UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Marjeta Novak

PROBLEMATIKA IN REGULACIJA SPAM SPOROČIL

Diplomsko delo

LJUBLJANA, 2004

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Marjeta Novak

Mentor: izr. prof. dr. Vasja Vehovar

PROBLEMATIKA IN REGULACIJA SPAM SPOROČIL

Diplomsko delo

LJUBLJANA, 2004

Hvala Vam profesor Vehovar,
hvala Tebi Andraž,
hvala vam vsem, ki ste z dobro voljo prispevali k podobi mojega diplomskega dela!

VSEBINSKO KAZALO

SLIKOVNO KAZALO

UVOD

Hitro naraščanje števila individualnih potrošnikov s specifičnimi željami in potrebami zmanjšuje učinkovitost množičnega marketinga na eni strani, hkrati pa po drugi strani pospešuje razvoj neposrednega marketinga. Neposredni marketing zato dobiva vse večje razsežnosti in nove oblike. Vse to prinaša podjetjem večji dobiček, potrošniku pa ogrožanje zasebnosti. Izjemno velik potencial neposrednega marketinga prinaša tudi internet. Zaradi narave tega novega medija – ki omogoča bolj intenzivno interaktivnost in bistveno večjo personalizacijo marketinških sporočil – se hitro pojavljajo tudi najrazličnejše nove oblike neposrednega marketinga.

Spletna tehnologija je napredovala že do te mere, da omogoča razvoj nadvse učinkovitih in kreativnih oglaševalskih akcij. Večje oglasne površine, novi formati, vključitev videa in praktično neomejene možnosti kreativnih rešitev odpirajo podjetjem nove možnosti. Tako lahko npr. s pravilno uporabo elektronske pošte (v nadaljevanju e-pošta ali e-mail) povečujemo prodajo in učinkovitost, gradimo ugled podjetja in blagovne znamke. E-pošta omogoča tudi hitro in poceni pošiljanje oglaševalskih sporočil velikemu številu internetnih uporabnikov in enostavno merjenje učinkovitosti. Žal je mogoče vse dobre stvari tudi zlorabiti. Zloraba e-pošte se imenuje nezahtevana e-pošta ali spam, ki ima svoje korenine v realnem svetu – v poštnih nabiralnikih, polnih brezplačnih revij, oglasov in katalogov.

Množično pošiljanje spama je danes prekoračilo že vse meje. Hromi sisteme, ki se uporabljajo za njihov prenos, polni e-poštne predale, preprečuje pravočasen prenos legalne e-pošte, krati čas in denar končnim uporabnikom ter ponudnikom interneta, poleg tega pa znižuje tudi produktivnost v podjetjih. Tovrstna sporočila ogrožajo tudi zasebnost uporabnikov in se uporabljajo kot orodje za prenos računalniških nadlog − virusov in parazitskih programov.

Količina spamov bliskovito narašča in je v mnogih državah že prehitela delež legalnih e-sporočil v naših e-poštnih predalih. Črnogledi strokovnjaki napovedujejo nazadovanje »e-mail maketinga« in lastno uničenje e-pošte kot medija komunikacije, če bo smer gibanja trenda spama ostala nespremenjena. Kljub velikim vložkom antispam gibanj je videti, da niti tehnologija niti zakonodaja ne moreta zajeziti spletne kuge - spama.

V diplomskem delu nameravam podati celovito obravnavo problematike spama. V prvem poglavju diplomske naloge sem opredelila pojme in oblike neposrednega marketinga.

Drugo poglavje opisuje nove možnosti dostopanja do potrošnikov, ki jih ponujata internet in e-pošta. Zaradi boljše primerjave s spamom sem navedla primer legalne e-pošte in opisala njene značilnosti ter etično vedenje pošiljateljev pri zbiranju e-naslovov, kreiranju sporočil in odločanju o načinu pošiljanja e-pošte. V poglavju obravnavam vse bolj želen marketing s privoljenjem oziroma »opt-in marketing«, ki spoštuje odločitve potrošnikov.

Tretje poglavje opisuje različne definicije in načine spama. Posebno pozornost sem namenila oblikam spama in virom e-naslovov, ki jih pošiljatelji spama »s pridom« izkoriščajo.

Empirični podatki, navedeni v četrtem poglavju, potrjujejo, da problem resnično dobiva vse večje razsežnosti in povzroča težave na različnih področjih, tako posameznikom kot tudi podjetjem. Visoki stroški prejemnika, prevare, ogrožanje varnosti, zmanjšanje produktivnosti v podjetjih in učinkovitosti e-poslovanja ter večanje splošnih družbenih stroškov so glavne posledice spama. Na tem mestu sem se dotaknila še področja mobilne telefonije, kjer se tudi že pojavljajo posamezni primeri spama, čeprav zaenkrat še ne ogrožajo delovanja omrežja in končnih uporabnikov.

V petem poglavju, ki je razdeljeno na tri dele, sem preučila številne načine omejevanja spama. Prvi del navaja različne načine samoreguliranja, delovanja tehnoloških rešitev in etičnih pravil, ki pa v današnjem času skoraj ne vplivajo več na vedenje uporabnikov interneta. Drugi del namenjam tako imenovanim »antispam« organizacijam in združenjem, ki v želji preprečitve pošiljanja spama z analizami pomagajo pri oblikovanju filtrirnih sistemov in zakonov. Tretji, najbolj obsežni del, prikazuje različne načine pravne regulacije v ZDA in Evropski uniji. Izpostavila sem problem razdrobljenosti in neučinkovitosti antispam zakonov, ki so zaradi hitrega tehnološkega razvoja že na začetku svoje veljave bolj ali manj zastareli.

V šestem poglavju sem uporabila RIS-ovo raziskavo, izvedeno s telefonsko anketo med uporabniki interneta splošne populacije. Navedla sem tudi rezultate raziskave »Motečnost spama med študenti Ekonomske fakultete in Fakultete za družbene vede«. V tem poglavju je nekaj vrstic namenjenih tudi slovenskim ponudnikom interneta, njihovim težavam, s katerimi se vse pogosteje srečujejo, in predlogom izboljšav. Čisto na koncu sem omenila tudi novi zakon, ki v Sloveniji regulira pošiljanje spama, ter morebitne težave neučinkovitosti zaradi, po mnenju stroke, pomanjkljivih določb.

V zadnjem poglavju je prikazana učinkovitost posameznih regulacij, ki jih po eni strani slabi tehnološki pristop, po drugi pa zakonske omejitve. Na koncu sem povzela še lastno mnenje, predlagala nekaj potencialnih rešitev in predstavila svojo vizijo razvoja neposrednega marketinga preko e-pošte in omejevanja spama.

1 OPREDELITEV NEPOSREDNEGA MARKETINGA

Potrošnik postaja vse bolj zahteven in individualističen pri nakupovanju. Išče različno ponudbo izdelkov in storitev, ponudbo, ki bo ustrezala njegovim osebnim željam. Učinkovitost množičnega oglaševanja počasi slabi, ker se pojavljajo potrošniki s specifičnimi željami, ki jih je mogoče zadovoljiti le z neposrednim pristopom, prilagojenim posameznemu potrošniku.

Neposredni marketing ni nov fenomen, kot mislijo nekateri. Svoje korenine ima v preprostih seznamih kupcev, ki so jih uporabljali že pred nekaj desetletji, da so lahko trgovci svojim kupcem po pošti pošiljali želene izdelke. Osnova neposrednega marketinga so seznami, kaj je kdo kupil, danes jih imenujemo baze podatkov. Direktna pošta je bila zato dolgo časa sinonim za neposredni marketing. Schultz takole opisuje izvor tovrstnega marketinga: "Neposredni marketing se je razvil iz potrebe trgovcev, ki so imeli izdelke, katere so morali nekomu prodati, na zalogi. V ta namen so razvili in vzdrževali sezname poštnih naslovov potencialnih kupcev, katerim so pošiljali ponudbe in čakali na odgovor. V primeru, da odgovora ni bilo, so ponudbo poslali večkrat. Tako se je oblikoval neposredni marketing" (Schultz v Reitman, 2000: 4). Za današnji neposredni marketing Schultz trdi, da še vedno bazira na seznamu potencialnih strank, ki jim pošljemo proizveden izdelek ali storitev.

Opredelitev neposrednega marketinga se je razvijala skozi čas. Nanjo so vplivale številne globalne spremembe družbe, proizvodnje in trženja. Najbolj jo je zaznamoval razvoj tehnologije in s tem tudi razvoj medijev, ki postajajo vse bolj globalni. Večina strokovnjakov podpira definicijo združenja DMA (Direct Marketing Association): "Neposredni marketing je interaktivni sistem marketinga, ki uporablja enega ali več oglaševalskih medijev in vpliva na merljivo reakcijo in/ali transakcijo na katerikoli lokaciji (DMA v Blois, Sargeant, 2000: 592).

Kotler trdi, da neposredni marketing uporablja različne oglaševalske medije, da bi se vzpostavil neposreden stik s potrošnikom, pri čemer je v ospredju težnja dobiti neposreden odziv (Kotler, 1996: 655).

Podobno tudi Bird označuje neposredni marketing kot vsako marketinško aktivnost, ki ustvarja in izrablja direktni odnos med tabo in tvojim potrošnikom kot posameznikom (Bird, 1990: 28).

Stone, ki ga mnogi imenujejo guru neposrednega marketinga, se pridružuje definiciji DMA in dodatno poudarja pomembnost interakcije ali ena na ena komunikacije med ponudnikom in potrošnikom. Skrito orožje neposrednega marketinga je vedenje, kdo so naše najboljše stranke, kaj in kako pogosto kupujejo (Stone, 1994: 5).

Večina avtorjev v svojih definicijah poudarja interakcijo med ponudnikom in potrošnikom, le dva dodajata različnost medijev in neposreden odziv potrošnikov. DMA opredelitev precej na široko opiše neposredni marketing, saj dodaja, da je transakcija sporočil izvedljiva na katerikoli lokaciji. S tem želi poudariti, da lahko pride do stika med prodajalcem in potrošnikom na več načinov in preko različnih kanalov, kjer je mogoče meriti odziv potrošnikov. Nobena definicija pa ne navaja pomembnosti seznamov oz. podatkovnih baz, ki predstavljajo pomemben vir informacij in so še vedno eden ključnih elementov za učinkovit neposredni marketing.

Poznavalci neposrednega marketinga menijo, da se je njegova doba šele začela. Sergeant napoveduje, da ponudba prilagojena vsakemu posamezniku ne bo izjema, ampak pravilo, s tem pristopom pa stroški oglaševanja ne bodo naraščali (Sergeant v Blois, 2000: 613). Trend hitro vzpenjajočega se neposrednega marketinga kaže tudi raziskava DMA. Ocenjujejo, da se bo v obdobju od 2002 do 2007 v Evropi povečala prodaja preko neposrednega marketinga za 11,39 %, najmanj v Švici za 5,2 %, največ pa na Irskem za 17,7 %, v ZDA se bo povečala za 8,3 %, v Aziji pa kar za 20 %. Večja rast prodaje preko neposrednega marketinga je v nekaterih nerazvitih deželah pogojena tudi z razvojem in uvajanjem novih tehnologij (povzeto po Turner, 2001: http://www.the-dma.org/isec/9.pdf). Tudi v Sloveniji je internet neizogiben, čeprav oglaševalci še vedno dvomijo v učinkovitost interneta kot oglaševalskega medija. Po podatkih internetne oglaševalske mreže Httpool, se vrednost internetnega oglaševanja v Sloveniji za leto 2002 giblje med 140 in 150 milijoni tolarji (Httpool v Oseli, 2003).

1.1 Značilnosti neposrednega marketinga

Značilnosti neposrednega marketinga, ki jih večina avtorjev smatra kot bistvene (Stone, 1994, Bird 1990, Kotler 1996):

- **Interakcija**: Zelo pomembna je ena na ena komunikacija med ponudnikom in potrošnikom, pri tem se razvija tudi osebni odnos, ki pripomore k boljši ponudbi, prilagojeni vsakemu posamezniku.

- **Eden ali več oglaševalskih medijev**: Strokovnjaki neposrednega marketinga so odkrili sinergijo med mediji, uporaba kombinacije medijev je v oglaševanju pogosto bolj učinkovita kot pa izbor le enega medija.

- **Merljivost**: Merljivost reakcije potrošnikov je ena bistvenih značilnosti neposrednega marketinga. Oglaševalci lahko merijo odziv in učinkovitost posamezne oglaševalske akcije s testi, ki jim koristijo pri določanju uspešnosti same akcije in načrtovanju novih ali spremembah obstoječih akcij. Drage raziskave niso potrebne.

- **Uporaba različnih kanalov in lokacij**: Za prenos sporočil lahko uporabljamo različne kanale: telefon, pošta, elektronska pošta in lokacije: v trgovini, na ulici, doma ter številne druge lokacije. Lahko rečemo, da neposredni marketing prepleta celotni svet.

- **Baza podatkov**: Osnova in izvor neposrednega marketinga so podatkovne baze, ki vsebujejo osnovne informacije o potrošnikih, kot so ime in naslov do podrobnejših, kot so njegovi interesi, navade in kaj ter kako pogosto kupujejo. Čim bolj so obsežne in kvalitetne informacije, tem bolj lahko prodajalec prilagodi svojo ponudbo in komunikacijo posamezniku.

- **Zmanjšanje tveganja**: Pri neposrednem marketingu istočasno spremljamo tudi odziv potrošnikov na trenutno ponudbo. Z merljivostjo odziva in spremljanjem položaja na trgu držimo vajeti v svojih rokah, tako se s hitrim prilagajanjem razmeram na trgu in ciljni skupini potrošnikov zmanjšuje potencialno tveganje.

- **Kontinuiteta**: Hitra prilagodljivost in ponudba prilagojena vsakemu posamezniku pripomoreta k lojalnemu odnosu med ponudnikom in potrošnikom.

- **Selektivnost**: Omogoča natančno določitev ciljne skupine, ki poveča možnost realizacije nakupa in zmanjša stroške oglaševanja.

- **Prilagodljivost**: Kontrola odziva potrošnikov omogoča, da se prilagodi način, čas, kanal in lokacijo dostopa do ciljne skupine.

- **Kompatibilnost**: Veliko tehnik, ki se jih poslužujemo v neposrednem marketingu, lahko uporabimo tudi v drugih oblikah marketinga, s čimer povečamo učinkovitost.

- **Kvalitetnejša ponudba**: Neposredni marketing nudi potrošniku bolj celovito in enostavnejšo zadovoljitev potreb. Potrošnik izbira in naroča od doma, prihrani čas in denar ter se izogne stresnim situacijam.

1.2 Vrste in oblike neposrednega marketinga

Oblike trženja, ki se uporabljajo v neposrednem marketingu:

- **Osebna prodaja - prodaja od vrat do vrat**

Osebna prodaja je ena najstarejših oblik tržne komunikacije in poteka dvosmerno med prodajalcem in potrošnikom. Stik s potrošnikom se lahko vzpostavi že ob najavi obiska ali ob samem srečanju prodajalca in potrošnika.

- **Trženje po pošti**

Ponudnik in potrošnik prideta v stik preko pošte. Tudi vsi ostali procesi, kot so odgovor na ponudbo, plačilo in običajno dostava blaga, se vršijo preko pošte.

- **Trženje po katalogu**

Katalogi se razlikujejo glede na širino in vrsto ponudbe. *Splošne kataloge* pošiljajo trgovske hiše nekajkrat letno. V njih ponujajo širok spekter izdelkov za vse družinske člane. *Sezonske kataloge* pošiljajo predvsem turistične agencije, v katerih predstavljajo aranžmaje za določen letni čas. *Specialni katalogi* so tematsko omejeni in namenjeni predvsem ozkemu izboru potrošnikov. *Industrijski katalogi* podrobno predstavijo izdelke, zato so poslani specializiranim trgovinam, prodajnim zastopnikom in uvoznikom.

- **Trženje po telefonu**

Trženje po telefonu je zaradi takojšne povratne informacije precej podobno osebni prodaji. informacije pomagajo prodajalcu oblikovati in prilagajati komunikacijo posamezniku. Razvoj trženja po telefonu so pospešile brezplačne številke in avtomatizirano sprejemanje in preusmerjanje klicev.

- **Trženje preko radia**

Radio je zelo razširjen medij. Oglas potrošnika informira o izdelku ali storitvi, nakupu, o naročilu blaga, ali kje so na voljo dodatne informacije.

- **Trženje preko televizije**

Do neposrednega stika s potrošniki lahko pridemo na tri načine. Pri predstavitvi izdelka se gledalcem ponudi *telefonsko številko*, preko katere lahko naročajo. Podobno je na *programih*, ki so namenjeni prodaji izdelkov. Oglasi so tam nekoliko daljši. Pri trženju preko *teleteksta* ima potrošnik možnost naročanja preko televizije, ki je s kablom povezana s prodajalčevo računalniško bazo.

- **Neposredno trženje v časopisih in revijah**

Oglasi z različnimi ugodnostmi bralce spodbujajo k nakupu izdelkov ali storitev. Navedeni so tudi telefonska številka, naslov ali informacija o naročilu in dostavi.

