Vanja Korać,
Matematički institut SANU

004.773.3.056

SPAM

ABSTRAKT

U ovom tekstu će biti obrađen pojam SPAM-a, šta email poruku čini spam-om, a šta ne, kako izbeći slanje i primanje spam poruka, zašto firme koriste ovakve vrste poruka i zašto napadači koriste ovakve tehnike. Kako spameri dolaze do email adresa i načini zaštite od spam napadača.

Ključne reči: Spam, direktni marketing, hakeri, virusi, antispam, antivirusi, CAN, antispam filteri, filteri.

1. ŠTA JE SPAM ?

Značenje reči „**SPAM**“ potiče iz Sjedinjenih Američkih Država [1]. U vreme II svetskog rata među USA vojnicima najomraženiji artikal u sledovanju hrane bila je konzerva sa šunkom, marke „**SPAM“**. Vremenom je uzrečica spam ušla u sleng kao nešto veoma lošeg kvaliteta, neupotrebljivo i krajnje nepoželjno. U Engleskom jeziku reči kao što su *annoyance, harassment* ili u Nemačkom jeziku reč *Belaestigung* koriste se kao epiteti spam-a. U našem rečniku su prevodi nekako previše blagi – dosađivanje ili uznemiravanje. Oko porekla fenomena spam je bilo mnogo debate.

Za sve ljubitelje britanske komedijaške grupe MONTHY PYTHON ovo poreklo reči je nedvosmisleno, jedino tačno pošto se većina njih seća njihovih izvanrednih skečeva.

Naime, Monthy Pytonsi su na indirektan način odgovorni za modernu upotrebu reči spam. Mnogo godina pre pojave spam-a, oni su izveli jedan skeč, čija se radnja odigravala u jednom malom kafeu, gde su dva gosta upitala šta se može dobiti za doručak:

„Konobarica: *Well, there's egg and bacon; egg, sausage and bacon; egg and spam; egg, bacon and spam; egg, bacon, sausage and spam; spam, bacon, sausage and spam; spam, egg, spam, spam, bacon and spam; spam, sausage, spam, spam, spam, bacon, spam, tomato and spam; spam, spam, spam, egg and spam*; (A u pozadini počinju da pevaju sa neba pali Vikinzi .... spam, spam, spam, spam, spam, spam, baked beans, spam, spam, spam and spam. “

Reč spam je bila pomenuta otprilike 85 puta u ovom kratkom skeču. Sad možete i sami da zaključite zašto je nekom palo na pamet da e-mailove, koji su smeće po značenju i ponavljanju, nazovu "**SPAM"**.

Spam je nezatraženi (komercijalni) e-mail ***(unsolicited commercial e-mail)*** koji u najblažem

slučaju može da izazove nerviranje kao nematerijalnu štetu, a u gorim slučajevima može da izazove i materijalnu štetu [2]. Može takođe i da se smatra da je spam distribucija nezatraženih e-mail poruka putem, elektronske pošte ili news grupa. Čak iako e-mail koji primimo ne traži od nas bilo kakvu intervenciju (recimo, obaveštenje o „novootkrivenom virusu" i sl.), ipak je u pitanju nezatražena poruka. Za njeno preuzimanje potrošićemo vreme na Internetu, da bi smo je nakon toga obrisali jer nas sadržaj takvog mail-a ne interesuje.

U stvari on predstavlja svaku email poruku koju korisnik dobije, a koja nema direktne ili indirektne veze sa njim. Pod direktnim vezama se podrazumevaju osobe i firme (servisi) sa kojima korisnik komunicira. Pod indirektnim vezama se podrazumevaju osobe i firme (servisi) koje se pozivaju na direktne veze (gde direktne veze mogu potvrditi da su prosledile email adresu drugoj osobi, firmi ili servisu). Jednostavnije rečeno, svaka pošta koja nema razloga da se pojavi u našem mail inbox-u (elektronskom poštanskom sandučetu) za korisnika predstavlja spam. SPAM ima i druga imena kao sto su „*junk mail"*, zatim „*scam"* kao spam sa "prljavim" sadržajem, dok su *bulk mail* i *bomb mail* podvrste koje označavaju onaj spam koji se na prvom mestu ističe svojom veličinom a zatim učestalošću – najčešće su nastale sa namerom da se ugrozi radna sposobnost primaoca. Kada su komercijalnog karaktera, onda se poruke šalju kao rafal kod kojeg barem jedna poruka treba da prođe kroz zaštitu od spama i pogodi korisnikov mailbox.

2. KO SU SPAM-ERI?

Globalno posmatrajući, prema izveštaju CipherTrust Spam Statistics **[3]** aktuelni podaci slanja spama po zemljama (tablela 1.) izgledaju ovako :

SAD:	56.77 %
Južna Koreja:	16.67 %
Kina i Hong Kong:	5.38 %
Kanada:	4.24 %
Brazil:	0.97 %
Japan:	1.41 %
Francuska:	2.29 %
Španija:	1.79 %
Velika Britanija:	1.17 %
Nemačka:	0.68 %
Tajvan:	1.0 %
Meksiko:	0.89 %
Ostali :	6.74

Tabela 1. *Statistika slanja spama*

Prema ovim istraživanjima interesantino je i to da su 62 % svih e-mail poruka spam poruke! U januaru 2001. godine, ovaj udeo je bio 8%. Zahvaljujući tome što većina firmi i organizacija nema potrebnu zaštitu, moguće je da se ovaj trend rasta nastavi.

Sistemi za slanje spama su jednostavni, usavršavaju se kao i metodi njihovog upravljanja, tako da je već sada moguće da pojedinac pošalje preko 200.000 spam poruka dnevno. Količina spama koja je dnevno bila prisutna u svetu izražene u milionima :

U Januaru: 2002 godine – 3 miliona,

U Januaru: 2003 godine – 6 miliona

U Januaru: 2004 godine – 11 miliona

U Januaru: 2005 godine – 20 miliona

Kao što vidimo broj spam poruka se svake godine udvostručuje.

