)]

Jako demonstraci skutečnosti, že obětí kyberšikany nemusejí být pouze děti a mládež, jako tomu bylo v předešlých příkladech, vzpomeňme na případ Mary Shielerové, která v roce 2006 pod identitou své dcery navázala online vztah s dvěma muži, z nichž jeden – bývalý americký voják Thomas Montgomery – po odhalení pravdy zavraždil svého soka. Případ byl o to otřesnější, že Mary Shielerová navíc bez vědomí dcery zasílala oběma mužům dívčiny fotografie, a to i např. v plavkách, či její spodní prádlo.[40,41] Doplňme, že případ natolik ohromil americkou veřejnost, že byl v roce 2009 podle něj natočen dokumentární snímek *talhotblond*:.[42,43]

Preventivní opatření

- Respektováním ostatních uživatelů nedáváme záminku, aby nám ubližovali.
- V komunikaci s anonymními uživateli jsme maximálně obezřetní a nesdělujeme jim žádné důvěrné informace o sobě ani o ostatních, neposíláme jim žádné fotografie, videa apod.
- Seznámením se s pravidly užívání příslušného komunikačního kanálu zjistíme, co si lze v daném prostředí dovolit a s kým řešit případné něčí nevhodné chování.
- Agresora od jeho počínání neodrazujeme, ani se mu nemstíme, ale přestaneme s ním komunikovat.
- Je-li to možné, zablokujeme útočníkovi přístup k našemu účtu (např. nastavíme filtr pro automatické mazání zpráv od agresora) nebo telefonnímu číslu (zablokujeme si příjem agresorových zpráv a hovorů).
- Myslíme-li si, že jsme se stali obětí kyberšikany, poradíme se s někým, k němuž máme důvěru (např. rodiče), aby s odstupem posoudil, nakolik je problém závažný a je-li třeba se obrátit na policii, požádat o pomoc psychologa apod.
- Zaznamenáme-li v okolí kyberšikanu, snažíme se jí zabránit (pomůžeme šikanovanému, dáme agresorovi na srozuměnou, že s jeho počínáním nesouhlasíme apod.)

4 Závěr

Představili jsme si pravidla netikety a některé z projevů internetové a počítačové kriminality. Je třeba zdůraznit, že výše uvedený text je pouze obecný nástin jinak složité problematiky, které se v současnosti věnují jak počítačoví experti, tak i právnická odborná veřejnost. Proto zájemcům o bližší seznámení s výše nastíněnými tématy doporučujeme ke studiu jak literaturu použitou pro vznik tohoto materiálu, tak i níže uvedené internetové stránky. Zejména doporučujeme sledovat univerzitní novinky z oblasti bezpečnosti na internetu, které naleznete na adrese https://security.ics.muni.cz/.

Užitečné odkazy

- http://www.svetsiti.cz/Tutorialy.asp
- http://www.bezpecnyinternet.cz/
- http://www.e-bezpeci.cz/
- http://www.saferinternet.cz/

5 Použité zdroje

[1] Hambridge S. *Netiquette Guidelines*. 1995. Available at: http://tools.ietf.org/pdf/rfc1855. Accessed April 6, 2012.

[2] Shea V. *Netiquette*. San Francisco: Albion Books; 1994.

[3] Musil J. Elektronická média v informační společnosti. *Obrana a strategie*. 2006;2006(2). Available at: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=6513. Accessed April 11, 2012.

[4] Jirovský V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada; 2007.

[5] Jirovský V, Hník V, Krulík O. *Základní definice, vztahující se k tématu kybernetických hrozeb*. 2008. Available at: http://aplikace.mvcr.cz/archiv2008/bezpecnost/informacni/zakladni_info.pdf. Accessed April 11, 2012.

[6] Gřivna T, Polčák R eds. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium; 2008.

[7] Denning DE. Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy. In: Arquilla J, Ronfeldt D, eds. *Networks and Netwars: The Future of Terror, Crime and Militancy*. Santa Monica, CA: RAND; 2001:239–288.