- **Elektronska prodaja**

Globalnost, dostopnost, preprostost, personifikacija in široka ponudba so lastnosti interneta, ki močno vplivajo na rast prodaje preko interneta. Potrošnik doma dobi veliko informacij, naroči in plača izdelek ali storitev ter naroči njeno dostavo brez večjih stroškov.

- **Trženje preko nakupovalnih avtomatov**

To so samostojni elektronski avtomati, ki stojijo v trgovinah in dopolnjujejo ponudbo, še več jih stoji v različnih ustanovah (bolnice, fakultete, šole, podjetja, železniška postaja). V avtomat s pritiskom na gumb vnesemo naše zahteve po izdelku, ki ga želimo, in ga plačamo z bankovci.

Zgoraj opisani načini so samo čiste oblike neposrednega marketinga, možne so tudi različne kombinacije posameznih oblik, kot sta telefonska in elektronska prodaja.

2 NEPOSREDNI MARKETING NA INTERNETU

Začetki interneta segajo v pozna 60. leta. Nastal je kot omrežje, ki je bilo sposobno na enotnem protokolu združevati naprave različnih proizvajalcev. Sprva so ga uporabljali le v akademskih in vojaških krogih. Razvoj svetovnega spleta (World Wide Web) v letu 1993 je povzročil dramatično rast uporabe interneta tudi na drugih področjih. Internet je postal komercialne narave in orodje, ki je prijazno uporabnikom ter omogoča hitro in preprosto iskanje informacij. Vnesel je nove dimenzije v razumevanje neposrednega marketinga in nove načine dostopa do potrošnika.

Z globalizacijo se zaostruje konkurenca, ki spodbuja težnjo po zniževanju cen, stroškov in uporabi globalnih medijev. V času recesije podjetja vse bolj iščejo notranje vire za zniževanje stroškov, zato se nekatera odločijo za neposredni marketing na internetu. Poznavalci pripisujejo internetnemu marketingu velik potencial, ki s svojimi lastnostmi prehiteva celo klasični neposredni marketing. Menijo, da je internet kot medij hitrejši, cenejši, nudi možnost prilagajanja posamezniku in takojšen odgovor, omogoča graditev kvalitetne baze podatkov ter bolj intenzivno interaktivnost med potrošnikom in ponudnikom. Roberts v svoji knjigi takole opiše povezavo med internetom in neposrednim marketingom: “Internet je raj za neposredni marketing, nudi interaktivnost in direkten dostop do informacij od doma” (Roberts et al., 2001: 4).

Klasični neposredni marketing še vedno predstavlja večji delež na trgu, čeprav mu napovedujejo zaton zaradi interneta. Raziskave kažejo na močno širitev interneta in e-trga v ZDA. Leta 1999 je imelo 97 milijonov ljudi v ZDA dostop do interneta in kar 47 % odraslih je uporabljalo svetovni splet. Predvidevajo, da bo število dostopov v letu 2005 naraslo na 1 milijardo uporabnikov interneta. Izkupiček internetnega marketinga na področju prodaje med podjetji kaže na trend rasti. V letu 1998 je bila vrednost prodaje 43 milijard dolarjev, v lanskem letu naj bi ta narasla na 1,3 trilijona dolarjev (Forrester Research in Nielsen Media Research v Roberts et al., 2001: 4).

Podatki kažejo, da internet prispeva k dodatni vrednosti neposrednega marketinga in k bolj razviti informacijski družbi z večjim nadzorom. Razvili so se novi načini dostopa do posameznega potrošnika in nove oblike sporočil prilagojenih posamezniku, ki omogočajo celovito zadovoljitev njihovih potreb in zadovoljstvo obeh strani. Žal pa internet povzroča vse večjo transparentnost v zasebnosti in varnosti posameznika. Zbiranje osebnih podatkov,

njihovo obdelovanje in posredovanje, pošiljanje nezaželenih e-sporočil in virusov postajajo vsakdanja praksa. Kdorkoli lahko razpolaga z našimi osebnimi podatki in kdorkoli nam lahko pošlje e-sporočilo.

Etika na internetu je resnično postala vse bolj pereča tema, zato so številna združenja napisala določbe za etično poslovno rabo, da bi vsi odnosi temeljili na poštenosti, nevsiljivosti in brez prevar. Priloga A navaja DMA določbe, ki so bile osnovane zaradi enormih primerov neetičnega vedenja neposrednih oglaševalcev.

2.1 Načini oglaševanja na internetu

Lastna spletna stran

Uspešna podjetja in prodajalne svoje spletne strani oblikujejo izrazito marketinško, uporabno in prijetno na prvi pogled. Obiskovalce želijo že na začetku navdati z dobrimi občutki o blagovni znamki in podjetju kot celoti in privabiti k izbiri njihove strani v prihodnje. Spletne strani nudijo informacije o storitvah in/ali izdelkih, njihovi kvaliteti, uporabnosti, prednosti pred drugimi artikli in včasih celo ceni, ali pa napišejo naslov in kontaktno osebo za dodatne informacije ali naročila. Da bi potrošnikom prihranili čas in naredili nakup čim bolj prijeten, spletne strani omogočajo nakup izdelka in plačilo ter povezavo na druge sorodne spletne strani. Glede na to, da trend kaže na porast prodaje preko interneta, predstavlja možnost prodaje na internetni strani velik potencial za podjetja, kjer narava izdelka dopušča takšen način prodaje.

Tuja spletna stran

Običajno se ponudniki podobnih izdelkov ali storitev dogovorijo za navzkrižne povezave. Določena spletna stran omogoča povezavo na drugo in obratno. Kadar ima ena od povezanih strani več obiskovalcev, morajo običajno druge manj obiskane spletne strani plačati za gostovanje (referral fee)[1].

Iskalnik

Večina uporabnikov pride do želene spletne strani z uporabo iskalnikov. Po vpisu iskane informacije se izpišejo vsi relevantni zadetki. Raziskava Forrester Research kaže, da je v letu

[1] Referral fee - je določen znesek od prodaje, če je potrošnik prišel do izdelka preko povezave iz tuje spletne strani.

2001 obstajalo na spletu približno 800 milijonov strani. AltaVista kot največji iskalnik jih je imel registriranih okoli 150 milijonov (Korper in Ellis, 2001: 45).

Elektronsko sporočilo (e-mail)

Oglaševanje z e-pošto je najbolj efektivno, če je pošta poslana točno določeni oz. ciljani skupini potrošnikov, ki je zainteresirana za izdelek ali storitev. Nezaželena in nepričakovana sporočila so za večino potrošnikov nadležna in v posameznih državah prepovedana. Pridobljeno potrošnikovo dovoljenje za pošiljanje e-sporočil je idealna rešitev za občasno obveščanje o novostih, dogodkih in drugih informacijah ter za vzdrževanje dobrega odnosa.

Pop-up

Imenovan tudi oglasno okno, ker se pojavi v obliki vmesnega okna. Pop-upi se odpirajo ob brskanju po spletnih straneh, največkrat se pojavljajo pri nalaganju novih strani. Za uporabnike je takšna oblika oglaševanja zelo moteča, saj je treba oglasno okno s klikom nanj zapreti.

Banner (pasica)

Med brskanjem po straneh opazimo na stotine majhnih svetlikajočih oglaševalskih sporočil. Samo en klik na takšen oglas, trenutek in že smo na drugi, običajno sorodni strani. S tem je naloga bannerja opravljena. Bannerji so zaradi številnosti eni najbolj vsiljivih oglaševalskih sredstev na internetu. Kljub nadležnosti raziskave kažejo, da ima banner takšen učinek na zavedanje blagovne znamke pri potrošnikih kot oglas na televiziji. Tudi če se izognemo bannerju, se ne moremo izogniti njegovemu sporočilu. (Korper in Ellis, 2001: 52).

Druge oblike spletnega oglaševanja

Plavajoči oglas - oglas različne velikosti se premika po spletni strani na trasparentni podlagi.

Celostranski oglas - imenovan tudi oglas »prevzema«, ker nenadoma prekrije celotno spletno stran.

Oglaševalski odmor – imenovan tudi »intromercial« ali »webmercial«, se pojavi ob spremljavi glasbe z vstopom na novo spletno stran. Banner se razširi čez celo spletno stran.

Razširjeni banner - vsiljivi banner želi čim bolj vzbuditi našo pozornost, zato je običajno v obliki plavajočega oglasa in prekrije del spletne strani. Interaktivnost je zelo izrazita.

Tapetni oglas - oglasno sporočilo je v obliki majhnih simbolov, ki prekrijejo ozadje spletne strani. Kadar v takšni obliki oglašuje manj znano podjetje, tapetni oglas spremlja dodatno sporočilo.

100K vljuden bannner – »obzirna« vsiljivost interaktivnega bannerja kjub njegovi prisotnosti dopušča nemoteno branje besedila na spletni strani.

2.2 E-mail marketing kot del neposrednega marketinga

Roberts v svoji knjigi takole opiše začetek e-mail marketinga: "E-milenium, začetek 21. stoletja in s tem tudi prehod neposrednega marketinga iz papirnate v elektronsko obliko preko interneta"(Roberts et al., 2001: 1).

Večina poznavalcev pripisuje e-mail marketingu velik potencial v prihodnjem obdobju. Zaradi cenenega in enostavnega pošiljanja e-pošte je prilagodljivo in osebno e-sporočilo postalo pomembno komunikacijsko orodje, ki omogoča hitro pošiljanje več tisočim uporabnikom željnih novih informacij in ne zahteva veliko truda pri odgovorih.

Prednost e-mail marketinga je v hitrih in cenejših oglaševalskih kampanjah in meritvah učinkovitosti posameznih akcij. Meritve namreč ne zahtevajo dragih raziskav, ampak le enostavno testiranje. K uspešnosti e-kampanje preko e-sporočil pripomore internetna stran podjetja, katere povezava je na voljo v oglaševanem sporočilu. Število obiskov lastne spletne strani je že prvi mehanizem za določanje odzivnosti prejemnikov (Roberts et al., 2001: 113).

Pomembno vlogo ima seznam prejemnikov, ki ga je treba vestno ažurirati. Največji učinek se doseže s pošiljanjem že obstoječim strankam, strankam, ki so v to privolile in želijo pridobiti čim več informacij o izdelkih ali storitvah podjetja.

E-sporočila oglaševalskih kampanj lahko uporabljamo v različne namene. Z njimi seznanjamo potrošnike o novostih, cenah, posebnih ugodnostih, izobraževanjih in še bi lahko naštevali. Predvsem želi vsako podjetje opomniti nase oz. na svojo prisotnost na trgu, čim večkrat stopiti v stik s potencialnimi kupci, v njih graditi zaupanje in dobro mnenje in si s tem pridobiti zvestega kupca.

2.3 Značilnosti e-mail sporočil in njihovo pošiljanje

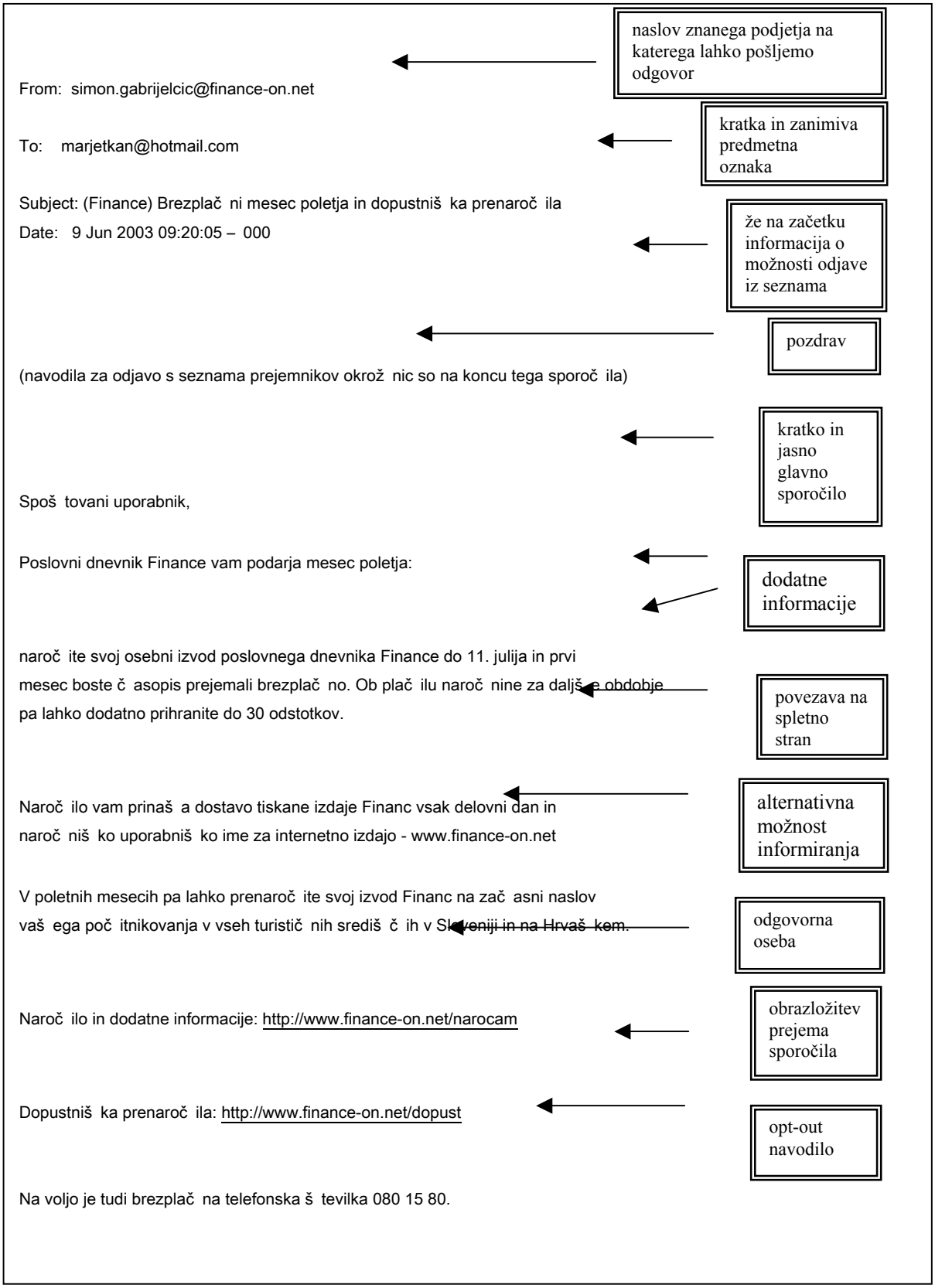
Pri oblikovanju in pošiljanju e-sporočil se moramo držati že preizkušenih pravil, drugače jih prejemniki označijo kot vsiljive in brez vrednosti ter jih izbrišejo, ne da bi jih prebrali. Ob takšnem ravnanju namen sporočila ni dosežen. Chaffey v svoji knjigi navaja pet lastnosti elektronskega sporočila (glej po Chaffey et al., 2001: 234):

- relevantnost in targetiranost komunikacije elektronskih sporočil,
- pravočasnost vzpostavljanja kontakta,
- personalizirana vsebina sporočila,
- avtomatičnost odgovorov naj bo izjema,
- možnost »opt-out«[2].

Elektronska sporočila je vredno pošiljati samo takrat, ko ocenimo, da ima vsebina e-sporočila visoko vrednost za potrošnika. Prepogosta sporočila so neučinkovita, ker postanejo prejemniku vsiljiva in še neprebrana izbriše. Kadar potrošnik opazi, da je sporočilo poslalo ugledno podjetje in njegov predmet vzbuja zanimanje potrošnika, bo sporočilo doseglo svoj cilj. »Opt-out« funkcija v e-sporočilih omogoča potrošniku izpis iz seznama in kaže na spoštljiv odnos pošiljatelja do prejemnika.

Odločilno vlogo imajo prve vrstice sporočila, saj delujejo kot naslov v tiskanih medijih. Irelevantne, dolgočasne, dolge in preveč komercialne predmetne oznake sporočila so vzrok takojšnega izbrisa. Avtomatično so običajno izbrisana tudi sporočila, ki vsebujejo v opisu predmeta besedo “free”, ker večina filtrov e-pošte označi takšno sporočilo kot spam[3]. Najbolj učinkovita so kratka sporočila, ki že v prvem odstavku povedo, za kaj gre, imajo povezavo na spletno stran in vsebujejo navodilo, kje in kako se prejemnik odjavi od prejemanja takšnih sporočil (glej sliko 2.1).

[2] Opt-out – potrošnik želi, da ga pošiljatelj izbriše iz seznama in v prihodnje ne dobiva več sporočil. Opt-out opcija je običajno na razpolago v elektronskih sporočilih.
[3] Spam – neželena pošta - nezaprošena pošta v internetu, ki jo prejemnik pogosto smatra za nezanimivo šaro (Meše 2003, 182).



Slika 2.1. Primer nevsiljivega e-sporočila, Vir: (2003) e-pošta Finance, Ljubljana.