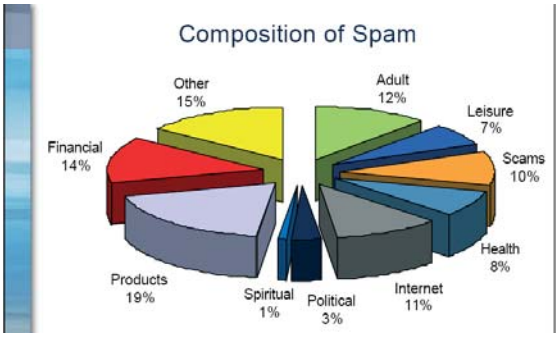
Čak iako SAD šalju daleko najveću količinu spama (na dan 01.07.2005 procenat spam mailova u SAD-u je iznosio rekordnih 85% od svih poslatih mailova u SAD-u prema izvoru CBS news

[4], Evropa ipak šalje milione spam poruka dnevno. Radi se dakle o stotinama miliona poruka u čitavom svetu.

Firma Sophos[1] koja je radila analize nad stotinama hiljada spam poruka, koristeći različite metode kaže da velika količina spam-a potiče i iz Rusije, iako ova zemlja leži na 28 mestu po spamu. Hakeri iz te zemlje, po njima, provaljuju u kompjutere iz drugih zemalja i šalju preko tih računara putem trojanaca i crva "inficiranih" PC-ova čak i 30% ukupnih spam poruka! [5]. Nije malo verovatno pa smo i sami nekome poslali spam ili inficirani mail, a da toga nismo ni svesni.

Tu se nameće pitanje ko je odgovorniji: počinilac ili nalogodavac?

Ako se pogledaju sadržaji spam poruka, onda ćemo jednostavno doći do zaključka koje firme/organizacije su odgovorne za spam. Statističkim obuhvatanjem se dobio udeo delatnosti koje se služe spam-om kao marketinškom metodom kao što se vidi sa slike 1.



Slika 1. *Sadržaji spam poruka*

Izvršioci su (pored kriminalnih organizacija i pojedinaca) uglavnom direkt-marketing firme.

Direkt marketing je područje marketinga, koje je postojalo i pre interneta. Zapravo to je obraćanje pojednincu putem „direktno na njega" adresirane reklame. Pre upotrebe e-maila, sastojao se slanjem pisma ili faksa na određene **izabrane** adrese ili naravno **direktnim** telefonskim pozivom.

Upravo zbog toga je i donet zakon u SAD i EU kojim se striktno zabranjuje slanje **svake** reklame faksom. U slučaju tele-marketinga (kada nas neko manje-više nasumice nazove i hoće nešto da nam proda), koji predstavlja još veće uznemiravanje, zakoni su skoro isto toliko striktni, ali ih se telemarketeri veoma retko pridržavaju.

Znači za razliku od javnih reklama koje se obraćaju masama, u ovom slučaju se poruke šalju ciljnim grupama ljudi koje bi trebalo (po raznim kriterijumima) da su zainteresovani za proizvod/uslugu koja se reklamira. Ovaj dirktan pristup ciljnim grupama je naravno daleko jeftiniji što se tiče troškova transporta poruke nego obraćanje čitavom narodu/populaciji jedne geografske celine pojedinačno.

Na ovom mestu dolazimo do onog što je najvažnije u poslu zvani direct marketing – **adrese**!

Evo jednog ilustatrativnog primera: zamislite da ste prodavac nove zamene za kravlje mleko (namenjeno deci koja ne podnose životinjsko mleko – relativno mala grupa ljudi...) i da želite, naravno, da svako ko je njegov potencijalni potrošač sazna za Vas i Vaš proizvod. Slanje reklamnih prospekata poštom na sve stanovnike države bi Vas odvelo u stečaj, sve i kad bi vas svi oni kojima je potreban taj proizvod neizmerno zavoleli i postali verni kupci.

Vi želite da odštampate (samo za njih) oko 5000 prospekata (uz to eventualno i malu probnu kesicu), investirate u još toliko frankiranih koverti (ukupna suma je X) i na taj način bolje prođete sa troškovima u odnosu na bilo koju reklamnu kampanju sa istim efektom.

Verovatno postoji osoba koja radi pri zdravstvu i koja Vam može pribaviti te adrese, iako je prosleđivanje ovakvih podataka zabranjeno.

Naravno, otkada je zakona, oni se i krše, naročito ukoliko je ponuda za kršenje veoma primamljiva. U ovom slučaju bi promućurnom trgovcu te adrese bile mnogo vrednije od iznosa X.

Moderni spam-eri se na žalost sve manje koriste prosečnim metodama direktnog marketinga (u nekim slučajevima i metode zvane CRM marketing),[2] ali budite uvereni da će

1. http://www.**sophos**.com/

2. CRM-Consumer Relationship Management (uprav-

Vas nakon redovnog posećivanja sajtova sa zabranjenim sadržajem, i naročito nakon unosa svojih podataka na njima, sigurno obradovati reklama za Vijagru ili slično. A broj tih poruka će se povećavati u raznovrsnosti i broju.

Na žalost, ni Internet puritanstvo Vas neće spasiti od spam-a. Ima nekoliko razloga zbog kojih je pitanje spam-a veoma problematično: Ako je korisnikova email adresa bilo gde javno istaknuta (liste i pretraživači E-mail adresa - White Pages, liste korisnika provider-a itd.), onda se može podrazumevati da onaj ko vidi tu adresu može i da je koristi. Isto tako, na osnovu Web adresa (URL-ova) može se pretpostaviti kako glasi email adresa. Na kraju dovoljno je da za Vašu adresu zna neko osim Vas i da je iskoristi.

Generalno posmatrano spam poruke možemo podeliti u nekoliko vrsta [6]:

1. Pravi spam – predstavljaju mailove koje neko konstantno šalje bez mogućnosti uticaja korisnika da ta pošta prestane. Određena populacija na Internetu šalje milione ovakvih poruka da bi isključila (ugušila) određeno mesto (čvor - node) na Internetu iz upotrebe. Ponekad je u pitanju čista obest pošiljioca poruke, koji pronađe žrtvu, pa je bombarduje različitim sadržajima. Ovakvih primera ima puno, a zajedničko za sve njih je da primalac poruke ne može da utiče na prestanak stizanja poruka. Ovo je globalno najozbiljniji spam problem.

2. Latentni (prikriveni-pritajeni) spam - ovo su poruke koje šalju osobe i firme (servisi) i koje na svom početku (ili kraju) imaju informaciju kako da korisnik prestane da ih dobija. Ovim se pošiljaoci ograđuju, nudeći korisniku mogućnost da se odjavi sa liste slanja. Obično na početku ovakvih poruka stoji rečenica "This is not spam" (ovo nije spam). Ova vrsta poruka je najučestalija na email servisima Interneta i predmet je polemika da li jeste ili nije spam.