[8] Janoušek M. Kyberterorismus: terorismus informační společnosti - Obrana a strategie. *Obrana a strategie*. 2006;2006(2):60–66. Available at: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=6513. Accessed April 11, 2012.

[9] Paukertová V. Elektronická informační kriminalita. *Ikaros*. 2006;10(8). Available at: http://www.ikaros.cz/elektronicka-informacni-kriminalita. Accessed April 11, 2012.

[10] Salomon D. *Elements of Computer Security*. London: Springer; 2010. Available at: http://www.springerlink.com/content/978-0-85729-005-2/#section=746943&page=1&locus=0. Accessed May 15, 2012.

[11] Aycock J. *Spyware and Adware*. New York: Springer; 2011. Available at: http://www.springerlink.com/content/978-0-387-77740-5/#section=778260&page=9&locus=14. Accessed April 11, 2012.

[12] Čandík M. *Základy informační bezpečnosti*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně; 2004.

[13] Říha P, Klaška L. Slovník počítačové informatiky a sítí. *Svět sítí: informace ze světa počítačových sítí*. 2012. Available at: http://www.svetsiti.cz/slovnik.asp. Accessed May 15, 2012.

[14] Bičianová A. *Kybernetický terorizmus a počítačová kriminalita*. 2008. Available at: http://dspace.k.utb.cz/bitstream/handle/10563/5482/bi%c4%8dianov%c3%a1_2008_dp.pdf?sequence=1. Accessed May 16, 2012.

[15] Microsoft. Creating strong passwords. *Microsoft Windows XP - Creating passwords*. 2012. Available at: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/windows_password_tips.mspx?mfr=true. Accessed June 26, 2012.

[16] Microsoft. Create strong passwords. *Change Passwords — Create Strong Passwords — Microsoft Security*. 2012. Available at: http://www.microsoft.com/en-gb/security/online-privacy/passwords-create.aspx. Accessed June 26, 2012.

[17] Anon. Vytvoření silného hesla a jeho vlastnosti. *Bezpečný internet*. Available at: http://www.bezpecnyinternet.cz/zacatecnik/hesla/vytvoreni-silneho-hesla.aspx. Accessed June 27, 2012.

[18] Dallas County Community College District. Password Dos and Don'ts. *Dallas County Community College District*. 2012. Available at: http://www.dcccd.edu/Emp/Policy%20and%20Procedures/IPSP/Security%20Procedures/Passwords/Pages/DoandDont.aspx. Accessed June 27, 2012.

[19] Hoeschele M, Rogers M. Detecting Social Engineering. In: Pollitt M, Shenoi S, eds. *Advances in Digital Forensics*. Vol 194. IFIP International Federation for Information Processing. Springer Boston; 2005:67–77. Available at: http://www.springerlink.com/content/26l1038701179u41/abstract/. Accessed May 31, 2012.

[20] Anon. Spam. *Bezpečný internet*. Available at: http://www.bezpecnyinternet.cz/zacatecnik/e-mail/spam.aspx?kurz=true. Accessed June 19, 2012.

[21] Poláková E. *Mediálne kompetencie: Úvod do problematiky mediálnych kompetencií*. Vranov nad Topľou: Elibrol; 2011. Available at: http://www.medialnavychova.sk/wp-content/uploads/Medi%C3%A1lne_kompetencie_Polakova_Eva_2011.pdf. Accessed June 19, 2012.

[22] Džubák J. Co je hoax. *Hoax: podvodné a řetězové e-maily, poplašné zprávy, phishing, scam.* 2012. Available at: http://hoax.cz/hoax/co-je-to-hoax. Accessed June 19, 2012.

[23] Džubák J. Miminko s rakovinou mozku a peníze od AOL. *Hoax: podvodné a řetězové e-maily, poplašné zprávy, phishing, scam.* 2012. Available at: http://www.hoax.cz/hoax/miminko-s-rakovinou-mozku-a-penize-od-aol/. Accessed May 31, 2012.