Seznami elektronskih naslovov

Elektronska sporočila pošiljajo podjetja na naslove iz lastne baze podatkov ali na naslove kupljene pri posrednikih[4], ki imajo kot primarno dejavnost posredovanje seznamov e-naslovov. Izbirati je mogoče med več kot 1000 e-seznami[5] različne kvalitete. Največji problem predstavljajo »spam seznami«, v katere so naslovi zbrani na nelegitimen način in pri prejemnikih povzročajo nejevoljo, ker so nepričakovani in neželeni. Internetnim oglaševalcem zagotavljajo velik uspeh »opt-in«[6] seznami, v katere se potrošniki vpišejo prostovoljno, niso pa še ničesar kupili. Zagotovo so najbolj uspešni seznami naslovov tistih potrošnikov, ki so že kupovali oz. pozitivno odgovarjali na ponudbe, prejete po e-pošti. Kvalitetni e-seznami poleg e-naslovov nudijo še druge osebne in demografske podatke o potrošnikih, ki jih pridobijo z večkratnim kontaktom, branjem log poročil[7] ali na načine, opisane v spodnjem odstavku. Takšne sezname nudijo zanesljiva podjetja oz. posredniške pisarne in zagotavljajo 100-odstotno dostavo in ažurnost. Kvalitetni seznami se običajno ne prodajajo, ampak razpošljejo sporočila posredniki sami, tako da ni možno kontrolirati, koliko je neveljavnih in koliko je podvojenih e-naslovov.

Drugi načini zbiranja informacij

Pošiljatelji pridejo do informacij z izmenjavanjem podatkov z drugimi pošiljatelji. Do izmenjave prihaja tudi s podjetji, ki v zameno ponujajo svoje izdelke ali storitve.

Kolaboracijsko filtriranje – to so programi, ki merijo vidik internetne aktivnosti, zbirajo demografske podatke, podatke o nakupovalnih navadah in druge podatke, pomembne predvsem za oglaševanje. Filtriranje bazira na ljudeh s podobnim obnašanjem in omogoča personalizirano ponudbo. Na primer, ponudba knjig: kupimo knjigo Stopping spam, čez en teden nas preko e-pošte sprašujejo o zadovoljstu in hrati priporočajo v branje knjigo z naslovom Marketing with e-mail.

Closed-loop marketing (marketing zaprte zanke) – za to tehniko je potrebna uporaba piškotkov za sledenje uporabnikom interneta. Omrežje DoubleClicka je eno prvih podjetij, ki spretno izrablja closed-loop marketing. Že vnaprej določi in shrani banner prilagojen stranem,

[4] Posredniki –ang. Email Service Bureau
[5] E-seznam – elektronski naslovi zbrani v seznamih.
[6] Opt-in – vpis v seznam na določeni spletni strani, da se strinjamo s prejemanjem oglaševalskih sporočil kateregakoli podjetja.
[7] Log poročilo – zabeležka o aktivnostih in dogodkih v računalniku

ki jih pregleduje uporabnik. Alternativno lahko DoubleClick pošlje uporabniku interneta tudi e-pošto, v primeru, da ima njegov e-naslov.

Pošiljanje e-sporočil

Pošiljatelji e-sporočil lahko izbirajo med dvema programoma za količinsko pošiljanje sporočil, lahko pa to opravilo prepustijo že omenjenim pisarnam. Strežnik seznama (listserver) je najboljši program, ki lahko pošlje sporočila na naslove v e-seznamu. Program omogoča, da se potrošniki sami vpišejo ali izbrišejo iz seznama. Poenostavljeno pošiljanje poteka avtomatično. Neveljavne naslove tudi briše sam, tako da ne pošiljamo v prazno. Pošiljateljeva naloga je samo dati znak strežniku seznama za pošiljanje, program prebere napisani ukaz in pošlje sporočilo na e-naslove iz seznama. Po končanem procesu strežnik seznama[8] obvesti pošiljatelja, katero sporočilo je bilo poslano in koliko ljudi iz seznama je prejelo sporočilo.

Dobro znani vendar neželeni so programi za množično pošiljanje e-sporočil (bulk e-mail program). Onemogočeni so ažurnost in avtomatski vpis ali izbris iz seznamov, katere uporabljajo predvsem za pošiljanje spama.

2.4 Obetajoč uspeh marketinga z dovoljenjem – opt-in marketinga

Zaradi koncentracije sporočil, poslanih po internetu, ki postajajo vedno bolj agresivna in neprijetna za prejemnika, je DMA proti spamu skupaj z odvetniki že v letu 1998 uvedla in opredelila pojem »opt-in«, ki pravi takole: “Opt-in se izvaja, ko potrošniki potrdijo in ne prekličejo želje po prejemu e-sporočila” (Roberts et al., 2001: 150). Opozarjali so pošiljatelje sporočil, naj ne bodo vsiljivi in nadležni ter naj spoštujejo potrošnike. Vsa opozorila so očitno naletela na gluha ušesa, ker se količina neželene pošte nenadzorovano množi.

Nekateri tržniki napovedujejo, da je prihodnost uspešnega elektronskega poslovanja v teoriji treh C-jev (Roberts et al., 2001: 207):

trgovina (Commerce),
zadovoljstvo (Content),
skupnost (Community).

[8] Strežnik seznama – avtomatizirani e-poštni system, ki pošilja isto sporočilo na več naslovov hkrati.
[9] Strežnik seznama – avtomatizirani e-poštni system, ki pošilja isto sporočilo na več naslovov hkrati.

Teorija zagotavlja uspešnost poslovanja ob izpolnitvi vseh treh C-jev. Za uspeh mora torej biti spletna stran prijazna vsem potrošnikom, jim nuditi informacije visoke vrednosti, le tako bo uporabnik zadovoljen in bo vzpostavil dober odnos s spletno stranjo ter posredno s ponudnikom. Za skupnost so nujno potrebni dobri odnosi med ponudnikom in potrošnikom. Dobra informiranost, zadovoljstvo, občutek pripadnosti in povezanost potrošnikov so elementi, ki vzpodbujajo k takojšnemu nakupu preko spletne strani.

Chaffey in soavtorji navajajo, da bo v prihodnje nujno vzpostaviti ravnotežje: "Narava marketinga, ki bo v prihodnje učinkovita na internetu, bo zahtevala vzpostavitev ravnotežja med koristmi posameznika oz. podjetja in ogroženostjo potrošnika. Ponudniki bodo morali upravljati le z informacijami, ki jih bo potrošnik pripravljen dati na razpolago podjetjem" (Chaffey et al. 2000, 465). Dejanski podatki tudi kažejo na visoko stopnjo odzivnosti na želena sporočila. Green, pomožni direktor podjetja Hearst Publishing, trdi, da je stopnja odgovorov na elektronska sporočila poslana potrošnikom prostovoljno vpisanim v seznam 20-ali več odstotna (Green v Roberts et al. 2001, 69).

Večina teorij in raziskave kažejo, da je potencial e-marketinga osnova, ki bazira na privoljenju potrošnikov. Agresija ne gradi dolgotrajnih in uspešnih odnosov. Potrebno je potrpljenje, vztrajnost, spoštovanje in upoštevanje vseh dejavnih udeležencev v odnosu. Veliko je govora, kaj je »opt-in« in kdaj se krši to načelo. Prerekanja so odvečna. Treba je le razumeti besedi »opt-in«, ki pomeni »odločiti se za nekaj«, in »opt-out«, ki pomeni »odločiti se proti«, ter prisluhniti željam potrošnikov, ko se odločijo za nekaj in se pozneje odločijo proti temu. Trgovina na internetu bi zagotovo bolj zaživela, če bi vsi pošiljatelji spoštovali ti dve pravili in bi maso podatkov, ki jih omogoča globalnost medija, uporabili v dobre namene. Koncentracija vsiljivih sporočil je postala tako velika, da so potrošniki razvili obrambni mehanizem, ki zavira pričakovani uspeh direktnega marketinga na internetu. Paul Soltoff napoveduje e-pošti črno prihodnost in lastno uničenje, če se stanje ne bo spremenilo in se pošiljatelj in prejemnik ne bosta zbližala. Kljub vsemu pa nekateri strokovanjaki napovedujejo pomembnost konvergence: "Dosegli bomo integracijo glasu in slike z e-sporočilom za večjo varnost, avtentičnost in pošiljanje sporočil. Boljša kompatibilnost e-sporočila s telefonom in televizijo, bo povzročila vsakdanjost interaktivnih sporočil. Uporaba bo enormno narasla" (Soltoff, 2003: http://www.clickz.com/em_mkt/em_mkt/article.php/2168761).

3 SPAM – OBLIKA NEPOSREDNEGA MARKETINGA

Beseda spam označuje e-sporočila, ki povzročajo vse več slabe volje med prejemniki. Nekateri ga označujejo s kraticama UCE (unsolicited commercial e-mail) ali UBE (unsolicited bulk e-mail), v paketih e-pošte se imenuje tudi »junk mail«. Vsa imena skupaj dobro označujejo glavne lastnosti spama: je nenaprošeno e-sporočilo, poslano množici prejemnikov, z nizko vsebinsko vrednostjo, ki je običajno komercialne narave. Izvor besede ni povsem jasen. Nekateri trdijo, da so tovrstna sporočila dobila ime po mesu v pločevinkah (Spiced Pork Ham), drugi po skeču, ki je bil predstavljen v Letečem cirkusu Monthy Payton 1970, v katerem skupina Vikingov poje »spam, spam, spam, …«.

3.1 Opredelitev spama

Kaj je spam? Vsaka organizacija in vsak posameznik imata svojo definicijo. Najbolj efektivna je prav gotovo tista, na osnovi katere jasno ločimo spam od drugih e-sporočil, določimo probleme, ki jih povzroča, in ga reguliramo z zakonom.

Schwartz in Garfinkel definirata spam kot nezaprošeno in neželeno sporočilo, ki je poslano osebi brez njenega dovoljenja. “Spam je skupek internetne različice »junk maila«, telemarketinškega klica v času kosila, neumnega telefonskega klica in nalepljenega letaka v mestu, ki predstavlja elektronsko nadlogo” (Schwartz in Garfinkel, 1998: 1).

“Spam preplavi internet s številnimi kopijami istega sporočila, ki se proti volji uporabnika e-pošte pojavi v njegovem e-poštnem predalu. Večina spamov ima oglaševalsko vsebino za izdelke in storitve vprašljive kvalitete. Stroške nosi predvsem prejemnik in prenosnik e-pošte, pošiljateljevi stroški so zanemarljivo nizki”.
(Müller, http://spam.abuse.net/overview/whatisspam.shtml).

Organizacija Brightmail opredeljuje spam kot nenaprošeno, komercialno ali sporno sporočilo, pogosto poslano na naslove pridobljene na nelegalni način (Brightmail, 2002: www. brightmail.com).

Veliko avtorjev definira spam tudi s kraticama UCE in UBE, ki ravno tako kot druge definicije ne opišejo spama v celoti. Nekatere organizacije celo trdijo, da obstaja bistvena razlika med spamom in UCE. Razlikoval naj bi ju način, na katerega so pridobljeni e-naslovi,

kot trdijo nekateri. Vseeno pa je rezultat, ne glede na prejšnje faze postopka, še vedno isti – vznemirjeni in ogorčeni prejemniki sporočil ter težave v sistemih, ki prenašajo e-pošto.

Največja francoska delodajalska organizacija MEDEF[10] celo razlikuje med dvema vrstama UCE-jev. Trdi, da oglaševalskega sporočila poslanega zgolj zaradi poslovanja s stranko, s katero je podjetje že imelo stik, nikakor ne moremo označiti kot nezaprošeno komercialno sporočilo (Gauthronet in Drouard, 2001: http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamstudy_en.pdf).

Soltoff je definiciji spama namenil malo več pozornosti. Meni, da le smiselna opredelitev spama pomaga pri določanju problemov, ki jih povzroča, in trdi, da je spam elektronsko sporočilo, ki ga lahko le prejemnik – in samo prejemnik – označi kot neprimernega, nezaželenega in nič več želenega iz kakršnegakoli razloga (Soltoff, 2002: www.clickz.com/em_mkt/em_mkt/article.php/1492521).

Slovenski zakon in direktive EU se ne ukvarjajo z opredelitvijo spama, ampak le omejujejo njegovo pošiljanje. Zakon posameznih ameriških držav in nekateri osnutki zakona na zvezni ravni spam definirajo kot UCE, ki je poslan osebi, s katero pošiljatelj še ni imel niti osebnega niti poslovnega stika in nima dovoljenja ali naročila prejemnika za pošiljanje. UCE pa definirajo kot e-sporočilo z oglaševalsko vsebino za zakup, prodajo, izposojo, darila, ponudbo ali druge vrste sporočil, kjer je jasno vidno, da gre za lastnino, izdelke ali storitve (Alaska statutes, 2003: http://www.spamlaws.com/state/ak.html).

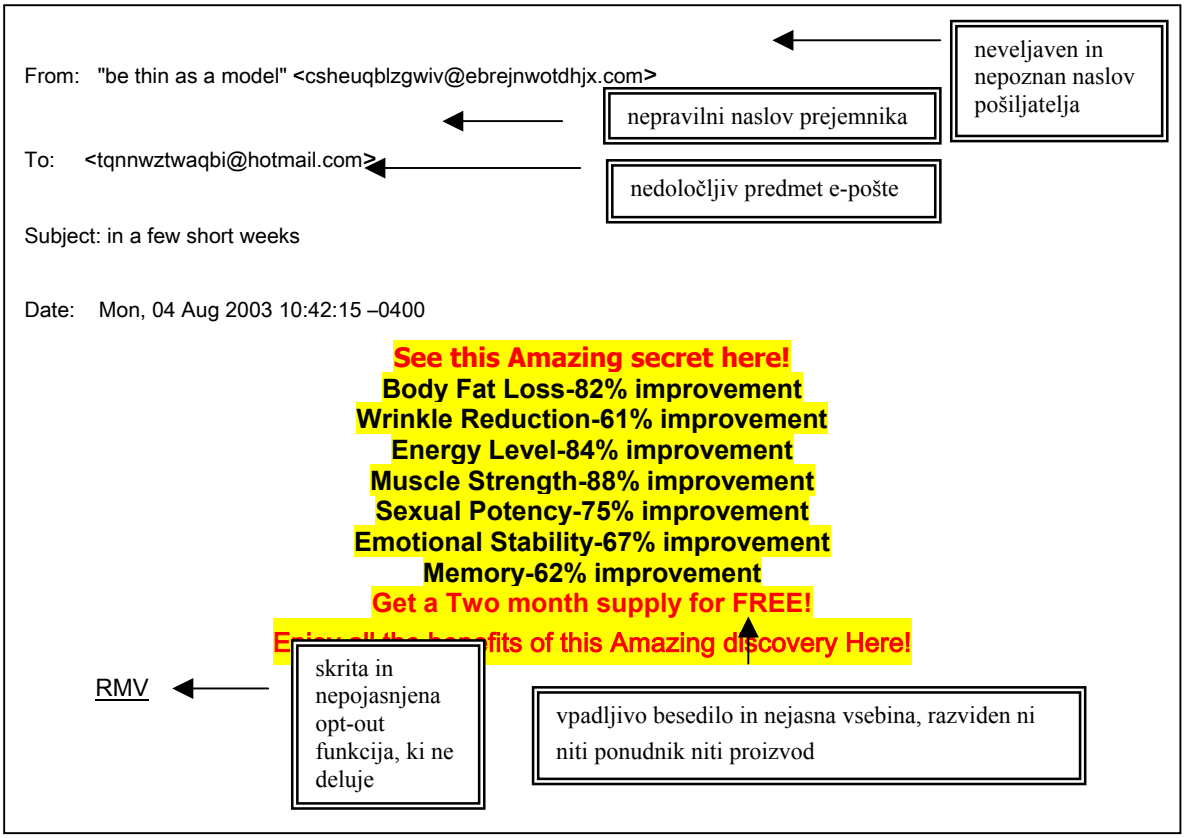
Soltoffova definicija še najbolj celovito opiše spam. Res je, da je prejemnik tisti, ki nadležna e-sporočila označi kot spam, vendar se slabost definicije kaže v neoziranju se na druge udeležence, ki trpijo zaradi blokad in visokih stroškov, ki jih povzročajo enormne količine e-sporočil. Po določeni količini e-sporočil verjetno tudi želena sporočila postanejo spam. Ravno količina je tisti dejavnik, zaradi katere je spam v zadnjem času ena najbolj perečih tem in povzroča težave pri razvoju in uresničevanju zastavljenih ciljev e-mail marketinga.

Značilnosti spama

Neznani in neobičajni naslovi pošiljateljev ter predmetne oznake polne klicajev in drugih ločil, ki navajajo edinstvene priložnosti in nenatančno opisane izdelke ali storitve, so atributi, ki ločijo spam od drugih e-sporočil. Vsebina spamov je običajno zelo kratka, nejasna in ne

[10] MEDEF: Mouvement des Entreprises de France

vključuje informacij visoke vrednosti za prejemnika. Besedilo e-pošte je skromno, gre bolj za navajanje nikoli uresničljivih obljub in vsebuje številne slovnične napake (glej sliko 3.2). Glavni pojmi, ki so tesno povezani s spamom, so: kršenje zasebnosti, nelegalnost, neprijetna vsebina, zavajanje in varljive ponudbe.



Slika 3.2: Primer vsiljivega e-sporočila, Vir: (2003) spam.