3. Poruke o postojanju nekog (uglavnom email) virusa - ovakve poruke same po sebi predstavljaju jednu vrstu virusa i spam. I veliki broj ljudi bar jednom nasedne na jednu od njih. Razlog zbog čega ove poruke predstavljaju neku vrstu virusa jeste geometrijska progresija i brzina kojom se šire, i time ovakve poruke utiču na već veliku zagušenost u Internet saobraćaju. U ovu kategoriju spadaju i poruke tipa "*Iz xxx razloga, pošaljite ovu poruku na xxx (što više) adresa i desiće vam se (ili neće vam se desiti) xxx*".

4. Poruke o brzoj zaradi - ovakve poruke, uglavnom, stižu bez naše volje, a primamljivi sadržaji naivne primaoce uspevaju da ubede u njihovu navodnu logičnost i istinitost. Iz ove grupe se izuzimaju "**Opt-in"** poruke. Kada se desi da korisnik dobije poruku koja u sebi sadrži informaciju (email adresu) o tome kome je još poslata ista poruka (CC: - Carbon Copy), ovo može značiti da svako ko je dobio ovu poruku može da upotrebi te adrese, ako hoće. Zato se preporučuje rad sa BCC: - Blind Carbon Copy, ili sa kopijama gde primaoci ne vide adrese onih kojima je poruka jos poslata.

SPAM se toliko infiltrirao u Internet komunikacije da priznati stručnjaci iz ove oblasti (npr. Matt Rosoff, http//www.cnet.com) često poistovećuju spam sa direktnim marketingom. Glavna razlika između ova dva pojma jeste u tome što direktan marketing predstavlja reklamiranje koje je namenjeno ciljnoj populaciji korisnika, nasuprot što većoj neciljnoj populaciji kojom se služe tvorci spam poruka.

Kako se dolazi do email adresa? Smatra se da postoji više načina da se stigne do nečije adrese npr.: javno isticanje email adrese, Use-net pošta, mailing liste, web strane, web papir i formulari, ident deamon, web browseri, finger deamon, irc i chat sobe, whois, pogađanje, razne žute, bele strane i direktorijumi, pristup na istom računaru, neko pre je imao istu adresu, kupovina adresa, socijalni inženjering, hakerisanje.

ljanje na osnovu veza /odnosa/ s korisnicima.

2.1 JAVNO ISTICANJE E-MAIL ADRESE

Svi korisnici koji se odluče da postave negde svoju e-mail adresu trebalo bi da budu upoznati sa negativnim posledicama ove, inače pozitivne akcije (pronalaženje prijatelja rođaka...). Obično se dešava da vlasnik e-mail adrese ne razmišlja o ovome kada postavlja ili daje svoju e-mail adresu na neki servis ili adresu gde će njegova adresa biti dostupna bilo kome (primer - liste korisnika provider-a, White Pages - pretraživači e-mail adresa). Rešenje za ovaj problem predstavlja otvaranje nove adrese za koju će znati samo ljudi koji direktno komuniciraju sa vlasnikom te e-mail adrese. Ovo je povezano sa otvaranjem novog e-mail naloga kod provajdera, bilo da je u pitanju provajder pristupa na Internet ili provajder prostora na Webu.

S druge strane, rešenje predstavlja obaveštenje korisniku od strane provajdera da ako želi privatan i javni pristup svojoj e-mail adresi mora imati minimalno dve e-mail adrese. Jedan od načina prevazilaženja ovog problema jeste uzimanje besplatne e-mail adrese na nekom od postojećih servisa (HotMail, Yahoo, Gmail).[3]

Kroz razumevanje o tome kako spam-eri dolaze do adresa možete doprineti u velikoj meri izbegavanju neželjenih poruka.

2.2 USENET POŠTA

Usenet servis predstavlja najveći izazov za spam-ere zato što je lako pristupačan i prividno se manje kontroliše od komunikacije na mailing listama [5]. U avgustu 1997. grupa sistemskih administratora iz Američke države New Jercey je blokirala sve Usenet poruke ISP-a UUNet. Ovom prilikom tokom Anti-SPAM protesta bilo je blokirano na desetine hiljada poruka u roku od nekoliko dana koliko je protest trajao.

SPAM-eri regularno skeniraju (pregledaju) UseNet u potrazi za email adresama,[4] koristeći se specijalnim programima za tu svrhu. Neki programi jednostavno gledaju u heder-e članaka koji sadrže email adrese korisnika (From: , Reply-to:, itd.) dok drugi idu korak dalje i pretražuju tekst članka po blokovima koji sadrže znak @. Čak i email adrese koje sadrže šifrovane adrese kao što je m2o5j3a6a9d3r8e9s6a@p4t5t.com (koje oprezni korisnici namerno koriste sa naznakom da svako ko želi da pošalje mail autoru, treba da izbaci brojeve iz adrese dobivajući pravu adresu - mojaadresa@ptt.com) bivaju dešifrovane od strane tih programa. Postoje izveštaji o tome da se spam-eri upravo na ovako prikrivene poruke iz osvete znaju okomiti...

2.3 MAILING LISTE

SPAM-eri se uvek trude da dođu do kopija adresa mailing listi potpisnika newsletters-a (neki mail serveri bazirani na listama će deliti svima koji te liste zatraže). Druga metoda je da spamer sazna nazive listi je takav da jednostavnim slanjem na listu pošalje (bez znanja o tome ko je na listi) svim korisnicima liste poštu, stavljajući istovremeno server pod težak rad - prosleđivanje kopije maila do pojedinca.

2.4 WEB STRANE

SPAM-eri skeniraju web strane po adresama koje stoje iza "mailto" html tagova (kad ih kliknete otvara vam se prozor mail programa). Široko rasprostranjena i efikasna tehnika pomoću koje se web masteri mogu zaštititi protiv ovoga je "poison CGI skript" http://www.monkeys.com/wpoison/

2.5 WEB I PAPIR FORMULARI

Neke web strane koje posećujete će tražiti od vas da ispunite online formulare, kao što su lista gostiju, narudžbenice i registracijski formulari. SPAM-eri dolaze do tih adresa zato što se iste objavljuju na nekim stranama kao reference ili ih

3. http://www.hotmail.com, http://www.yahoo.com http://www.gmail.com

4. Spisak UseNet provajdera: http://www.exit109.com/~jeremy/news/providers/providers.html

jednostavno dobiju od vlasnika tih strana za novac ili neku drugu uslugu.