[24] Soukal J. *Nebezpečí na Internetu*. 2011. Available at: https://security.ics.muni.cz/public/edu/bit/Nebezpeci_na_internetu_Jan_Soukal_2011.pdf. Accessed April 4, 2012.

[25] Jangl M. *Počítačová kriminalita*. 2007. Available at: http://is.muni.cz/th/81532/pravf_m/DP_pocitacova_kriminalita.pdf. Accessed April 4, 2012.

[26] APWG. *Welcome to APWG & CMU's Phishing Education Landing Page*. Available at: http://education.apwg.org/r/. Accessed June 8, 2012.

[27] Česká spořitelna. *Ukázky phishingových e-mailů - Česká spořitelna*. 2012. Available at: http://www.csas.cz/static_internet/cs/Komunikace/Phishing/Phishing_ukazky/Prilohy/120221_phishing_ii.pdf. Accessed June 8, 2012.

[28] OneMoreExploit. *How Hackers Steal Facebook Passwords*. 2009. Available at: http://www.youtube.com/watch?v=zBZrynmd7cU. Accessed June 8, 2012.

[29] Brody RG, Mulig E, Kimball V. Phishing, Pharming and Identity Theft. *Academy of Accounting and Financial Studies Journal*. 2007;11(3):43–56.

[30] Ctrust Network. *Real-life examples for pharming Scams*. Available at: http://images.ctrustnetwork.com/static_pages/scams/pharming_scams/pharming_scam_example.jpg. Accessed June 11, 2012.

[31] IFPI. Právní aspekty P2P. *IFPI*. Available at: http://www.ifpicr.cz/?rubrika=1141. Accessed June 20, 2012.

[32] Komárová L. Cybersquatting? červená spekulantům! (1.díl). *Právo IT*. 2007. Available at: http://www.pravoit.cz/article/cybersquatting-cervena-spekulantum-1-dil. Accessed June 20, 2012.

[33] Komárová L. Cybersquatting? červená spekulantům! (2.díl). *Právo IT*. 2007. Available at: http://www.pravoit.cz/article/cybersquatting-?-cervena-spekulantum-2-dil. Accessed June 20, 2012.

[34] Říčan P, Janošová P. *Jak na šikanu*. Vyd. 1. Praha: Grada; 2010.

[35] Malíková B. Kyberšikana. *Pedagogicko-psychologické poradenství*. 2008;(54):28–36.

[36] Krejčí V. *Kyberšikana: kybernetická šikana*. Olomouc; 2010. Available at: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=14%3Akybersikana-studie. Accessed June 20, 2012.

[37] Kovářová P. *Ohrožení dětí na internetu: teorie a doporučení pro vzdělávání*. 2011. Available at: http://is.muni.cz/th/136790/ff_r/Rigo_Kovarova.pdf. Accessed June 20, 2012.

[38] WireKids. STOP cyberbullying: Direct attacks. *STOP cyberbullying*. Available at: http://www.stopcyberbullying.org/how_it_works/direct_attacks.html#im. Accessed June 20, 2012.

[39] Ondrůšková Z. *Proměny a specifické rysy komunikace v prostředí internetu*. 2010. Available at: http://dspace.k.utb.cz/handle/10563/12468. Accessed June 21, 2012.

[40] Staba D. A Pretend Web Romance, Then a Real-Life Murder. *The New York Times*. Available at: http://www.nytimes.com/2007/01/07/nyregion/07triangle.html. Published January 7, 2007. Accessed March 22, 2012.

[41] Avila J, Martz G, Napolitano J. Online Love Triangle, Deception End in Murder. *ABC News*. 2011. Available at: http://abcnews.go.com/US/online-love-triangle-deception-end-murder/story?id=14371076#.T2rTktlGaao. Accessed March 22, 2012.

[42] Anon. *Talhotblond: everybody lies online*. 2009. Available at: http://www.talhotblond.com/. Accessed June 21, 2012.

[43] IMDb. *Talhotblond*. 2009. Available at: http://www.imdb.com/title/tt1370889/. Accessed March 22, 2012.