Elektronska pošta kot prenosni medij

E-sporočilo je funkcija interneta, ki omogoča uporabnikom prejemanje in pošiljanje sporočil preko svetovnega spleta, ki povezuje vse internetne ponudnike. Ponudniki zaradi medsebojne povezanosti omogočajo tudi storitve tretjih ponudnikov. Torej je glavna funkcija ponudnikov interneta in e-sporočil omogočanje potrebne infrastrukure za pošiljanje in sprejemanje e-sporočil.

Obstajajo štiri osnovne komponente email sistema: »Mail Transport Agent« je komponenta, ki skrbi za prenos e-sporočil od pošiljatelja do prejemnika. Pogosto je »email sistem« sestavljen iz več MTA-jev. Mail User Agent (MUA) je vmesnik, ki ga uporabljajo končni

uporabniki za pošiljanje in dostop do sporočil. Dodatno je še Mail Filter Agent (MFA) komponenta, ki se jo uporablja za filtriranje e-sporočil. Mail Storage Agent (MSA) je komponenta, ki skrbi za shranjevanje.

Internetni »email sistem« omogoča »slepo« in množično pošiljanje e-sporočil, ki istočasno dostavi številne kopije sporočil na različne naslove. V končni e-pošti pa niso navedeni naslovi vseh prejemnikov. Sistem deluje tudi, kadar ni razpoznaven naslov pošiljatelja. Zloraba te prednosti omogoča pošiljateljem ponarejanje naslova, iz katerega pošiljajo e-pošto.

3.2 Zgodovina spama

Pionir interneta Jon Postel je že leta 1975 spoznal pomembno pomanjkljivost e-pošte. Menil je, da bo možno istočasno »napasti« računalnik s številnimi sporočili, ki bodo presegla zmožnost računalnika (Schwartz in Garfinkel 1998, 17).

Že v 80-ih se pojavijo prva verižna pisma in z njimi tudi problemi. Po več generacijah so se sporočila tako povečala, da so zavzela v računalniku ves prostor, ki je bil še na razpolago. Številna verižna pisma so pozneje spremljali virusni programi. »Christmas«, eden prvih virusnih programov, je v gostujočem računalniku posnel vse elektronske naslove, na katere je poslal verižno pismo.

Kot vsi drugi internetni fenomeni ima tudi spam kratko razvojno dobo. Univerzitetni profesor Alan Schwartz in svetovalec informacijske tehnologije Simson Ganfinkel dobro opišeta tri glavne mejnike v zgodovini spama (povzeto po Schwartz in Garfinkel 1998).

– *1994: Canter & Siegel in spam »Green Card Lottery«*
  Odvetnika Canter in Siegel sta poslala oglas več kot 6000 novičarskim skupinam preko useneta[11]. Oglas je nudil pravni nasvet za 100 dolarjev vsem imigrantom, ki so zaprosili za delovno zeleno karto, čeprav je bila brezplačna. E-sporočilo je povzročilo veliko ogorčenje med prejemniki, saj so ga prejeli vsi, ne glede na potrebe po zeleni karti. Na tisoče jeznih prejemnikov jima je poslalo pritožbo, tako da so onesposobili delovanje ponudnika interneta, ki jima je zaradi tega preprečil dostop do interneta. Pozneje sta svoje izkušnje o pošiljanju masovne e-pošte opisala v knjigi, ki je močno vplivala na posameznike.

– *1995: Jeff Slaton, »Spam King«*

Zamisel o »spam marketingu« je v zgoraj omenjeni knjigi dobil Slaton. Zbiral je e-naslove posameznikov in novičarskih skupin in si napravil zelo dobro osnovo za pošiljanje oglaševalskih sporočil. Z oglaševanjem načrta za atomsko bombo je zaslužil ogromno denarja. Takšne kampanje je izvajal tudi po naročilu drugih podjetij. Slaton je postal pravi pionir »spam marketinga«, saj je uvedel številne zvijače, ki jih uporabljajo še danes: neresnični e-mail naslovi pošiljatelja, v e-pošti je navedel telefonsko številko telefonske tajnice, izkoriščal je druge strežnike za pošiljanje spama, uvedel je tudi opcijo »opt-out«, čeprav je ni upošteval. Obseg njegovih sporočil je presegel vse meje. Začela se je prava vojna med Slatonom in branilci interneta. Osnovali so črni seznam (Black-Hole List) in vanj vpisali veliko Slatonovih podatkov, da bi prejemniki in filtri e-pošte takoj prepoznali pošiljatelja in mu onemogočili masovno pošiljanje.

– *1996: Sanford Wallace in Cyber promocija*

Wallace je imel svojo domeno, iz katere je po vzoru svojih predhodnikov pošiljal spame v več deset tisočih izvodih. Sam je pobral naslove vseh uporabnikov AOL[12] ponudnika e-pošte in dnevno bombardiral vsakega posameznika s 5 spami. Vrhunec je dosegel s 30 milijoni spamov na dan. Sporne vsebine je pošiljal tudi za druge naročnike. Številne pritožbe so vzpodbudile AOL, da s filtrirnim sistemom zaščiti kršene pravice svojih uporabnikov. Wallacovi spami zaradi filtrov niso dosegli prejemnikov. Tožil je AOL zaradi kršitve prvega zakona Amerike – svobode govora in na koncu tožbo izgubil. Začel si je izposojati druge domene in iz njih pošiljati spame, kar ga je na koncu veliko stalo.

3.3 Vrste spama

Veliko je načinov, po katerih lahko klasificiramo spam. Razvrščamo ga glede na pošiljatelja, prenos, vsebino in na motiv pošiljanja. Najbolj obči sta razvrstitvi po vsebini in načinu prenosa.

Organizacija FTC[13], ki se zavzema za pravice potrošnikov, razvršča spame v 12 kategorij glede na vsebino. Analizirali so 250.000 sporočil, na katere so se prejemniki pritožili in identificirali skupine: (FTC, 1998: www.ftc.gov):

[11] Usenet – glavno omeržje novičarskih skupin, ki so dosegljive v internetu.
[12] AOL – American Online je največji ponudnik storitev e-pošte
[13] FTC – Federal Trade Commission

- piramidne sheme, ki obljubljajo velik zaslužek za majhno investicijo,
- nagovarjanje in pridobivanje novih »spamerjev«[14],
- verižna pisma,
- delo na domu,
- goljufive ponudbe zdravstvenih nasvetov in dietnih predlogov,
- nelegitimne ponudbe menjalniških tečajev,
- prazne obljube, da plačilo članarine omogoča brezplačne izdelke,
- izmišljene investicijske priložnosti,
- ponudbe različnih oprem, orodij, ki običajno ne delujejo,
- ponudbe ponarejenih kreditnih kartic,
- lažne obljube o prenosu kreditov na nove kreditne kartice proti plačilu,
- ponudbe počitniških aranžmajev.

Tej klasifikaciji so dodane še igre na srečo in pornografske vsebine. Pornografska sporočila so se močno razširila v zadnjem času in predstavljajo kritično točko v nespoštovanju otrokovih pravic.

Schwartz in Garfinkel razvrstita spame glede na prenos sporočila v dve skupini: email spam in usenet spam. Slednji predstavlja komunikacijo »eden na mnoge« oz. vsako e-sporočilo je posredovano vsem novičarskim skupinam, dosegljivim na internetu. Samo eno takšno sporočilo je v trenutku poslano več deset tisočim uporabnikom in s tem povzroči težave različnim sistemom, ki podpirajo prenos sporočil. V to skupino prištevata prekomerno multi-pošiljanje in navzkrižno pošiljanje, izmečke (spew), sporočila z neresnično vsebino, dvojna sporočila in komercialna sporočila. K spamom uvrščata še UCE, UBE, sporočila za hitre zaslužke in napade na ugled.

3.4 Viri e-naslovov

Celotni proces pošiljanja spamov se začne pri zbiranju e-naslovov. Nekateri spamerji naslove pridobijo z odkupom legalnih ali nelegalnih seznamov e-naslovov, drugi uporabijo svoje znanje za kreiranje programov, s katerimi na različne načine in na različnih lokacijah pobirajo naslove. Zaradi neveljavnosti že zbranih naslovov in zastarelosti seznamov, se večina pošiljateljev odloči za lastni seznam.

[14] Spamer – pošiljatelj spamov

3.4.1 Usenet

Spamerji neprestano oblegajo usenet, ki omogoča, da sporočilo v kratkem času doseže veliko število uporabnikov, ki imajo enake interese. Usenet novice so osnovane na prispevkih oz. člankih, organiziranih v novičarske skupine. Hierarhičnost skupin postavlja najširši pojem na začetek. Npr. novičarska skupina »*comp.lang.C++*« je prispevek o računalniškem programskem jeziku C++. Hierarhična struktura omogoča, da vsak uporabnik interneta brez težav najde novičarsko skupino, ki je v njegovem interesu. Za sodelovanje v novičarskih skupinah je potreben poseben program, ki deluje na istem principu kot e-pošta.

3.4.2 Direktna sporočila

Direktna sporočila so pomembna za spamerje iz dveh razlogov: predstavljajo vir e-naslovov in kanal za pošiljanje nezahtevanih oglasov. V primerjavi z usenet sporočili ali spletnimi stranmi, iz katerih so naslovi »pobrani« zelo hitro, predstavljajo direktna sporočila manjši vir naslovov. Drugi dve lastnosti direktnih sporočil spamerjem omogočata pridobitev veljavnih naslovov in pomembnih informacij, ki pomagajo pri oblikovanju bolj targetiranih sporočil.

IRC (Internet Rely Chat) – spletni klepet

V 80-ih se pojavijo prvi začetki IRC-a, ki bazira na sistemu odjemalec-strežnik. Vsi vključeni v spletni klepet so priključeni na IRC strežnik preko IRC odjemalca. Na začetku prvi uporabnik definira oz. kreira kanal (npr. narava), da vsi udeleženci poznajo rdečo nit pogovora. Oseba, ki kreira kanal, ima tudi med klepetom možnost, da neprimerne sogovornike izključi iz sistema. Vsako sporočilo na odjemalcu doseže vse druge odjemalce, ki so priključeni na strežnik. IRC sistem omogoča simultani klepet med množico ljudi iz celega sveta, kadar je IRC strežnik povezan z drugimi strežniki.

ICQ

Tudi ICQ sistem je osnovan na odjemalec-strežnik principu. Vsak udeleženec se mora najprej registrirati na strežniku Mirabilis, da dobi svojo IRC številko. Ob registraciji je treba vpisati v seznam svoje podatke, ki so spamerjem še kako zaželeni. Za razliko od drugih direktnih sporočil je IRC strežnik potreben le pri vzpostavitvi povezave med uporabnikoma, nadaljnja sporočila potekajo direktno od enega na drugega odjemalca.

3.4.3 Formularji

Skoraj vedno, kadarkoli želimo priti do želenih informacij, se naročiti na elektronske novice ali kupiti izdelek, moramo izpolniti obrazec. Večina obrazcev zahteva od uporabnika precej informacij od osebnih do demografskih, nekateri celo zahtevajo vpis posameznikovih interesnih dejavnosti. Organizacije, ki nočejo škodovati svojemu ugledu, takšne podatke resnično uporabijo le za svoje potrebe oz. za interakcijo s stranko. Določba o nezlorabljanju in o neposredovanju informacij tretjim osebam je jasno napisana v njihovem pravilniku, največkrat pa kar poleg obrazca, katerega izpolnjuje obiskovalec spletne strani. Organizacije, ki izkoriščajo pridobljene podatke svojih strank in jih uporabljajo za druge namene ter celo prodajajo tretjim osebam brez dovoljenja, običajno napišejo zadržanje te pravice na najbolj neopazno mesto z medlimi črkami.

3.4.4 Verižna pisma

Verižna pisma so napisana iz razloga, da jih prejemnik pošlje vsem znancem in tako dosežejo v kratkem času veliko množico prejemnikov. Sporočila so izmišljena in neresnična. Na različne načine (predvsem čustvene) skušajo prepričati prejemnika, da pošto pošlje čim več znancem. Nagovarjajo k pomoči socialno šibkim in bolnim, svarijo pred računalniškimi nadlogami in verižnimi pismi, obljubljajo hitri zaslužek in srečo v življenju, ponujajo učinkovite računalniške programe za zaščito pred virusi, inteligenčne in drugi teste, sprašujejo po pogrešanih otrocih. S pismi krožijo še peticije, protesti, politični govori, voščilnice za različne priložnosti, šale in legende. Vsebina pisem spodbuja prejemnika k pošiljanju z obljubljanjem večne sreče in denarja, vplivanjem na čustva in k prebujanju sočutja do soljudi.

Največji problem verižnih pisem je možnost njihovega hitrega množenja. Večina ljudi jih pošlje na vse e-naslove svojih prijateljev. Organizacija CIAC[15] je izračunala stroške, ki jih povzroči pošiljanje teh pisem. Predpostavili so, da vsak prejemnik porabi minuto, da pismo prebere in ga pošlje na vse svoje naslove. V izračunu so določili, da vsak prejemnik oz. vsaka generacija posreduje verižno pismo le desetim, tako da se deset pisem iz prve generacije že v šesti generaciji pomnoži na milijon pisem (CIAC, http://hoaxbusters.ciac.org/HBHoaxInfo.html#what):

[15] CIAC - Computer Incident Advisory Capability

1.000.000 ljudi * 1/60 ura * $50/ura = 833.333,3 $

Verižna pisma ne povzročajo samo visokih stroškov, ampak tudi upočasnijo delovanje sistemov, ki podpirajo pošiljanje e-pošte, ali jih celo blokirajo.

Hitro širjenje verižnih pisem med različnimi uporabniki e-pošte je pravi raj za spamerje. V kratkem času lahko pridobijo več milijonov e-naslovov, zato se veriga pisem začne velikokrat pri spamerjih. Najbolj iznajdljivi pismu pripnejo še virus, ki z odprtjem e-pošte avtomatsko pošlje pismo na vse e-naslove, zapisane v prejemnikovem imeniku.

Verižna pisma je moč spoznati že na prvi pogled, saj so za njih značilni zvijačni opisi *predmeta e-pošte*. Običajno ponujajo zaslužek za nič dela, opozarjajo na nevarnosti ali vzbujajo sočutje do umirajočih in trpečih otrok. Z navajanjem izmišljenih ali resničnih odgovornih oseb, organizacij brez njihove vednosti ter tehničnih podatkov želijo *prepričati bralca o resničnosti*. Na koncu *pismo prosi* prejemnika, da ga pošlje na čim več naslovov in mu s tem obljubi srečo v življenju ali visok dobiček. Primer verižnega pisma je v prilogi B.

3.4.5 Cookies – piškotki

Zahteve brskanja zapisane na http protokolu so med seboj neodvisne, zato spletni strežnik ni seznanjen z uporabniškim predhodnim iskanjem in obiskanimi spletnimi stranmi. Piškotek je program, ki ga komunikacijski strežnik pošlje in shrani na disku računalnika. Mehanizem, ki deluje kot zaznamovalec ali identifikator, spletni strežnik prepozna avtomatično. Posredujejo mu informacije o brskanju po spletnih straneh vsakega posameznika. Lahko rečemo, da so piškotki informacije za prihodnjo rabo. Sprva so imeli funkcijo, ki je bila prijazna uporabnikom, danes se je njihova uporaba precej razširila in ogroža varnost in zasebnost uporabnika. Podjetja jih uporabljajo za ugotavljanje števila obiskov spletne strani, posredno lahko tudi ocenjujejo privlačnost in uporabnost strani ter interes za izdelke ali storitve. Piškotki so priljubljeno orodje marketinških podjetij. Omogočajo kroženje bannerjev, prilagoditev spletne strani posameznemu uporabniku tako jezikovno kot izbor ponudbe, glede na njegovo zanimanje ali nakup ob prvotnem obisku strani. Na osnovi številnih informacij, ki jih omogočajo piškotki, podjetja pošiljajo bannerje, pop-upe in e-sporočila, prilagojena posamezniku. Kadar ob nakupu izdelka preko interneta izpolnimo obrazec, piškotek shrani vse vpisane podatke (ime, priimek, e-naslov, telefon, interesi, in druge) ter jih deli z drugimi

strežniki. Dragocenih informacij se poslužujejo številni ponudniki izdelkov in storitev ter spamerji, ki zlorabljajo funkcijo piškotkov in nadlegujejo uporabnike interneta.

3.4.6 Virusi, pajki in parazitski programi

Programi vsebujejo skrite komponente, s katerimi v našem računalniku poiščejo aktivne e-naslove in jih posredujejo zbiralcem naslovov.