Neke firme, kao što su organizatori skupova ili seminara, će prodati adrese koje su skinule sa papirnih formulara.

2.6 IDENT DEMON

Kod mnogih servera u pozadini radi demon (program inicitran od strane administratora) čiji je zadatak da dopusti drugim kompjuterima da identifikuju ljude koji se na njih povezuju. Kada se osoba koja surfuje na takvom kompjuteru konektuje na neki sajt, chat ili news server, taj sajt tj., server se može konektovati nazad i zatražiti od demona email adresu. Neki chat klijenti na PC-u se ponašaju tako, pa korišćenje IRC-a može imati za posledicu prosledivanje email adrese spam-eru.

2.7 WEB BROWSERI

Neki sajtovi se služe raznim programerskim veštinama pri izvlačenju email adresa iz web browsera korisnika koji ih posećuju, obično bez da su korisnici toga uopšte svesni. Evo i nekih programerskih trikova :

Browser se prisiljava da downloaduje neki fajl, npr. sliku sa sajta putem anonymous FTP-a, pri čemu se za login, ako je browser tako konfigurisan , koristi email adresa kao lozinka.

Koristeći JavaScript daju se instrukcije posetiočevom browseru da pošalje mail sa adresom koja je već unesena u browser posetioca. Neki browseri će dozvoliti slanje emaila-a pukim prelaskom miša preko određenog polja web strane, bez obzira da li korisnik dobije ikakav signal o tome (ukoliko je browser tako podešen).

Koristeći «HTTP_FROM» heder neki browseri jednostavno prosleđuju taj heder koji sadrži email adresu svakom serveru koji se posećuje. Da bi proverili da li se Vaš server ponaša ovako kao i ako Vas interesuju druge zanimljive informacije, posetite http://www.privacy.net/analyze/. Korisnik treba biti svestan opasnosti koje sa sobom nosi aktivni sadžaj (Java applets, JavaScript, VB,...) bez obzira na to da li koristi browser ili email klijent pri čitanju HTML poruka. Jedan email koji u sebi sadrži HTML može da sadrži i skript koji nakon što je kliknut da bude pročitan (čak je dovoljno da samo subjekt poruke bude markiran...!) automatski šalje email na bilo koju adresu. Primer za to je Melissa virus, koji ne samo da šalje spam-eru korisnikovu adresu, nego i sve adrese iz adresara.

2.8 IRC I CHAT SOBE

Neki IRC[1] klijenti će dati email adresu onog koji chat-uje bilo kome ko je zatraži. Mnogi spameri kradu te adrese znajući da su one validne i aktivne. Ovaj način hvatanja adresa je posebno interesantan za spam-ere, jer je IRC jedna od prvih aktivnosti Internet početnika , tako da na ovaj način dolaze do svežih adresa i ljudi koji još ne znaju kako da postupaju sa spam-om.

2.9 FINGER DEMON

"Finger query" demon šalje upit za informacije o korisniku na serveru. Npr., upit "finger pera@ host" će izbaciti listu informacija koje uključuju login imena za sve ljude koji se zovu "pera" na tom hostu/serveru. Takođe, upit „finger @host" će izbaciti sve trenutno aktivne korisnike na serveru. SPAM-eri rado koriste ovako dobijene adrese, jer su „žive/aktuelne"

2.10 Whois

Svaki Internet domen ima javno pristupačan zapis - kontakt osobe odgovorne za taj domen : administrativca, tehničara i komercijalistu. Najmanje jednom od njih moraju biti objavljeni ime, email adresa i telefonski broj. Dakle ovi podaci moraju biti validni i šta više, ovi ljudi su u obavezi da redovno čitaju poruke, tako da su radi izbor spam-era. (Tipično je da su upravo one adrese koje nisu validne, ustvari one adrese kojima se služe sami spam-eri).

2.11 Pogađanje

Neki spam-eri uspešno šalju test poruke ili pravi spam sa listom izmišljenih adresa. Nakon

1. Internet Relay Chat (IRC).

toga oni čekaju na odgovor da adresa ne postoji ili bez odgovora. Slučaj bez odgovora je za Spamera dobar odgovor. Takođe nekada šalju nestandardni ali često korišćen mail heder koji zahteva da sistem isporuke ili krajnji klijent potvrdi prijem ili čitanje poruke.

Dalje, u svojim porukama često stavljaju HTML sadržaj (web stranu) sa usađenim slikama. Mail klijenti koji automatski prikazuju sadržaje HTML-a u pretprikazu (*preview pane*) - kao što su Outlook, Outlook Express, Eudora - će pokušati da download te slike istovremeno šaljući sopstvenu e-mail adresu koja se naravno registruje. (Malo uprošćeno objašnjenje, ali u principu ovako radi) Outlook 2003 ima ugrađene mehanizme zaštite od ovoga, dok se kod ostalih preporučuje da se jednostavno ukine „*preview pane*".

Takođe, spam-eri koriste nepažnju većine korisnika/opsluživača sistema koji i dalje rado koriste standarna imena u mail adresama kao: administrator, admin, support, info, postmaster, sales, register, purchase, prvoime.drugoime ...

2.12 Razne bele, žute strane i direktorijumi

Postoje na Internetu razne bele strane ili „people finder" web strane. I žute strane danas imaju svoj mail direktorijum. Oba servisa izvlače svoje adrese iz izvora kao što su UseNet ili chat sobe. Ponekad će vaša adresa biti automatski registrovana kod ovih. Na primer Hotmail će automatski proslediti Vašu adresu ka „BigFoot"[2]-u, obznanjujući vašu adresu ljudima koji žele da Vas nađu (pa ... recimo da onda mogu da Vas „**baš nađu"** probavajući razne lozinke dok jedna ne upali...). U nastavku je data tabele (tabela 2.) raznih belih, žutih strane i direktorijuma.

2.12 PRISTUP ISTOM KOMPJUTERU (lokalno ili sa daljine)

Na UNIX kompjuterima je lista aktivnih korisnika *„users" file (/etc/passwd)* javno dostupna upitom *who.*

2.13 Neko je već imao istu adresu

Što se dešava. Ljudi menjaju provajdere koji svakom novom korisniku koji dođe dozvoljavaju da koristi bilo koju slobodnu email adresu, ne vodeći računa da bi ipak bilo bolje dodati samo jedno slovo ili broj koji Vas pošteđuje od spama koji je dobijao prethodni vlasnik te email adrese.