Parazitski programi omogočajo zunanjim podjetjem vpogled v navade pri spletnem brskanju, pregledujejo dokumente in uporabljajo neporabljeno procesorsko moč in prostor v pomnilniku. Večina parazitskih programov trenutno le razpečuje usmerjene oglase, žal pa so ti programi sposobni narediti še veliko več. Globoko v drobnem tisku uporabniških pogodb se skrivajo pravni členi, ki programskim podjetjem dovoljujejo nekontroliran dostop do naših računalnikov. Programi se delijo v tri kategorije: »adware«, »spyware« in »prikrita omrežja«. Programi pridejo v naš računalnik kot priponka ob nameščanju nekega drugega programa, ki smo ga kupili. Veliko novejših programov, zlasti brezplačnih, ima navedene pogoje, s katerimi se ne bi strinjali. Zaradi nepozornosti avtomatično kliknemo na »OK« in s tem potrdimo, da se strinjamo z vsemi pogoji, čeprav si podjetja pridržujejo pravico, da lahko kadarkoli delno ali popolnoma dodajo, izbrišejo ali spremenijo funkcionalnost programov v povezavi s prevzetim programom. Zelo znani so primeri iz programa KaZaA. Parazitski programi imajo v računalniku dostop do sistema in vseh datotek na njem. Lahko nadzorujejo tudi našo e-pošto in razpošiljajo njeno vsebino. (Arnes, 2002: http://www.arnes.si/si-cert/obvestila/2002-CIACT.html).

3.4.7 Seznami e-naslovov

Spamerji se poslužujejo različnih seznamov, ki jih je moč dobiti preko spletnih strani. Veliko spam sporočil je poslanih na e-naslove, katerih lastniki so preko »opt-out« funkcije prepovedali nadaljno pošiljanje e-sporočil. Za spamerje »opt-out« funkcija torej pomeni le potrditev veljavnega in še vedno delujočega naslova. Sezname takšnih naslovov prodajajo naprej kot potrjene oz. »opt-in« naslove. »Goljufive« sezname je moč kupiti preko interneta in/ali od propadlih dotcom[16] podjetij. Tretji način pridobivanja seznamov e-naslov je še bolj neetičen in nelegalen. Spamerji oblikujejo programe, ki jim omogočajo pregled spletnih

strani, in iz njih pobirajo e-naslove. Včasih jim celo uspe vdreti v sistem ponudnikov e-pošte ali drugih organizacij, ki imajo dobro urejene podatkovne baze svojih potrošnikov. Legalnih »opt-in« seznamov se spamerji le redko poslužujejo.

3.4.8 Ugibanje e-naslovov

Spamerji kreirajo programe imenovane »dictionary attack«, ki iz različnih seznamov pobirajo imena in priimke. Izberejo si eno pripono oz. domeno, npr. @hotmail.com, za lokalno ime ustavljajo različne kombinacije naključno izbranih imen in priimkov. Ime in priimek napišejo različno: skupaj, narazen, dodajo številko, napišejo le kratice ipd.. Na takšen način spamerji kreirajo tudi do milijon e-naslovov. Nekaj tisoč sporočil zagotovo pride do prejemnikov, nepravilni pa so zavrnjeni na naslov, iz katerega so bili poslani in verjetno ne obstaja več (Ellis in Speed; 2001, 175).

3.4.9 Web bugs (spletni hrošč) v e-pošti

Za pridobivanje in preverjanje pravilnosti e-naslovov s spletnimi hrošči in zapisi e-pošte so usposobljeni le vešči poznavalci (spamerji) sistema e-pošte. Spletni hrošči so nameščeni na spletnih straneh za profiliranje posameznega uporabnika. Ker beležijo poti iskanja na iskalnikih, se uporabljajo predvsem v statistične namene in so dobre smernice oglaševalskim agencijam za izdelovanje internetnih kampanj. Spletni hrošči v e-pošti ne služijo toliko za pridobivanje novih naslovov kot za preverjanje veljavnosti naslovov. Nameščeni so v e-pošto in javijo pošiljatelju ali je prejemnik prebral sporočilo in ali ga je poslal naprej.

3.4.10 Mail logs – zapisi

Kadar pošljemo e-pošto ali jo transportiramo, se kreira zapis e-pošte pri ponudniku, ki omogoča pošiljanje e-pošte. Najpogosteje se na njih zapiše naslov pošiljatelja in prejemnika, čas pošiljanja in predmet e-pošte. Vsebina sporočila iz njih običajno ni razvidna, razen če so zapisi tako programirani. Zapise uporabljajo za oblikovanje seznamov e-naslovov in so dostopni samo strežnikom, na katerih so nameščeni. V primeru slabe zaščite se do njih prikradejo tudi »hekerji«, željni novih e-naslovov. Tako pridobljene naslove uporabljajo za

[16] dotcom podjetje – podjetje, katerega izdelke ali storitve je moč kupiti samo preko interneta (npr. Amazon)

pošiljanje spamov in/ali jih prodajo drugim spamerjem. Druga veja zapisov so spletni zapisi, ki dopolnjujejo zapise e-pošte in se kreirajo na internetnih strežnikih, požarnih zidovih in proksi strežnikih. Vsebujejo informacije o brskanju po spletnih straneh, s katerimi je moč izoblikovati ponudbo, prilagojeno vsakemu posamezniku.

Zanimive lokacije za »pobiranje« e-naslovov

FTC je v letu 2002 izvedel raziskavo, v kateri so na 175 različnih lokacijah »posejali« 250 novih, še neznanih e-naslovov. E-naslove so pustili na različnih spletnih straneh, straneh novičarskih skupin, klepetalnicah, oglasnih deskah, imenikih spletnih strani, seznamih e-pošte in na straneh direktnih sporočil. Želeli so preveriti, katere strani na internetu so najbolj izpostavljene spamerjem. V šestih mesecih, kolikor časa je trajala raziskava, so prejeli kar 3.349 spamov. Rezultati kažejo, da so pravi virtualni magneti klepetalnice. Na vse naslove klepatalnic so bili poslani spami. Posredovani naslov v klepetalnico je prvi spamer »napadel« že po devetih minutah. Spamerjem so mikavne tudi spletne strani in novičarske skupine, saj je večina (86 %) naslovov poslanih na ti dve lokaciji prejelo spam. Polovica naslovov, poslanih na brezplačne osebne spletne strani, je tudi bila izrabljena za pošiljanje spamov. Naslovi, poslani na druge lokacije, niso izpostavljeni spamerjem in so prejeli precej manj neželenih sporočil oz. spamov. Le slaba tretjina (27 %) naslovov objavljenih na oglasnih deskah in 9 % naslovov iz e-mail seznamov je prejelo spam. Naslovi na preostalih lokacijah pa niso prejeli niti enega spama. (glej How Spammers Reap What You Sow: ttp://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm).

3.5 Pošiljatelji spama

Vse več je e-sporočil, v katerih pošiljatelji oglašujejo, prodajajo, obveščajo in vabijo. Na takšen način dosežejo milijone potrošnikov z minimalnimi stroški in pri tem običajno vodijo enosmerno komunikacijo. Sofisticirani računalniški programi jim še dodatno pomagajo pri hitri graditvi seznamov e-naslovov in masovnem pošiljanju. Razlikujemo med dvema tipoma spamerjev: »samo spamerji« in »spamerji za zakup«. »Samo spamerji« pošiljajo e-pošto samo zaradi lastnih potreb in je ne pošiljajo v tako velikem obsegu kot »spamerji za zakup«, ki imajo obsežne sezname e-naslovov in jih za določeno vsoto nudijo tudi drugim ali pa namesto njih pošljejo e-sporočilo. V prilogi C je primer ponudbe posrednika e-naslovov Quadra

Webside Promotions, ki zagotavlja 100-odstotne »opt-in« e-naslove in zagovarja neetičnost »junk mailov«.

Spamerji najpogosteje uporabljajo tri kanale, s katerimi razmnožujejo sporočila med številne uporabnike e-pošte:

- tuji ponudnik internetnih storitev, ki je specializiran za masovno pošiljanje sporočil;
- zavajajoč uporabniški račun za klicno povezavo (dial-up account), ki ga spamer kreira z lažnimi podatki, ga uporablja le kratek čas, nato pa ga odpre pri drugem ponudniku klicne povezave (dial-up);
- programi za masovno pošiljanje e-pošte, ki najdejo nezavarovane »sisteme e-pošte« na internetu, imenovane odprte povezave (open relays) in odprti proksi strežniki (open proxy), so danes zelo problematični. Odprte povezave omogočajo tretjim osebam pošiljanje e-pošte preko strežnikov drugih organizacij in s tem zakrivanje svoje identitete. Med spamerji so takšne povezave priljubljene, saj jim omogočajo anonimnost, nedostopnost pritožb prejemnikov, izogibanje nekaterim filtrom in uveljavljenim zakonom. V letu 2003 so v FTC identificirali še 1000 delujočih odprtih povezav in jih pozvali k zaprtju v smislu zmanjšanja spam sporočil.

4 SODOBNI TRENDI IN ZNAČILNOSTI SPAMA

Pošiljanje nezaželenih e-sporočil je zelo poceni oblika neposrednega marketinga. Seznam e-naslovov je moč kupiti pri nelegalnih prodajalcih ali pri propadlih dotcom podjetjih, ki so med delovanjem še zagotavljali zaupnost podatkov svojih strank. Že za dvesto dolarjev lahko spamer v zelo kratkem času pošlje sporočilo na več tisoč e-naslovov. Stroški pošiljanja pošiljatelja so pri množičnem pošiljanju skoraj zanemarljivi, skoraj vse si razdelita prejemnik oz. podjetje in ponudnik internetnih storitev.

4.1 Škodljivost spama

Stroški

Klasično oglaševanje je pogojeno z visokimi stroški pošiljatelja, zato so sporočila poslana le ciljnim skupinam. Nizek strošek e-pošte je dejavnik, ki pošiljatelju omogoča pošiljanje sporočil v enormnih količinah. Minimalni stroški jih torej ne spodbujajo k pošiljanju targetiranih sporočil, temveč k preplavljanju čim več e-poštnih predalov. Večji del stroškov pošiljanja spamov je na strani prejemnika, administratorja ali tretje osebe, preko katere spamer nezakonito pošilja e-pošto:

- *posameznik:* spamer lahko pošlje v 10 minutah milijon uporabnikom interneta e-sporočila, kumulativen čas izbrisa in stroški prejema pa so precej višji.

- *administrator:* obsežni seznami spamerjev z veljavnimi in neveljavnimi naslovi povzročajo ponudnikom interneta težko breme v sistemu administratorja in dodatne stroške. Nedostavljena e-pošta se shrani v poštnem predalu interneta (postmaster).

- *tretja oseba:* spamerji pogosto zlorabljajo naslove tretjih oseb, preko katerih razpošljejo e-pošto do končnih uporabnikov. Poštne predale nedolžnih »pošiljateljev« bremenijo številne pritožbe prejemnikov.

Vsebina

Spam problemi so povezani tudi z vsebino sporočil, ki vsebuje informacije nizke vrednosti in niso koristne prejemniku. Oglaševalska sporočila nudijo izdelke in storitve vprašljive kvalitete, kot so piramidne sheme in »multi-level« marketing. Vsebina spama, ki je največkrat namenjena odraslim, ne razkrije namena sporočila.

Varnost

Informacijska družba je pravzaprav družba nadzora. S ponudbo tehnologij, ki omogočajo končnemu uporabniku prijazno delovanje, sorazmerno raste tudi ponudba tehnologij, ki omogočajo vdore v računalniške sisteme, prestrezanje in zbiranje podatkov in e-naslovov. "Spam je aktivnost, ki trati čas, posega v varnost in relevantnost internetne komunikacije", meni Sorkin (Sorkin, 2001: http://www.spamlaws.com/articles/usf.html). Spam, poslan preko tretje osebe oz. podjetja, ne ogroža samo varnosti pošiljatelja, ampak tudi njegov ugled v javnosti. Predvsem pa je omajana zasebnost prejemnikov nezaželenih e-sporočil in posredno tudi e-pošta kot komunikacijski medij.

Prevare

Spam in njegov način razpošiljanja imata veliko elementov prevar, ki se istočasno nanašajo tudi na varnost v sistemu. Že prej omenjene odprte povezave omogočajo prevare na številnih ravneh: zavajajoče glave dokumentov in njihova vsebina ter uporaba deviantnih metod za prekritje identitete in lokacije spamerja. Z masovnimi sporočili zapolnijo ali celo blokirajo zmogljivosti internetnih ponudnikov, ki jih zaradi zabrisanih sledi težko identificirajo. Vir je še težje določljiv, kadar pošiljatelj uporablja brezplačni ali začasni e-poštni predal, v katerem so bili navedeni izmišljeni podatki.

Zmanjšanje produktivnosti

Zmanjšanje produktivnosti je naslednji negativni učinek spama. V podjetjih stroška ne predstavlja povezava na omrežje, ampak odsotnost zaposlenih od legitimnega dela. Pregovor »čas je denar« povsem drži, saj zapravljanje časa s spami skrajša čas za produktivno delo. Skupni stroški podjetja hitro naraščajo, če se zaposleni ukvarjajo s spamom le nekaj minut dnevno.

Družbeni stroški

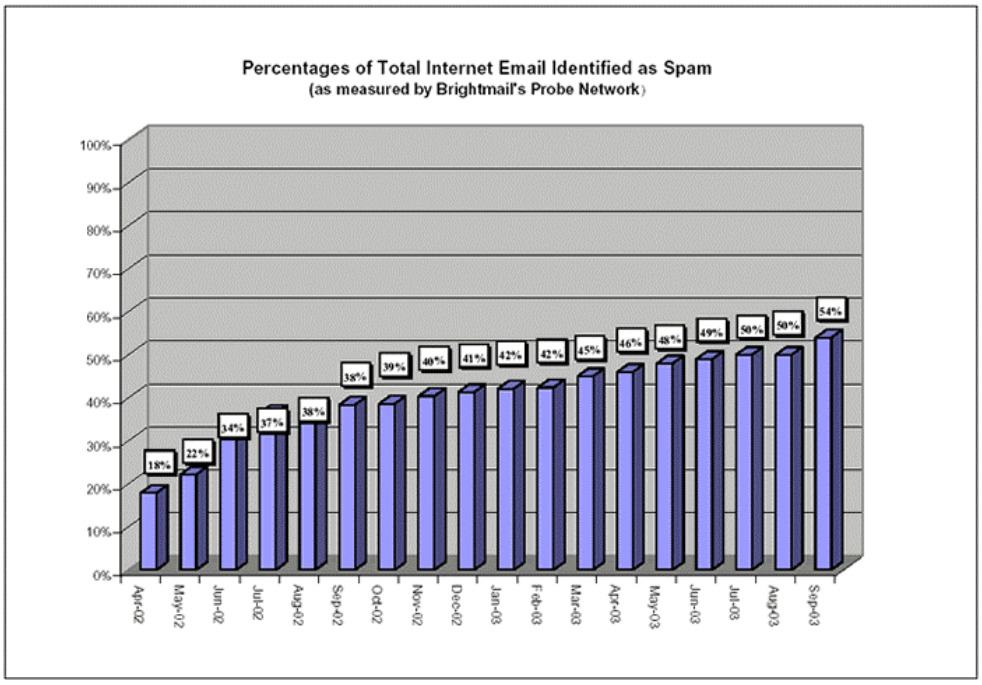
Največje posledice bo utrpel e-mail sam. Ogrožene so novičarske skupine, ki so glavna tarča vsakega spamerja. E-pošta je v zadnjem času postala kritično komunikacijsko sredstvo, ki neposredno ogroža tudi nadaljnji razvoj e-mail marketinga. Organizacija CAUCE predvideva uničenje uporabnosti in učinkovitosti e-pošte, če se rast UCE ne bo ustavila (CAUCE, www.cauce.org/about/problem/shtml). Prekomerne količine neželenih sporočil lahko v končni fazi povzročijo splošno nezaupanje in neučinkovitost interneta kot medija.

Zmanjšanje učinkovitosti storitve e-pošte

Velika količina spamov v e-predalu ogroža oz. ne dopušča prispetja legalne e-pošte, ki si jo prejemnik želi in ima zanj visoko vrednost. Lahko rečemo, da je uporabnost e-predala neposredno povezana s številom uporabne e-pošte oz. je v premem sorazmerju s številom vseh uporabnih e-pošt. Kadar je obseg spamov večji kot obseg legitimne e-pošte, se uporabnost storitve e-pošte zmanjša.

4.2 Trendi širjenja spama

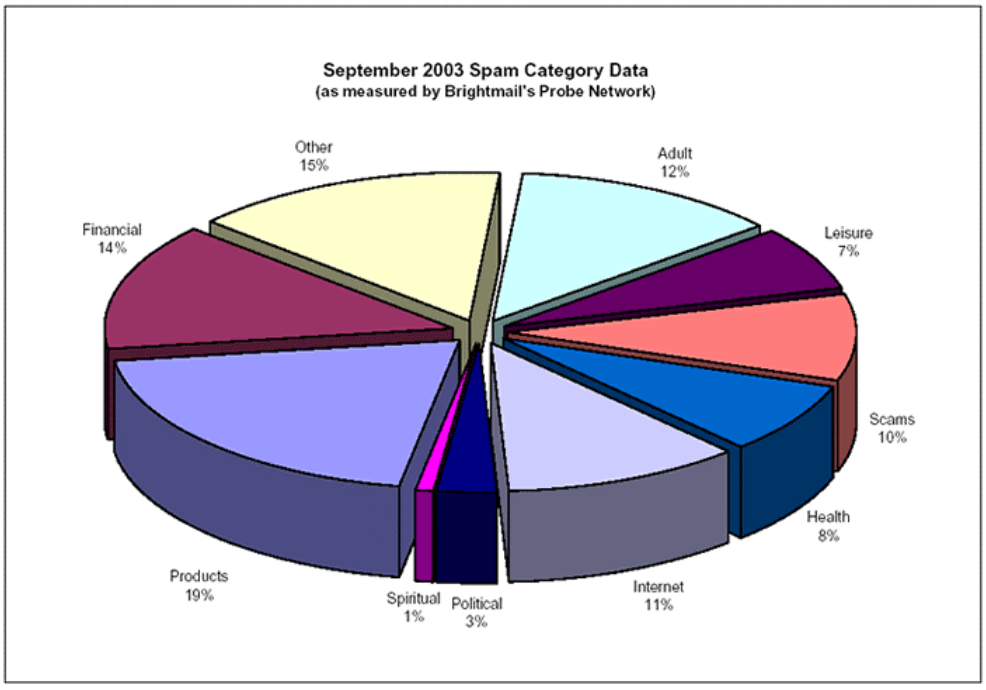
Pred desetimi leti so spam že označili kot nekaj neetičnega in nadlogo, vendar se zanj nihče ni čutil odgovornega. Od takrat pa do danes se je spam nepričakovano razširil in postal resen problem posameznega uporabnika in globalni problem organizacij, e-mail marketinga, e-komunikacije in varnosti na internetu. Problem, predvsem v ZDA, rapidno dobiva večje razsežnosti. Brightmailova raziskava, ki jo izvajajo na svojem Probe Networku, navaja, da je spam v ZDA sredi poletja že zasenčil legalno e-pošto. V septembru pa se je njegov delež v celotni e-pošti povzpel že na 54 %.



Slika 4.3: Odstotek spama v celotni e-pošti, Vir: (2003) Brightmail, http://www.brightmail.com/spamstats.html.

Obseg spama se je v letu 2001 povečal šestkrat in še vedno narašča. Nekateri celo trdijo, da narašča hitreje kot navadna e-pošta. Vse več je targetiranih spamov, katerih vsebina zavisi od letnega časa ali praznikov. Največji porast spamov je moč zabeležiti v času praznikov, kot so novo leto, valentinovo, materinski dan in drugi (Greenspan, http://cyberatlas.internet.com/big_picture/applications/article/0,,1301_1591431,00.html).

Glede na karakteristiko vsebine spamov organizacija Brightmail razvršča spam v 10 različnih skupin. Kot kaže spodnji graf v septembru ni bilo večjega odstopanja med kategorijami. Največ je bilo spamov s ponudbo izdelkov in storitev (product, 19 %), sporočil, ki ponujajo hitri zaslužek ali druge finančne priložnosti (financial, 14 %), in tistih, ki so namenjena odraslim (adult, 12 %), med katerimi prevladujejo sporočila s pornografsko vsebino. Število slednjih po besedah analitikov v zadnjem času najhitreje narašča. Najmanjši delež zavzemajo spami s politično (3 %) in duhovno (1 %) vsebino.



Slika 4.4: Delež posameznih kategorij spam v septembru 2003, Vir: (2003) Brightmail, http://www.brightmail.com/spamstats.html.

Anti-Spam Research Group (ASRG) se intenzivno posveča problemom, ki jih povzroča spam. V marcu 2003 so organizirali 56 IRTF[17] srečanje. Osredotočili so se na probleme, ki jih povzroča spam in skušali najti efektivne predloge za njegovo omejitev. Steve Atkins, član

SpamCon Fundacije, je v svojem prispevku predstavil dejansko stanje spama in probleme, ki jih povzroča (Atkins, 2003: http://www.ietf.org/proceedings/03mar/slides/asrg-1/):

- *obseg spama*

Atkins meni, da je za skoraj vse (96 %) uporabnike interneta spam zelo moteč, v ZDA predstavlja to 61 milijonov končnih uporabnikov in 682 milijonov vseh končnih uporabnikov. Februarja so pri AOL, največjemu ponudniku interneta, zabeležili 4 milijone spamov, marca se je število povzpelo že na 5,5 milijona.

- *stroški spama*

Rezulati so pokazali, da končni uporabnik zaradi spama letno odšteje od 30 do 50 dolarjev. Če se uporabnik ukvarja s spamom na delovnem mestu, nosi stroške tudi delodajalec. Že en sam spam zmanjša produktivnost za 1 do 2 dolarja in konec leta jo en delavec zmanjša za 730 dolarjev. SpamCon raziskava kaže, da je spam stal celotno ameriško industrijo 8,9 milijarde dolarjev v letu 2002. Visoke stroške nosijo tudi ponudniki interneta. Ocenjujejo, da jih posamezna stranka, ki izvaja spam preko »dial-upa«, stane od 2000 do 10.000 dolarjev. Dodatno jih bremenijo še pritožbe končnih uporabnikov. Večji ameriški ponudniki odštejejo kar 8 dolarjev na pritožbo, katerih lahko mesečno prejmejo več tisoč. Odvečen strošek ponudnikov predstavljajo še filtrirni sistemi, ki so v prvi polovici leta Ameriko stali že 650 milijonov dolarjev. Še večjo škodo pa povzročajo nekvalitetni filtri, ki zaustavijo visok delež (15 %) legalne e-pošte. Atkins je v svoji prezentaciji poudaril, da trend kaže na slabšanje situacije, ki naj bi ameriško industrijo v letu 2003 stalo 10 milijard dolarjev.

Paul Graham[18] je nedvomno prepričan, da so korenine problema masovne e-pošte v skoraj zanemarljivih stroških pošiljatelja. Spam primerja s čebelami in pravi, da je boleče, kadar nas piči ena čebela, kadar nas napade roj čebel, pa ima obseg problema popolnoma druge razsežnosti (Graham; www.paulgraham.com/spamdiff.html, 3). Spodnja tabela kaže, da je spam resnično stroškovno najugodnejši način pošiljanja sporočil, ki si ga lahko privošči vsak uporabnik e-pošte.

[17] IRTF - Internet Research Task Force, sestavljena je iz več manjših raziskovalnih skupin, ki se ukvarjajo z internetnimi temami..

[18] Paul Graham je oblikovalec Arc jezika. Največ je delal za Yahoo, še pred tem pa je bil direktor Viaweb, ki je postal Yahoo-jeva trgovina.

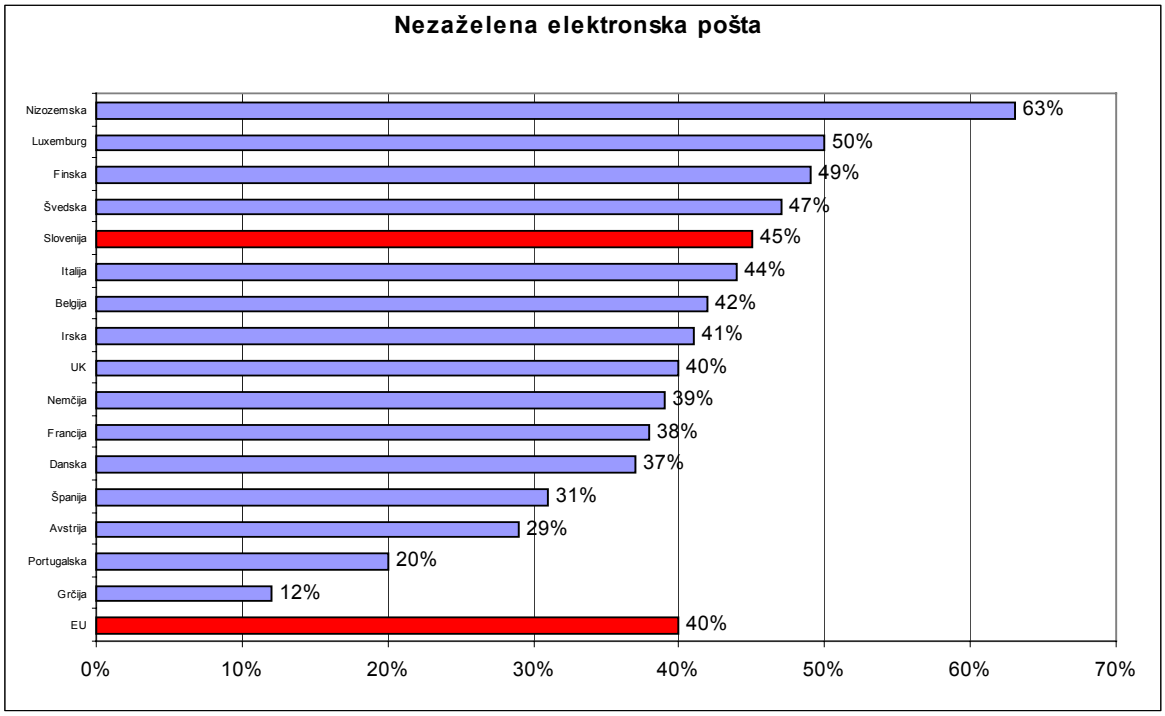
Tabela 4.1: Primerjava stroškov nezaželenih marketinških metod, Vir: http://www.spamcon.org/about/news/newsletters/008/opinion.shtml, avgust 2001.

Oblika	**Stroški pošiljatelja ($)**	**Stroški prejemnika ($)**	**Stroški pošiljatelja (%)**
Telemarketing	1.00	0.10	91.00
Poštna pošiljka	0.75	0.10	88.00
Fax	0.03	0.10	23.00
Samodejno klicanje	0.07	0.10	41.00
Spam	0.00001	0.10	0.01
* vse postavke stroškov so ocenjene na en stik s stranko			

Kljub znanju, visokim vložkom in tehnologiji nas spam še vedno ogroža. Trendi še ne kažejo vrhunca, temveč strmo vzpenjanje. Agencija Jupiter napoveduje, da bo uporabnik e-pošte v ZDA v letu 2006 prejel kar 1.400 spamov (Jupiter v Lieb: http://www.clickz.com/feedback/buzz/article.php/1432751, 1). Z naraščanjem števila spamov napovedujejo vzpon vrednosti antispam industrije. Leta 2002 so jo ocenili na 88 milijonov dolarjev, v letu 2006 Liebova[19] napoveduje, da bo vrednost poskočila na 181 milijonov dolarjev, če se bo trend spama gibal v isti smeri (Lieb, http://www.clickz.com/feedback/buzz/article.php/1432751, 2).

Spam predstavlja vedno bolj pereč problem tudi v posamznih evropskih državah. Spodnja slika kaže, da je delež uporabnikov interneta, ki so že prejeli spam, zelo visok predvsem v skandinavskih deželah, kjer presega evropsko povprečje (40 %). Nizozemska, znana kot država z največ varnostnimi problemi pri uporabi interneta, ima najvišji delež uporabnikov, ki so že prejeli spam (63 %), najmanj uporabnikov je prejelo spam v Grčiji (12 %). Presenetljivo visok je delež prejemnikov spama tudi v Sloveniji (45 %) in se glede na druge evropske države uvrščamo v zgornjo polovico.

[19] Rebecca Lieb – glavna urednica internetnega kanala Interactive Marketing



Slika 4.5: Delež uporabnikov interneta, ki so že prejeli nazaželena e-sporočila, Vir: (2002) RIS, http://www.sisplet.org/ris/ris/dynamic/readpublications.php?sid=59.

4.3 SMS spam

Hitri tehnološki razvoj omogoča spamu prodiranje tudi v mobilno telefonijo. Forrester research napoveduje, da bo letna rast števila sporočil preko mobilnih telefonov (SMS, MMS in e-pošta mobilnih telefonov naslednje generacije) 100-odstotna do leta 2004. Število SMS-ov naj bi se po tem letu počasi umirilo in doseglo vrhunec. V prihodnjih letih hitro rast sporočil pripisujejo predvsem neposrednemu marketingu in nezaželenim sporočilom multinacionalnih organizacij. Večina mobilnih operaterjev, vključno s slovenskimi, o večjih težavah, ki bi jih povzročilo množično pošiljanje SMS-ov, še ni poročala. Prejeli pa so že kar nekaj pritožb končnih uporabnikov zaradi prejemanja motečih, nezaželenih sporočil.

Z največjimi težavami so se soočili španski mobilni operaterji v preteklem letu, ko se je prvi računalniški virus, imenovan »Timofonica«, razmnoževal na omrežju mobilne telefonije in samodejno pošiljal SMS-e na vse številke iz imenika. (Siol, http://samurai.siol.net/novice/rac_clanek.asp?site_id=2&page_id=1&article_id=210105061911330).

Podjetje Threeant iz Maribora je na slovenskem trgu predstavilo spletni program SMSCity, ki omogoča izvajanje neposrednega marketinga v mobilni komunikaciji. Program nudi možnost neposrednega obveščanja, anketiranja, glasovanja in izvajanja različnih akcij. Lahko rečemo, da je idealno orodje za vzpodbujanje širitve SMS-spama.

Do sedaj je veljalo, da je nemogoč napad računalniških virusov v mobilno omrežje, danes pa strokovnjaki napovedujejo, da bo zaradi integriranja komunikacijskih orodij še več takšnih primerov. Problematičnosti spamov na tem področju se že zavedajo mobilni operaterji, ki na pritožbe končnih uporabnikov takoj ukrepajo z opozorilom pošiljatelja in z začasno izključitvijo iz omrežja v skrajnem primeru. Vodafon je že začel z reševanjem problemov. V posameznih državah omogoča namestitev antispam filtrov in na podlagi pritožb končnih uporabnikov oblikujejo antispam tehnologijo.

5 REGULIRANJE SPAMA

5.1 Načini omejevanja spama

Mag. Maja Bogataj v prispevku na konferenci »Poslovna raba interneta« pravi, da internetu ne vlada centralna avtoriteta in da ni reguliran iz enega centra moči. Posamezne države sicer urejajo najbolj problematična področja, zlasti svobodo govora, pornografijo, zasebnost, igre na srečo, davke in tudi pravice intelektualne lastnine. Tako so udeleženci komunikacije kot tudi tehnična infrastruktura, ki sestavljajo internet, podvrženi najmanj pravu držav, v katerih se nahajajo. Kljub temu pa ni mednarodnih pravilnih instrumentov, ki bi internet obravnavali kot celoto. Internet zato v veliki meri še vedno ostaja nereguliran ali samoreguliran (Bogataj; 2003: 3). Prva linija obrambe proti spamu je samoregulacija, sledijo ji tehnični mehanizmi – filtrirni sistemi. Mehanizme lahko implementira končni uporabnik sam ali ponudnik internetnih storitev kot tudi tretje osebe, ki se borijo proti spamu.

5.1.1 Samoregulacija

Samoregulacija zahteva od končnega uporabnika kar nekaj znanja, časa in neprestano pozornost. Če se želimo izogniti veliki količini spamov, moramo že e-naslov oblikovati tako, da bo spamerjem nedostopen. Čimbolj je naslov zapleten, tem manj imamo možnosti, da bi ga lahko uganili spamerji, ki se poslužujejo »dictionary attack« tehnike pridobivanja e-naslovov.

Nezaželeno e-pošto lahko zavrnemo z »opt-out« funkcijo ali pritožbo, vendar le takrat, kadar smo prepričani, da ne bomo poslabšali situacije. Večina zlonamernih spamerjev povratno sporočilo obravnava kot potrdilo pravega in delujočega e-naslova. Na takšen način si izoblikujejo seznam potencialnih prejemnikov za prihodnja e-sporočila. »Opt-out« funkcija deluje le takrat, kadar je v sporočilu naveden pravi e-naslov pošiljatelja in je le-ta želel dobronamerno informirati prejemnika. Manj tvegana je pritožba naslovljena na internetnega ponudnika, FTC ali druge organizacije, ki sprejemajo spam pritožbe. Ponudnik internetnih storitev lažje izsledi in opozori spamerja na nepravilno delovanje. V skrajnem primeru ima pravico ukinitve računa e-pošte in mu s tem prepreči nadaljnjo pošiljanje. Tudi FTC lahko neposredno graja spamerja ali proti njemu sproži postopek na sodišču, če vsebina sporočila ali način pošiljanja ni v skladu z zakonom države, katere državljan je prejemnik ali pošiljatelj (zavisi od zakona posamezne države).

Skoraj za vsako želeno informacijo, brezplačno naročilo na novice ali poskusni program je treba izpolniti obrazec, ki od nas zahteva splošne, demografske, včasih celo osebne podatke. Še preden potrdimo in odpošljemo prijavo se moramo vedno prepričati o pravilih posamezne spletne strani. Pogosti so primeri, ko izkoristijo našo nepozornost in jim nevede odobrimo pravico razpolagati z našimi podatki, ki jih posredujejo tretjim osebam. Internet je kot javna oglasna deska, do katere lahko vsi dostopamo. Kot kaže FTC raziskava v poglavju 2.6, spamerji nenehno prežijo nad spletnimi stranmi, novičarskimi skupinami, klepetalnicami in javnimi imeniki in iz njih pobirajo naslove. Z uporabo dveh ali več e-naslovov, katerim točno opredelimo uporabo za privatne in javne namene, se spretno izognemo takšnim problemom.