2.14 Socijalni inženjering

Čuvajte se razgovora na temu vezanu za Vašu email adresu sa nepoznatim osobama. Spameri ili hakeri će se pretvarati da su neko koga poznajete, kao prijatelj, saradnik itd. Ovo je već razvijena i najčešće korišćena hakerska veština, koja eto nema nikakve veze sa poznavanjem modernih kompjuterskih tehnologija, ali je najefikasnija.

U tom smislu i na ovom mestu bih apelovao na korisnike da ne nasedaju na «dobronamerne» lančane mailove tipa «pošalji ovu (veliku) poruku na adrese još 5 dragih osoba i svi ćete postati srećni...». Postaćete sami spam-er i saučesnik u spam-u. Neki će se obradovati možda Vašem znaku pažnje. No ako ih primaju često ili ako saznaju da su preko Vas postali žrtve spama, onda možete i da budete podstrekač spama.

2.15 Kupovina listi

Postoje dva izvora nabavke listi :

a) Od ljudi koji su došli do gore navedenim (sumnjivim) metodama, najčešće na CD-u, ili do onih koji su te adrese i sami kupili od istih.

b) Od firmi i organizacija koje su legalno došli do adresa. Znači sve moguće organizacije kojima ste dali adresu bilo u papirnoj formi bilo da ste im pisali. Pri tome ste se složili (najčešće jer ste brzo čitali ili vam u tom momentu nije bilo važno, da Vaša adresa sme biti prosleđena nekom drugom u svrhe informisanja o uslugama i proizvodima.

2.16 Hakerisanje

Nedavno je u više zemalja došlo do hapšenja pripadnika jedne hakerske grupe. Oni su prodavali IP adrese kompjutera, koji su bili zaraženi virusima-trojancima, raznim spam-erima. Ne zato

2. http:// www.**bigfoot**.com

Tabela 2. Tabela belih i žutih strana.

Personal Homepage Directories	Whitepages A-M	Whitepages N-Z
1st Search Personal Homepages	411 Locate	NedSite's listing of whitepage directories
Ahoy! The Homepage Finder	AnyWho Directory	Needle in a CyberStack - the InfoFinder People Finders
CULTURE--People--Lists -- directories, home pages	AOL NameCheck	Netbook
Excite Personal Home Pages	Bigfoot	Net Citizens
Home of Homes	Canary-Guide Email-Email Directory	Netscape Guide: People
Homepage Connection	Club Quest White Pages	The Online Chatter Directories
Housenet	CyberAddress by Monte Cristo	People Finder
Magellan Personal Home Pages Topics	The Directory Organization	People Finder Search Engine
MARCO's Worldmap of Homepages	E-Search	PeopleSearch
Meeting Place	EmailChange.com	People Search
The People Page	Email Finder	Persona
People Pages	Email Search	Pin-Point People Search
Personal Home Page Directories by Country	ESP - Email Search Program	PHWWW - Web Access to NetPages
One Nation Worldwide	Excite Email Lookup Excite People Finder	Populus People Locator
The People Place	Find A Friend ($)	SearchAmerica ($)
Personal Pages Worldwide - College and University Collections	Find mE-Mail	Switchboard
Personal Seek	Find People Fast ($)	Sycrawler: Penpal and Personals Search Engine
Search Personal Pages!	Four 11	Usenet Addresses Service (MIT)
	Grafix's World Wide White Pages	
	HotWire's People Finder	

da bi ovi slali na te adrese spam, nego zato što je uz pomoć virusa "Randex"[1] na ovim PC-ima bio instaliran takav trojanac, koji je instalirao Socks-Proxy Server koji je opet služio za prosleđivanja i generisanje bezbrojnih spam-ova. Naravno sve bez znanja vlasnika zaraženih računara. Virus se preko Windows-Directory servisa sam lako razmožavao dalje po subdirektorijima lokalne mreže. Naravno, isti trojanci mogu poslužiti i za druge vrste napada (DDoS), ne samo u "komercijalne" svrhe, ali Scotland Yard je izrazio zabrinutost od ovoga, jer su se do sada hakeri bavili ovakvim napadima više iz radoznalosti i obesti, dok im se sada pruža prilika da zarade poprilične sume novca.

Takođe, ako web strana krije u sebi dovoljan broj adresa, spam-eri neće prezati od toga da u nju provale**.**

1. http://securityresponse.symantec.com/avcenter/venc/data/w32.randex.e.html

3. MERE ODBRANE

Koliko je spam uzeo maha o tome svedoči i zakon koji je G. Bush potpisao 16.12.2003.(29.4.04 slika 2) čime je otpočeo prvi kazneni proces po ovom zakonu koji predviđa zatvor do pet godina, kao i novčane kazne do šest miliona dolara. Prostire se po važenju i na spam koji dolazi iz inostranstva. Dvojica od svih optuženih su već u pritvoru. Dakle veoma strog zakon što se tiče kazni. Izvod iz zakona je predstavljen na slici 2.

Interesantna je i činjenica da je sa stupanjem na snagu ovog zakona nije smanjena količina spam-a, nego se čak i malo povećala (možda treba sačekati neko vreme da bi se efekti pokazali).

Razlog tome je što se (sad) kriminalni spam-eri koriste metodama zavaravanja identiteta (preko 85 % spam-a krši Can-Spam Act), i što je spam ipak pod određenim uslovima dozvoljen i pun rupa.

Regarding Federal Anti-Spam Legislation: "CAN-SPAM" or Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (S 877)

The CAN-SPAM Act was signed into law by President Bush on December 16, 2003, with an effective date of January 1, 2004. It pre-empts state laws (including California's) regarding sending commercial e-mail- with the exception of state laws dealing with fraud. The new law is for the most part positive for business and for e-mail list rental. Essentially, honest commercial email is legal as long as it meets specific requirements. E-mail messages with the primary purpose of advertising are considered commercial e-mail in CAN-SPAM. The basic requirements and DM2's plans for complying are:

CAN-SPAM Requirements	DM2 Plans for Compliance	Change from DM2's Practices in 2003
Clear and conspicuous notice of opt-out opportunity and a working Internet based opt-out mechanism to future offers from the marketer. Marketer must offer an opt-out to all e-mail from the brand promoted throughout the message - but may also include more detailed options (opt-out just to offers from third parties, opt-out to promotions, events, etc.)	Marketer will be required to include a link to their own opt-out mechanism. DM2 will place marketers opt-out link, with instructions, on the first "screen" or "above the fold". If the marketer does not have an opt-out mechanism, DM2 may offer, under a seperate contract and fee arrangement, to provide this service for a limited time. DM2 will also include an opt-out to future messages from receiving all third party offers from the list owner.	New requirement based on CAN-SPAM. Only DM2's opt-out mechanism was included in the past.
Opt-outs must be removed from future commercial e-mail campaigns from marketer within 10 business days. Mechanism must be functional for at least 30 days after the campaign is sent.	Marketers will be required to provide a list of past opt-outs for suppression before each campaign. DM2 will suppress list of past opt-outs provided by marketer for suppression before each campaign.	New requirement based on CAN-SPAM. Only DM2's past unsubscribe/opt-outs were suppressed in the past.
Marketer's physical postal address must be included on the message.	Marketer's physical postal address will be included on the message as will DM2's.	New requirement based on CAN-SPAM.
"From" line must be either the list owner or the marketer.	This is in keeping with our current policy and practices.	No change
Clear and conspicuous "identification" of message as advertisement or solicitation.	DM2's standard "header" meets the requirements as we understand them.	No change
Subject lines must be honest and clear as to what is being offered.	This is in keeping with our current policy. In addition, we are encouraging best-practices - the subject line should include a benefit and the brand name of the marketer.	No change

Slika 2. Izvod iz Zakona

SPAM ima svoj veoma jak lobi i kontakte sa vladama. U 2002. godini su samo pošiljaoci spama platili porez na preko 250.000.000 USD. (Ta suma je danas višestruko veća). Oko njih se razvio i još jedan čitav biotop koji zahvaljujući njima isto zarađuje pare, proizvođači hardvera i softvera koji štite od spama, konsultanti, advokati i da ironija bude veća, i oni koji vas izveštavaju o spamu.

Nedavno se i „Kaspersky“ (poznati osnivač istoimene antivirus-firme [1]) izjasnio protiv striktnije zabrane spama, navodeći poređenje sa vremenima prohibicije alkohola početkom prošlog veka, zaključivši da će to samo podpomoći kriminalnim strukturama u ovom unosnom poslu.

Dakle ukratko, dozvoljen je spam sve dok primaoc eksplicitno ne zatraži da bude skinut sa liste primaoca spam-a. Zato spam da bi bio legalan mora u sebi da sadrži opciju (*Opt-out*) čijim klikom se mi izjašnjavamo da ne želimo da primimo više nijednu reklamnu poruku od tog pošiljaoca. Međutim, kao što je to u ovom tekstu na jednom mestu objašnjeno, ne preporučuje se da odgovarate na spam poruke, pa čak i da ih uopšte ne otvaramo, jer ćemo verovatnije dobijati još mnogo više spam-a nego pre (dajući do znanja pošaljiocu da je email adresa živa i da se koristi).

Pošto spam i virusi idu često ruku pod ruku, ovo poglavlje ću proširiti pričom o čistom poštanskom sandučetu [7]. Ako se zaštitite od spam-a, uveliko ćete se zaštititi i od zaraza koje dobijate putem maila. Nezaštićenost od virusa će Vas kad tad koštati.

Dakle od „zaraza“ se štitimo na dva načina metode :

I) kroz disciplinu neizlaganja opasnostima i

II) kroz upotrebu softvera (antispam, antivirus programi).

4. NEIZLAGANJE OPASNOSTIMA

Disciplina uzdržavanja od izloženosti je skoro ista za spam i viruse tako da ću izložiti samo jednu listu [8]:

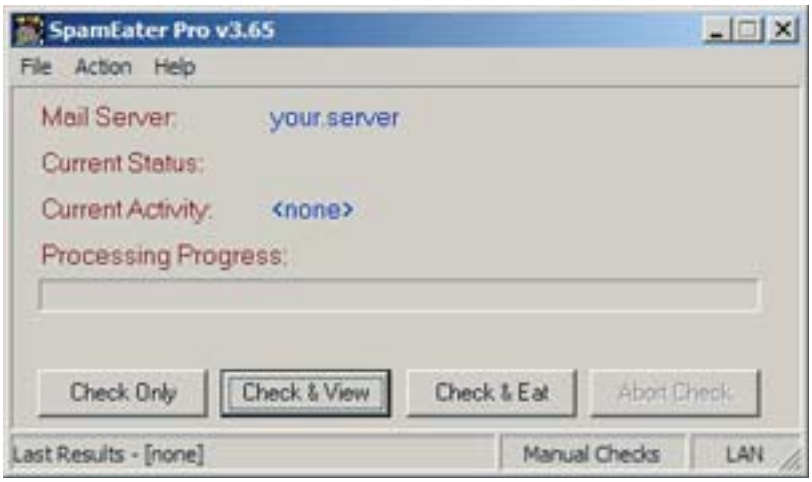
1. Ne otvarajte nikad poštu od pošiljaoca koga ne znate (pogotovu ne fajlove koji su prikačeni). Čak i u slučajevima kada pošta dolazi od poznate adrese, ne mora da znači da nije izlažirana ili da nije zaražena virusom. U tom slučaju se preporučuje da prikačeni fajl (ako imate vremena) ostane malo duže u inbox-u dok antivirus kuća, čiji se program koristi, napravi update za najnoviji virus. Ovo takozvano vreme reakcije je od (u proseku i zavisno od komplikovanosti virusa, kao i antivirus programa) tri sata do 24 sati od pojave virusa. Savet bi bio da se instalira update i proveri da li je poruka od poznate osobe koju ste dobili zaražena.

2. Bacite pogled na poglavlje koje govori o načinu na koji spam-eri dolaze do listi i ne dajte im da lako dođu do Vaše adrese. U tom smislu, savet je da se koriste više mail adresa. Neka neke od njih služe za “opušteniju” podelu i korišćenje, mada se i pored toga mora biti oprezan. Kad tad će naići neko ko će od Vas tražiti neku drugu mail adresu pod izgovorom da iz nekog razloga pošta neće da stigne na datu adresu. Ako baš morate, dajte mu opet neku rezerevnu, najbolje neku web mail adresu ali nikako adresu Vaše firme ili ličnog ISP-a.