Hotmail kot tudi drugi ponudniki e-pošte nudijo možnost blokiranja vsakemu posamezniku v svojem e-poštnem predalu. Žal so spamerji še vedno en korak pred regulacijo in se filtrom in blok funkcijam spretno izogibajo tako, da pošiljajo sporočila iz različnih e-naslovov, z različnimi predmetnimi oznakami sporočila. Torej blok funkcija ni najbolj primerna rešitev, saj za blokado vsakega spama porabimo kar nekaj časa in se neprestano vrtimo v istem krogu.

5.1.2 Filtriranje in blok funkcije

Z naraščanjem obsega spama narašča tudi število filtrirnih sistemov. Starejši filtrirni sistemi sčasoma izgubljajo svojo učinkovitost. Spamerji jih kmalu prepoznajo in oblikujejo takšna sporočila, ki filtre obidejo. Nekateri filtri lahko arhivirajo sporočila v poštne predale, izbrišejo sporočila ali jih pustijo nedotaknjene, drugi lahko zaženejo zunanje programe in jim posredujejo sporočila. Vsi filtri pa lahko izvajajo funkcijo na osnovi glave sporočila, nekateri celo na osnovi vsebine sporočila. Se pravi, da večina filtrov razporeja e-pošto glede na naslov pošiljatelja ali prejemnika ali glede na opis predmeta sporočila. Test za preskušanje učinkovitosti posameznih filtrirnih sistemov ni samo število izbrisanih spamov, ampak je treba zraven upoštevati še število izbrisanih legalnih e-pošt. Tako da kvaliteto filtrirnega sistema ocenjujemo glede na število napak v smeri »pozitivne napake«[20] in »negativne napake«[21].

[20] pozitivna napaka (false positives) – je število fitlriranih legalnih e-pošt
[21] negativna napaka (false negatives) – je število spamov, ki jih filter ne zadrži in jih naslovnjenec prejme v svoj e-poštni predal

Splošno znane metode filtriranja na MUA (poštni uporabniški agent) in MTA (poštni prenosni agent) so danes že zastarele in neučinkovite. MUA je aplikacija posameznega računalnika in omogoča uporabniku pošiljanje ter vrnitev e-pošte. Najbolj običajni MUA je sestavljen iz Netscape Messengerja, Microsoft Outlooka in Eudore. MTA ima nalogo usmerjanja in prenos e-pošte. Tako MUA kot MTA filtri izločajo spame na osnovi informacij v glavi e-pošte, po karakteristikah adresarja, IP naslovu ali po domeni pošiljatelja.

Filtriranje v novičarskih skupinah

Tudi v novičarskih skupinah, ki so pomembna tarča spamerjev, je mogoče omejiti pošiljanje spamov. S tako imenovanim »presejanjem« vseh sporočil, se loči spame od pomembnih sporočil, ki se ne nanašajo na novičarsko skupino. Funkcijo presejanja izvaja moderator, zato je filtriranje spamov predvsem odvisno od njegove aktivnosti.

Novičarske skupine lahko izbirajo med robomoderatorji in retromoderatorji. Robomoderatorske skupine imajo računalniške moderatorje, ki nadomeščajo ali dopolnjujejo človeka. Računalniški program zavrne ali sprejme sporočilo glede na že prej preizkušena pravila. V primeru, da ne ve, kam bi uvrstil določeno sporočilo, na listo sprejetih ali na listo zavrnjenih, posreduje sporočilo moderatorju – človeku. Retromoderacijske skupine nastanejo kot neurejene, v katerih nekateri člani pozneje želijo uveljaviti svojo voljo z brisanjem sporočil z neprimerno vsebino. Čeprav število spamov sorazmerno raste s številom moderiranih skupin, lahko skupine še vedno zagotavljajo okolje, v katerem je relativno malo spamov (Schwartz in Garfinkel, 1998: 108).

Kolaborativno filtriranje

Filtriranje, ki ga izvajajo internetni ponudniki ali tretji proksi strežnik, kot je na primer Brightmail, je najbolj učinkovito in ne zahteva posebnega znanja končnega uporabnika. Brightmail, velik proizvajalec filtrov za ponudnike interneta in operaterje mobilne telefonije, kritizira učinkovitost MTA in MUA filtrov, ker blokirajo visok delež legitimne e-pošte, znižujejo produktivnost zaposlenih pri ponudnikih interneta, ker posvečajo precej časa njihovemu pravilnemu delovanju. Menijo, da zastareli filtri zaradi hitrih sprememb tehnik in orodij spamerjev vrtijo njihove uporabnike v začaranem krogu. Tudi blokada domene za spamerja ne predstavlja ovire, saj kmalu pridobi novo. Vztrajni spamerji brez večjih težav pridobijo nov IP naslov in novo enodnevno domeno ter dalje bombardirajo e-poštne predale. (The spam problem and Brightmail's solution, 2002: 16).

Nekateri poznavalci stavijo na bayesian filtre, ki delujejo z umetno inteligenco. Na osnovi prejšnih spam sporočil, ki si jih »zapomnijo«, izločajo sedanja sporočila. Njihova fleksibilna narava delovanja preprečuje malo drugače oblikovanim spamom, da bi dosegli prejemnikove e-poštne predale. Na primer, če je v preteklosti filter e-pošto s predmetno oznako »don't worry!« označil kot spam, ga tudi spročilo »don't w00rry!!!!« ne more prelisičiti. Drugi poznavalci prvo mesto pripisujejo filtrirnemu programu SpamAssassin, ki deluje na osnovi točkovanja. Večje število točk pomeni večjo verjetnost, da je sporočilo spam. Preusmeritveni filtri sporočilo glede na skupno število točk posredujejo na različne naslove. Točkovanje program vrši po poljubnih merilih.

Vse več podjetij zavrača nasvete strokovnjakov in nasprotuje kakršnimkoli filtrom, ker menijo, da le slabijo njihove rezultate. Filtri zaradi svoje neučinkovitosti in neprestanega posodabljanja predstavljajo uporabnikom le dodatni strošek. Tabela v prilogi D, ki obsega vse načine delovanja sodobnih filtrov, predstavlja njihove pomanjkljivosti, zaradi katerih noben sistem ne more zagotoviti popolne varnosti. Na neučinkovitost filtrov opozarja tudi dogodek, ko je Braightmailov direktor seznanil javnost z lansiranjem najnovejšega filtra. Znanega spamerja Ronalda Scelsona novica ni pretresla, saj je brezskrbno priznal, da potrebuje le 24 ur za razrešitev njihovih filtrov. Pohvali se je še, da mu v 12 urah uspe poslati od 120 do 180 milijonov e-sporočil. Nadležni pošiljatelj prejemnike zasipa s ponudbami od zdravilnih zelišč do antivirusnih programov, poroča TechWeb (Keizer, 2003: http://www.internetweek.com/story/showArticle.jhtml?articleID=10100104).

5.1.3 Opt-in, opt-out ureditev

OPT-OUT

»Opt-out« funkcija omogoča vsakemu prejemniku izraziti željo o prenehanju prejemanja nadaljnjih sporočil in izpis iz seznama. Skoraj vsi spami nudijo možnost izpisa preko navedenega e-naslova ali določene spletne strani. Običajno »opt-out« funkcija ne igra svoje vloge, ampak ima vlogo potrditve, da je naslov veljaven in delujoč. Preverjene e-naslove spamerji še z večjim užitkom zasipajo z neželenimi sporočili ali jih zberejo v seznam, ki ga prodajajo kot »opt-in seznam«.

David E. Sorkin trdi, da je »opt-out« funkcija relativno učinkovita v drugih oblikah neposrednega marketinga. Pri direktni pošti in telefonskemu marketingu naraščajoči stroški

na stik s potrošnikom neposredno prisilijo pošiljatelje, da upoštevajo prejemnikovo »opt-out« zahtevo. Ravno obratno pa masovno pošiljanje e-pošte ni povezano z naraščajočimi stroški, ki jih ne sili v prenehanje pošiljanja e-sporočil (Sorkin, www.spamlaws.com/articles/usf.pdf: 352).

Iznajdljivi spamerji so »opt-out« spremenili v funkcijo za razmnoževanje nezaželenih sporočil in pošiljateljev spama. Strokovnjaki razmišljajo o uvedbi enotnega oz. globalnega »opt-out« sistema, ki bi ravno tako zahteval spoštovanje, ažurnost in poštenost. Kultura spamerjev je precej drugačna in se ne odlikuje z omenjenimi vrlinami, zato bi gotovo tudi ta seznam izkoristili sebi v prid.

OPT-IN

Večja in bolj ugledna podjetja se v neposrednem marketingu poslužujejo »opt-in« načela. Svoje ponudbe pošiljajo le tistim potrošnikom, kateri so sami zaprosili za njihove informacije. Žal ima tudi ta oblika regulacije pomanjkljivosti, predvsem zaradi netočno definiranih pravil delovanja. Zlorabe izvajajo tiste tretje osebe (običajno so to spamerji), ki v »opt-in« sezname vpisujejo e-naslove potrošnikov brez njihovega privoljenja, in podjetja, ki svoje sezname izposojajo drugim sorodnim podjetjem. Za rešitev problema je predlagan »*dvojni opt-in«*, ki deluje na osnovi vpisa v seznam in ponovne potrditve ob prejemu prve e-pošte. Uspešnost tako enojnega kot »dvojnega opt-in-a« je vprašljiva vse dotlej, dokler bo to le pravilo posameznih organizacij in ne vseh uporabnikov interneta.

Zaradi številnih zlorab in slabo definiranih neobčih »opt-in« pravil menijo strokovnjaki, da to ni orodje, ki bi v celoti zatrlo spam, ampak je le eno iz med mnogih. Zagotovo bo moč »opt-in« načela narasla, ko se bo zakonodaja dokončno odločila zanj, ga natančno opredelila in sankcionirala njegove zlorabe. Zaradi nasprotujočih si interesov javnosti, ki zagovarja »opt-in«, in industrije – zagovornica »opt-out«, se stvari zelo počasi premikajo. Evropska unija je konec oktobra s sprejetjem nove direktive, ki temelji na »opt-in« načelu, naredila prvi korak.

5.1.4 RBL – Realtime Blackhole List

Veliko ponudnikov interneta uporablja »črne sezname« za »lov« spamerjev. Danes je aktivnih približno 150 takšnih seznamov, ki so si bolj ali manj podobni in imajo isto funkcijo. Najbolj poznan je seznam Realtime Blackhole List (RBL), ki ga upravlja mreža internetnih

ponudnikov MAPS (Mail Abuse Prevention System). Uporabljajo ga sistemski administratorji ponudnikov internetnih storitev za masovno bojkotiranje. Mrežo, ki ima danes vključenih že tretjino svetovnih internetnih ponudnikov, je organiziral dolgoletni aktivist proti spamu Paul Vixie. MAPS poleg RBL seznama upravlja še druge črne sezname: Dialup User List (DUL), Nonconfirming Mailing List (NML), Relay Spam Stopper (RSS) in RBLPLUS, ki je sestavljen iz RBL, RSS in DUL-a.

»Črni seznam«, v katerem je vključen vsak račun (account) interneta, ki ga je ponudnik interneta izključil zaradi zlorabe, informira vse včlanjene internetne ponudnike o posameznem primeru množičnega pošiljanjih spama. Informacija z IP naslovom in imenom domene, ki jo uporablja spamer, pomaga ponudnikom interneta preprečevati njihovo nadaljnje pošiljanje ali odprtje novega računa za pošiljanje e-pošte. RBL ima še eno funkcijo imenovano »ime domene serverja« V njem so shranjeni zapisi vseh spletnih strani, ki so povezane s spamom. Tako MAPS sistem lahko deluje kot filter, ki avtomatično blokira vsa sporočila iz te liste (http://www.mail-abuse.org/rbl/enduser.html, Why was I referred to this website?).

Graham in drugi strokovnjaki spam področja »črne sezname« označujejo negativno. Blokade, ki delujejo na osnovi »črnih seznamov, avtomatično brišejo vse e-pošte, katerih domene so zapisane na listi. Visoko število »pozitivnih napak« in slaba filtracija spamov označujejo sezname kot nizko učinkovite (Graham, www.paulgraham.com/falsepositives.html:1).

Togost RBL sistema in neažurnost sta velikokrat vzrok blokiranja nedolžnega ponudnika interneta. Takoj ko eden njegovih uporabnikov povezavo izrabi za pošiljanje spamov, je že vpisan v »črni seznam«, zaradi katerega najhujše posledice utrpijo »dotcom« podjetja. Dotcom podjetje, Internet Billing, so štirje dnevi na črnem seznamu stali 400.000 dolarjev izgube (Gaudin in Gaspar, http://www.nwfusion.com/research/2001/0910feat.html). Zaradi takšnih krišitev je MAPS večkrat obtožen neučinkovitega in nepravilnega delovanja ter nespoštovanja pravil.

5.1.5 Netiquette

Na začetku interneta je bil majhen krog uporabnikov, ki so bili dobro tehnično podkovani in so razumeli njegovo naravo delovanja. Z večanjem obsega uporabnikov, neveščih »internetne kulture« in poznavanja protokolov in sistemov za prenos sporočil, so se začele pojavljati prve

zlorabe. Zato se je FTC v 90-ih odločil napisati smernice imenovene Netiquette[22], ki naj bi prispevale k pravilnemu vedenju uporabnikov, jih kultivirale na področju interneta in preprečevale zlorabe vseh udeležencev, tako končnega uporabnika kot tudi sistemov, ki podpirajo delovanje interneta in e-pošte.

Pravila v Netiquette se delijo v tri osnovne skupine:

1. Prvo je namenjeno *ena na ena komunikaciji*, kjer so definirana pravila e-pošte in komunikacije oz. dialoga preko interneta. Opozorila, prepovedi in zapovedi so namenjene končnim uporabnikom in administratorjem.

2. Drugo poglavje je namenjeno *komunikaciji z več uporabniki interneta*. Pravila iz prvega poglavja so nadgrajena in naslovljena na končne uporabnike, administratorje in moderatorje novičarskih skupin. Opozarjajo na nevšečnosti pri pošiljanju sporočil na e-naslove iz seznamov in v novičarskih skupinah.

3. Zadnje poglavje obravnava *informacijske servise,* kot so IRC, WWW in nekatere druge, ki jih danes skoraj ne uporabljamo več. Opozorila in navodila za pravilno ravnanje so spet razdeljena na uporabniška in administratorska.

Pravila v »netiquette« podrobno seznanjajo z računalniško etiko vse udeležence komunikacije in administratorje, ki komunikacijo podpirajo. Zaradi svoje obsežnosti in nizke »internetne kulture« vseh uporabnikov v dobi komercialnega interneta ne dosegajo svojega namena. Tudi Sorkin ugotavlja, da je bil približno do leta 1996 socialni pritisk dovolj močen in upoštevan v boju proti spamu (Sorkin, 2001: www.spamlaws.com/articles/usf.pdf). Danes ima spletna stran »netiquette« samo še zgodovinski pomen in jo obiščejo le še tisti, ki iščejo začetne regulacije spama. Vse večjega obsega spama v dobo visoke potrošnje in komercializacije pa tudi represivni ukrepi ne morejo zaustaviti.

5.2 Antispam gibanja

Tako v Ameriki kot tudi v Evropi in drugih državah sveta je delujočih veliko antispam organizacij. Zaradi nemočnosti, ki se kaže v večanju obsega spama, se organizacije povezujejo in združujejo moči, znanja ter predloge. Prizadevajo si doseči večjo vplivno moč, ki bo pospeševala sprejetje prepotrebnih regulativ in zakonov za zajezitev problema.

[22] Netiquette – ime izvira iz dveh besid obmrežje (network) in predpisi (etiquette)

5.2.1 CAUCE

CAUCE – »Coalition Against Unsolicited Commercial Email« se je oblikovala iz diskusijske skupine imenovane SPAM-LAW, ki je bila produkt seznama SPAM-L. CAUCE je bila osnovana iz uporabnikov interneta, ki so spoznali, da tehnologija sama ni dovolj močna za preprečitev internetne nadloge – spama. Njene pristopnice so: EuroCAUCE, CAUCE Canada, CAUCE India in CAUBE.AU in nekatere manjša združenja znotraj Evrope. Vse imajo lastnosti »ad hoc« in prostovoljnega delovanja. Sestavljene so iz uporabnikov interneta (netizens), ponudnikov internetnih storitev in tehnoloških ter pravnih strokovnjakov, ki se borijo proti spamu in sodelujejo pri oblikovanju pravnih zakonov. CAUCE je povezana tudi s številnimi vladnimi in nevladnimi organizacijami, ki s skupnimi močmi oblikujejo močan lobi.

CAUCE je internetna kreacija, ki ne pobira nikakršnih donacij. Obstajajo na spletnih straneh, v novičarskih skupinah, različnih diskusijskih skupinah in v idejah tistih, ki se zavzemajo proti spamu. Navidezno upravo oblikuje devet članov. Ker je spam problem nas vseh in ga nihče ne more ignorirati, je kot član dobrodošel vsak uporabnik interneta, ki podpira njihove pobude. Svoje cilje uresničujejo s pravniško verodostojnostjo in aktivnimi člani, ki spodbujajo člane zakonodajne skupščine k sprejetju njihovih predlogov. Leta 1997 so predlagali dodatek k zveznemu statutu o zakonski prepovedi »junk« faksov. Od takrat je koalicija prevzela vodilno vlogo v boju proti spamu.