3. Ne se biti mnogo sporiji od hakera. Operativni sistemi i programi se moraju redovno ažurirati. Na žalost Microsoft je nenamerno veliki pomagač hakera. U svojoj revnosti, Microsoft objavljuje svaki njemu poznati bug i rupu u sistemu u želji da obavesti korisnike o rizicima kojima su izloženi. Međutim, oni koji prvi saznaju o njima su hakeri koji odmah žure da iskoriste te rupe. Jako mali deo krajnjih korisnika za razliku od hakera svakodnevno posećuje Microsoftov sajt. Na žalost, slično čini i većina administratora, tako da mnogi sistemi ostaju ranjivi danima, mesecima, godinama... Postoje posebni patche-vi update-i za operativni sistem, browser, mail client, antivirus software i programe uopšte.

4. Ako se ima i najmanja sumnja ili indikacija da je računar zaražen, vadi se mrežni kabl iz računara i time će se sprečiti veće zlo na vašem i

1. http://www.kaspersky.com/



Slika 3. Interfejs programa SpamEater

tuđim računarima. Posle toga preći na skeniranje sistema sa nekim od Antivirusnih programa i ako (i samo ako) je sve u redu, nastaviti sa normalnim radom.

5. Ispravno konfigurisanje sistema. Ovde bih naveo par saveta koji imaju za cilj veću bezbednost email klijenata (izostaviću OS, browser i druge programe) i to Outlook Express-a i Outlook-a kao najčešćim mail klijentima u praksi, čime se istovremeno umanjuje mogućnost izazivanja štete pri slanju i primanju mailova.

Outlook Express – Otvoriti program i pod tools/options/read karticom čekirati "read all messages in plain text", što će imati za posledicu da program sve HTML poruke formatira kao čisti tekst. Nema više slika. Ali na taj način nema ni JavaScript napada. Međutim, ovo se može podesiti već od šeste verzije ovog mail klijenta.

Onaj ko ipak želi da čita povremeno i "slikovitije" poruke, bolje neka to čini samo od slučaja do slučaja. Najlakše uz pomoć besplatnog programa "OE Tool"[2] koji stavlja posebno dugme u program pomoću kojeg "šetate" između dva moda.

Onaj ko ni po koju cenu neće da se odrekne multimedijskog doživljaja, neka pod view/layout isključi View Bar. Postoje napadi koji se dese prostim otvaranjem/prikazom HTML mail-a. Na ovaj način, pogledom na zaglavlje poruke možete proceniti da li je poruka spam/virus i izbrisati je bez otvaranja.

Sledeća stvar je da se pod tools/options/security/virus protection aktiviraju tri stvari *: Restricted sites zone* (prethodno u exploreru podesite da se aktivni sadržaji ne mogu izvršavati), zatim *Warn me when other applications try to send mail as me* (čime se postiže da se dobije poruka upozorenja pre nego što se počne slanje virusa i spam drugima) i na kraju *Do not allow attachments to be saved or opened that could potentially be a virus*. U ovom zadnjem slučaju Outlook Express blokira sve vrste fajlova koji mogu da sadrže skripte i kodove, pa čak i bezazlene formate .gif ili .jpg. Ukoliko se koristi ova restrikcija, a ipak treba da se pogleda sadržaj koji nije samo čisti tekst, onda se deaktivira ova zadnja opcija privremeno, pročita se poruka i opet se aktivira ta opcija. Ako vam je stalo do sigurnosti i mira.

U Service Pack-u 2 koji je Microsoft objavio ubačeni su nekoliko sigurnosnih poboljšanja.

Outlook – Ovaj email klijent ima u sebi već ugrađen automatski filter koji HTML poruke pretvara u tekstualne i ne pušta naknadno nikakve elemente. Treba ga samo aktivirati pod tools/options/security/change automatic download settings popunjavajući sva polja zelenim kvakama. Starije verzije Outlook-a takođe mogu da suzbiju HTML prikazivanje, samo što korisnik mora ipak da uđe u Registry i napravi male izmjene: Za

2. http://www.insideoe.com/resources/tools.htm

Outlook 2002 sa/od SP1 pod ključem: HKEY_CURRENT_USER\SOFTWARE\Microsoft\OFFICE\10.0\ Outlook\Options\Mail postavite jedan novi DWORD sa oznakom ReadAsPlain i postavi mu se vrijednost na 1.

Kod Outlooka 2000 sa/od SP1 koristite isti trik samo što se koristiti drugi ključ, koji u sebi ne sadrži 10.0 nego 9.0 . Za dodatnu zaštititu Outlook-a protiv skripti, postupak je isti kao i kod Outlook Express-a. (tools/options/security.....)

Što se tiče zabrane pristupa raznim formatima, ovde je Outlook za razliku od Outlook Express-a preterano rigorozan i ne dozvoljava povremeno skidanje ovih zabrana. Ali zato postoji besplatan eksterni softver "Attachment Options"[1], koji vam omogućava da sami odredite koji tip falova želite da vidite/propustite.

5. ANTISPAM, ANTIVIRUS PROGRAMI

Druga način da se spreče Spam poruke i virusi, podrazumeva upotrebu specifičnih programa kao što su Spam blokeri, Spam filteri, antispam filteri, email-filteri, imaju zadatak da štite od spam-a. Oni to sigurno ne postižu u 100% slučajeva, ali se polako približavaju toj brojci [9].

Postoje različiti spam filteri i metode njihovog rada, ali prvu podelu ćemo napraviti na one koji su predviđeni za pojedince i male firme, i na one koji su predviđeni za velike organizacije i ISP provajdere. Trend u filozofiji zaštite od spam-a, je da ovi mailovi uopšte ne dođu do korisnikovog računara, dakle da se već kod ISP-a ili lokalnog mail servera isfiltriraju. Međutim zasad to još naravno ne funkcioniše, tako da je najčešće lični PC- filter dobrodošao.

1. http://office.weblogsinc.com/entry/1234000243059431

6. ONLINE SPAM FILTERI

Spam Arrest[2] nudi pametno rešenje pri čemu se nepoznatom pošiljaocu šalje „challenge request" i time traži da se ručno/neautomatski odgovori na ovaj zahtev. spam-eri se na sreću još uvek pozabavili time da na ovaj metod reaguju odgovarajućim automatizmima, tako da njihova pošta biva zadržana na vašem mail serveru i ne dolazi do vas.

6.1 server bAZIRANI spam filteri

Kao što sama reč kaže, ovi spam filteri instaliraju se na servere kod ISP-a ili u vašoj firmi, i imaju zadatak da poštu koja pristiže analiziraju pre nego što stigne do vašeg PC-a.

Na žalost ovo nekad ne funkcioniše kako treba (za razliku od gornje metode) i dešava se da legitimna pošta bude okvalifikovana kao spam i bude izbrisana. Primer ovakvih programa **je iHate Spam Server Edition**[3].

6.2 PC bazirani spam filteri

Mailwasher pro[4] je jedan od popularnijih programa na tržištu. Svaki put kada želite da proverite poštu onda se startuje ovaj program koji vam dozvoljava da napravite tzv. *preview* (pre-pogled) Vaše pošte i ako je ne želite, da je izbrišete pre nego što ste je spustili na Vaš računar. Jedna od dobrih radnji koje ovaj program izvodi je da vam dozvoljava da pošaljete spam-eru odgovor koji glumi "mailer daemon error message" - poruku da nema nikoga iza te adrese. Pošto se kod spamera sve odvija automatski, bićete i automatski skinuti sa liste. Jednostavno, ali efikasno. Ostali dobri spam filteri : **MacAfee Spamkiller, Cloudmark Spamnet, Spam Inspector 4.0, Spam Bully, SpamPal, Brightmail, Sophos...** Napominjem da Spam filteri nisu poređani po nekom kvalitetu ili pripadnosti, nego nasumice, ali im je zajedničko to da su veoma dobri i provereni. Neki

2. http://www.spamarrest.com/
3. http://www.sunbelt-software.com
4. http://www.mailwasher.net/

su i besplatni. Takodje, neki od njih se mogu nazvati i inteligentnima. To su oni koji koriste teoriju Thomasa Bayes-a, pa se zovu i ***Bayesian spam filters***. U principu su to programi koji su u stanju da uče na osnovu poređenja grupe poruka koje ljudi definišu kao spam i grupe legitimnih poruka. Jedan po meni dobar i efikasan program je i Spameater pro firme High Mountain Software[5]

Posle konfigurisanja POP3 email accounta dodajemo username i password. Ukoliko postoji više naloga na tom serveru koji se vode na isto ime postoji opcija acceptable email address (prihvatljive email adrese). Glavna stvar je da se podese filteri. To je ključni deo. Dakle tu definišemo kriterijume po kojima će poruka biti prihvatljiva ili deklarisana kao spam. Ovde treba biti obazriv jer možemo da utičemo tako da nam i legitimne poruke budu deklarisane kao spam. Naravno možemo da istestiramo naš filter tako što posle konfiguracije samog programa pritisnemo opciju na programu check & view (slike 3.) da dobijemo informacije koje su poruke po zadatom kriterijumu deklarisane kao spam. Ukoliko su to i neke poruke koje nisu spam možemo da korigujemo filter. Ovaj program pripada kategoriji anti-spam softwera za pojedince ali može da se upotrebljava i u preduzeću jer možemo da unesemo veliki broj naloga za proveru.

4. ZAKLJUČAK

Posle ovog izlaganja ostaje nam da zaključimo da je sve više ljudi koji slobodu koju u svakom pogledu pruža Internet pogrešno tumače. Oni Internet servise koriste na taj način da nanose štetu kako drugim korisnicima tako i sistemima Internet provajdera, ostvarujući korist bilo u materijalnoj formi ili u formi satisfakcije ili zbog nekih "viših ciljeva". U žargonu ih zovemo spamerima i u izlaganju smo ih podeliti u tri kategorije: one koji svoju slobodu koriste da se zabavljaju na tuđ račun, oni koji žele da ostvare korist (direktni marketing), opet na tuđ račun, i treća, možda najbrojnija kategorija, a to su obični korisnici Interneta koji iz neznanja rade neke stvari koje nanose štetu drugima.

Razumljivo je, samo prve dve kategorije ljudi svrstavamo u „štetočine" i oni spadaju u grupu protiv koje se stvarno borimo, jer samim tim što se bave takvim aktivnostima oni pokazuju svoju bezobzirnost i nepoštenje. Svi pokušaji da se neko od njih preobrati u normalne korisnike završili su potpuno bezuspešno. Oni su inače veoma maštoviti u nalaženju načina da maltretiraju što više ljudi ne prezajući ni od čega.

Treća kategorija, "novajlije-neznalice" su obični, normalni ljudi, koji nalaze Internet korisnim. Ipak, zbog svog neznanja umeju da naprave popriličnu štetu, i najčešće toga nisu ni svesni. U praksi, kada im se skrene pažnja oni se izvinjavaju i trude se da ne ponove greške. Sve u svemu, sloboda na Internetu je ograničena samo time da se od Vas očekuje da svojom aktivnošću ne nanosite materijalnu ili drugu štetu drugima. Deviza koja treba da glasi : **Imajte obzira prema drugima**.

Na Internetu ne postoje sudovi i sudski procesi. Kod očigledno nelegalnih aktivnosti stvar rešavaju administratori, najčešće onog sistema čiji je korisnik napravio štetu. Jednostavno mu zabrane dalje korišćenje Interneta sa tog sistema. I na kraju teksta ostaje mi još samo da napomenem da je prva metoda - oprez i uzdržavanje od riskantnih poteza delotvornija, od druge metode hvatanja i čišćenja spama, koja dolazi u stvari tek ako ste pali na prvoj..

RESUME
SPAM

In this text will be elaborated the idea of spam. It will be explaned what does make an email message a spam, and what doesn`t, how to avoid sending and receiving spam messages, why the firms are using such messages and why the hackers are using these techniques.

5. http://www.hms.com/spameater.asp

BIBLIOGRAFIJA

[1]Wikipedia:
http://en.wikipedia.org/wiki/SPAM .

[2] Barracuda Networks:
http://spam.abuse.net/overview/whatisspam.shtml

[3] CipherTrust Spam:
http://www.ciphertrust.com/resources/statistics/spam_sources.php.

[4] CBSnews:
http://www.cbsnews.com/stories/2004/07/06/tech/main627736.shtml.

[5] Sophos annual reports:
http://www.spamfo.co.uk/component/option,com_content/task,view/id,206/Itemid,2/ .

[6] Dragan Varagić, Kultura komunikacije na Internet-u i njen odnos sa Internet marketingom, http://www.pretraga.co.yu/osnove/internet/strana.php?s=sta_je_spam.

[7] Business Internet International News Digest
http://www.clickz.com/stats/sectors/email/article.php/3521046 .

[8] CNet - http://reviews.cnet.com/4520-3664_7-5020441.html .

[9] Electronic Communications Privacy Act - http://www.rewi.huberlin.de/Datenschutz/USA/ElectronicPrivacyAct.html .