5.2.2 FTC – Federal Trade Comission

Komisija je bila ustanovljena 1914 z namenom, da se bori proti nepoštenim metodam konkurence. FTC danes deluje neodvisno od drugih organov države in podpira ameriški kongres pri njegovih odločitvah. Vodi jo pet pooblaščencev, ki jih imenuje predsednik in potrdi senat. FTC skrbi predvsem za močan, učinkovit nacionalni trg brez omejitev, ki ne škoduje potrošnikom. Sodeluje z drugimi državnimi organi in svetuje pri uvajanju zakonov ter spodbuja k sprejetju novih, da bi preprečevali prevare, goljufije in nepoštene poslovne odnose. Njeno glavno poslanstvo je zaščita potrošnikov.

S spremljanjem številnih ekonomskih raziskav in analiz, ki so zaradi njihove narave in vpletenih subjektov nedostopne javnosti, komisija predlaga oblikovanje potrebnih zakonov.

Pomaga pri odločitvah na kongresu, izvršilni oblasti, drugim neodvisnim ustanovam, državi in lokalnim oblastem.

Oddelek za zaščito potrošnikov se deli na šest pododdelkov, ki strokovno podpirajo vsak svoj program. Predvsem skrbijo za resnično in dostojno oglaševanje, ki ne žali potrošnikov in ne krši njihovih pravic. Ob kršitvi zakona posamezni primer posredujejo sodišču in tako pripomorejo k preprečitvi in zmanjšanju prevar. V zadnjem času FTC precej časa namenja boju proti internetnim in telefonskim prevaram, nepravilnostim v neposrednem marketingu in piramidnih shemah ter drugim goljufijam, ki zavajajo potrošnike z namenom »čim več zaslužiti«. Organizacija na različne načine potrošnike informira o njihovih pravicah, jih opozarja na nevarnosti in jim pomaga. Na e-naslovu »uce@ftc.gov« FTC zbira pritožbe potrošnikov, ki so žrtve množičnega spama. Na podlagi teh pritožb lahko organizacija opredeli spame, jih razvršča v različne skupine glede na vsebino, pošiljatelja in prejemnika ter določi trend. Takšne analize prispevajo k bolj izpopolnjenim antispam filtrom in pri dokazovanju kongresa o sprejetju skupnega antispam zakona.

FTC je leta 2003 kongres zaprosila za večjo moč v boju proti spamu. Njen namen je oblikovati enotne zakone in razširiti ukrepe, ki regulirajo telemarketing, na področje spama za celotno Ameriko. Svoje informacije želi narediti bolj trensparentne in jih deliti s podobnimi ustanovami iz drugih držav. Predvsem si prizadeva za skrajšanje dolgotrajnih postopkov, s katerimi se ugotavlja nezakonita dejanja spamerjev.

5.2.3 SpamCon

SPAMCON je neprofitna korporacija, ki se zavzema za zmanjšanje neželenih masovnih sporočil in za zaščito e-pošte kot medija komunikacije in marketinga. V ta namen organizira številne forume za izobraževanje in sodelovanje internetnih uporabnikov, administratorjev in internetnih tržnikov. Njihovo poslanstvo se odraža v celotni antispam skupnosti, ki vzpodbuja k odgovornemu e-mail marketingu. Cilj korporacije je omogočiti uporabnikom interneta optimalno kontrolo prejete e-pošte in njeno nemoteno kroženje .

Organizacije, kot so Anti Spam Research Group, MessageLabs, SpamCop, SpamHaus, DMA, ADMA in druge, imajo tudi »antispam poslanstvo«. Nekatere sponzorirajo podjetja, ki jih

spam ogroža, druge so vladne organizacije, nekatere analizirajo in poročajo o dejanskih stanjih in spremembah, druge iščejo in predlagajo rešitve.

5.3 Pravna regulacija spama

Pravica do zasebnosti je sicer temeljna, vendar ne absolutna. V sodobni družbi je postala ena pomembnejših človekovih pravic. Poročilo Privacy & Human Rights pravi, da sta najbolj ogroženi informacijska zasebnost in zasebnost komunikacij. Ogrožajo ju *globalizacija*, ki odstranjuje geografske omejitve pri pretoku podatkov, *konvergenca med tehnologijami*, ki omogoča povezanost in skupno delovanje različnih tehnologij, in *multimedialnost*, ki omogoča spreminjanje podatkov iz ene oblike v drugo (Banisar, 2000: www.privacyinternational.org/survey/index99.html). Razvoj je tako privedel do potrebe po učinkoviti zakonodaji za zaščito zasebnosti. Danes ima skoraj že vsaka ustava države opredeljeno pravico do zasebnosti, ki jo ogroža informacijska družba. Tehnologija je pospešila zbiranje in obdelavo podatkov, njene zmožnosti so zahtevale nova pravila na področju osebnih podatkov. Prvi zakon o varstvu osebnih podatkov je sprejela Zvezna republika Nemčija v letu 1970 (Kovačič, 2003: 35). Že leta 1974 je generalni sekretar OZN predvidel ogroženost informacijske zasebnosti, zato je priporočil tri načela, ki naj bi jih vsebovala zakonodaja. Načelo *relevantnosti,* ki zahteva, da se o posamezniku zbirajo samo nujno potrebni podatki za dosego namena, zaradi katerega se zbirajo; načelo *notifikacije,* ki zahteva, da bo posameznik predhodno seznanjen o tem, kateri podatki se o njem zbirajo, shranjujejo in obdelujejo; ter načelo *privolitve*, ki pravi, da naj se zbirajo samo tisti podatki, za katere je posameznik privolil (Kovačič, 2003: 36).

Zlorabe, jezni prejemniki, zmanjšana učinkovitost v podjetjih, upočasnjeno delovanje celotnega sistema ali celo blokada ponudnikov interneta so stopnjujoči problemi, ki kličejo h korenitim spremembam in novostim v zakonodaji na področju spama.

5.3.1 Regulacija spama v Evropi

Pravna regulacija v Evropi obsega pet direktiv, ki so relevantne v boju proti spamu: direktiva o zaščiti podatkov, elektronski zasebnosti, zasebni telekomunikaciji, pogodbah na daljavo in direktiva o elektronskem poslovanju. Direktive niso zakoni *per se,* so le smernice, ki od držav članic zahtevajo, da na nacionalni ravni sprejmejo zakone ali dopolnitve z vsebino členov

direktiv, kot sta jih določila Evropski parlament in Svet. Direktive ne zajamejo vseh sporočil, temveč regulirajo samo tista, poslana v Evropi.

5.3.1.1 Direktiva zasebnosti

Ena prvih direktiv, ki se nanašajo na pošiljanje nezaželenih e-sporočil, je direktiva 95/46 EC, sprejeta oktobra 1995. Ureja pravice vsakega posameznika in dopušča »predelavo« le tistih osebnih podatkov, ki so zbrani in obdelani pošteno iz specifičnega in legitimnega razloga.

Člen 2(a) opredeljuje *osebne podatke* kot katerikoli podatek, ki se nanaša na določeno ali določljivo osebo. Osebo pa kot določljiv subjekt, ki ga je moč posredno ali neposredno določiti z identifikacijsko številko ali z enim oz. več faktorji, značilnimi za njegovo fizično, fiziološko, mentalno, ekonomično, kulturno ali socialno identiteto. Za obdelavo osebnih podatkov je nujno potrebno dovoljenje, ki ga oseba izrazi s kakršnokoli neprisiljeno, specifično in neoporečno indikacijo svojega mnenja in s tem izrazi strinjanje za obdelavo svojih osebnih podatkov (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://www.spamlaws.com/docs/95-46-ec.pdf).

Direktiva ščiti posameznika proti zlorabi njegovih osebnih podatkov in dovoljuje njihovo obdelavo le ob jasni privolitvi osebe oz. navaja posamezne situacije, v katerih je odobrena uporaba osebnih podatkov [23]. Oseba mora biti ob privolitvi posredovanja svojih podatkov obveščena o namenu zbiranja in prejemniku ter mora imeti pravico dostopa in urejanja podatkov, ki jo zadevajo[24]. Pojem »obdelava podatkov« je zelo širok in zajema zbiranje, registriranje, urejevanje, shranjevanje, prilagajanje ali spreminjanje, kompenziranje, posvetovanje, uporabo, razkrivanje pri prenosu, širjenje, formiranje ali kombiniranje, blokiranje, izbris ali uničenje osebnih podatkov[25]. Kjer pa podatki niso prejeti neposredno od subjekta, je določeno, da mora biti oseba informirana najpozneje do prvega razkritja njenih podatkov[26]. V primeru, da so osebni podatki uporabljeni za izvajanje neposrednih marketinških aktivnosti in so posredovani tretji osebi brez njene vednosti, ima posameznik pravico nasprotovati uporabi svojih osebnih podatkov v takšne namene[27].

[23] Člen 7, Direktiva o zaščiti podatkov.
[24] Člen 10, Direktiva o zaščiti podatkov.
[25] Člen 2(b), Direktiva o zaščiti podatkov.
[26] Člen 11, Direktiva o zaščiti podatkov.
[27] Člen 14(b), Direktiva o zaščiti podatkov.

Iz definicije osebnih podatkov in fizične osebe je jasno razvidno, da je večina e-naslovov oblika osebnega podatka. Naslovi pogosto vsebujejo uporabniško ime kot tudi državo bivanja in ponudnika interneta ali kraj zaposlitve. Tudi če takšni podatki niso razpoložljivi, ni težko povezati e-naslova s podatki, ki naredijo osebo določljivo. Pri določanju osebe in njene identitete pripomorejo na videz neškodljivi piškotki, ki so raztroseni po internetnih straneh.

Direktiva o zaščiti osebnih podatkov prepoveduje pošiljanje nenaprošene e-pošte. Vseeno pa je zadnja beseda v rokah posameznih držav članic Evropske unije. Direktiva sama ne prepoveduje pošiljanja tovrstnih e-sporočil, zahteva le transparentnost zbiranja in uporabe osebnih podatkov, kot je e-naslov. Posamezniku oz. e-mail uporabniku torej daje možnost prepovedi uporabe njegovega osebnega podatka - e-naslova - za namene neposrednega marketinga - pošiljanja spama.

5.3.1.2 Direktiva o zasebnosti v telekomunikacijah

Direktiva 97/66 EC je bila sprejeta decembra 1997 in sega na področje osebnih podatkov v telekomunikacijah. Komunikacije preko e-pošte ne navaja izrecno. Direktiva določa: "Uporaba sistema avtomatičnega klicanja brez posredovanja človeka ali faksimile naprave za namene neposrednega marketinga je dovoljena le ob vnaprejšnjem soglasju osebe vpisane na seznamu" (Directive 97/66/EC of the European Parlament and of the Council of 5 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, http://www.spamlaws.com/docs/97-66-ec.pdf). Direktiva še prepoveduje pošiljanje kakršnihkoli brezplačnih in/ali nenaprošenih klicev brez privoljenja že vpisanih oseb na seznamu ali tistih, ki ne želijo teh klicev[28].

Ščiti posameznika pred vdorom v njegovo zasebnost in nezaželenimi stiki, ki bi ogrožali in vznemirjali uporabnika telekomunikacijskih sistemov. Njen namen je prenos direktive o zasebnosti v okolje telekomunikacij. Žal se vse njene določbe nanašajo na »klic«, tako da ne zavzemajo e-pošte in drugih e-komunikacij.

Nekatere članice EU, kot so Avstrija, Danska, Finska in Italija, so že do leta 2000 na nacionalni ravni dopolnile direktivo in sprejele zakon, ki v smislu 12. člena direktive o

[28] Člen 12(2), Direktiva o zasebnosti v telekomunikacijah.

zasebnosti v telekomunikacijah prepoveduje tudi spam ali nenaprošeno komercialno e-sporočilo.

5.3.1.3 Direktiva o pogodbah na daljavo

Direktiva 97/7 EC je bila sprejeta maja 1997. Podobno kot že opisana direktiva o zasebnosti v telekomunikacijah prepoveduje uporabo sistema avtomatičnega klicanja brez posredovanja človeka in faksimile naprave brez predhodne odobritve potrošnika[29] (Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, http://www.spamlaws.com/docs/97-7-ec.pdf). Člen 10 nadalje zahteva, da države članice zagotovijo pravi pomen komunikacije na daljavo in jo uporabijo le takrat, ko ji prejemnik ne nasprotuje.

5.3.1.4 Direktiva o elektronskem poslovanju

Direktiva 2000/31 EC je bila sprejeta junija 2000. Člen 7 ureja nenaprošeno komercialno komunikacijo in pravi, da naj države, ki odobravajo nenaprošeno komercialno komunikacijo preko e-pošte, zagotovijo prepoznavnost pošiljatelja prejemniku. (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), http://www.spamlaws.com/docs/2000-31-ec.pdf). Direktiva še zahteva, da pošiljatelji redno upoštevajo in spoštujejo »opt-out« register, v katerega se fizične osebe, ki ne želijo več prejemati nezaželenih e-sporočil, vpišejo same[30].

Dvoumnost posameznih določb direktive še nadalje pušča odprto pot pošiljanju nezaželene e-pošte. Zahtevana je jasna razpoznavnost identitete pošiljatelja, nikjer pa ni omenjena obveznost pošiljatelja, da izpiše prejemnika iz seznama e-naslovov na njegovo željo. Direktiva tudi ne opisuje postopka izpisa iz seznama, tako da veliko spamerjev, ki omogočajo izbris e-naslova prek telefona, zasluži s tem visok honorar. Pomanjkljivost direktive je tudi v nenatančni opredelitvi glede oblikovanja in upoštevanja »opt-out« registra. Ni razvidno, ali predpisuje en register za celo EU ali več registrov, v katere se mora prejemnik vpisati, spamer pa vse upoštevati. Določba »redno upoštevanje« tudi ni opredeljena in si jo lahko razlaga vsak

[29] Člen 10(1), Direktiva o pogodbah na daljavo.
[30] Člen 7(2), Direktiva o elektronskem poslovanju.

po svoje kot enkrat na mesec, enkrat na teden ali pred vsakim pošiljanjem večje količine e-sporočil. Lahko rečemo, da tudi ta direktiva ne prepoveduje pošiljanja nenaprošenih e-sporočil.

5.3.1.5 Direktiva o zasebnosti v elektronski komunikaciji

Direktiva 2002/58/CE, sprejeta oktobra 2003, posodablja direktivo o zasebnosti v telekomunikacijah v smislu novih tehnologij in zagotavlja, da bodo pravila zasebnosti, ki veljajo za storitve telefonije in faxa, veljala tudi na področju e-pošte in interneta. Njen namen je zaščititi zaupnost komunikacije in osebnih podatkov, postaviti pogoje poslovanja in nameščanja ter dajati smernice vsem vpisanim v sezname. Glavni namen je regulacija nenaprošene, direktne in mrežne komunikacije za namen marketinga prek telefona, faksa, e-pošte in tudi SMS-ov.

Direktiva spama kot takšnega žal ne opredeljuje, zato bodo še nadalje ostajali dvomi, kaj spam sploh je. Definirana je le e-pošta kot kakršnokoli besedilo, glas, zvok ali slika, poslana preko javnega komunikacijskega omrežja, in je lahko shranjeno na omrežju ali opremi končnega uporabnika, dokler jo prejemnik ne prejme (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, http://www.spamlaws.com/docs/2002-58-ec.pdf). Direktiva se s pojmom »dovoljenje« nanaša na opredelitev o zaščiti podatkov.

Popravlja napako direktive o elektronskem poslovanju, saj pošiljateljem e-sporočil določa omogočanje brezplačnega in enostavnega izpisa prejemnikov iz seznama. Omejuje pošiljanje SMS sporočil, ki še niso tako množični kot e-pošta. Problemi na tem področju verjetno nastajajo prav zaradi cenene možnosti pošiljanja SMS-ov preko interneta.

Člen 5 je razdeljen v tri dele. Prvi in drugi del pozivata države članice k zagotavljanju zaupne komunikacije in varovanju njenih podatkov. Prepovedujeta prestrezanje (prisluškovanje), shranjevanje in nadzor komunikacije ter z njo povezanih podatkov tretjih oseb brez njihovega dovoljenja. Prepoved ne velja za tiste primere, za katere je zaradi državne varnosti, uveljavljanje zakonov ali podobnih razlogov izdano dovoljenje.[31]

[31] Člen 15(1), Direktiva o zasebnosti v elektronski komunkaciji.

Tretji del 5. člena poziva države članice k zagotovitvi dovoljene uporabe elektronske mrežne komunikacije za shranjevanje informacij ali za pridobitev povezave do informacij shranjenih na končni opremi uporabnika le v primeru, da je uporabnik, ki ga podatki zadevajo, seznanjen z jasnimi, obsežnimi in razumljivimi informacijami. Upoštevati je treba tudi »predelavo podatkov«, ki mora biti v skladu z direktivo o varstvu podatkov 95/46/EC. Uporabnik mora imeti pravico zavrnitve obdelave podatkov s podatkovnim revizorjem[32] (Directive on privacy and electronic communications, http://www.spamlaws.com/docs/2002-58-ec.pdf). Uvodna dela direktive, (recital) 24 in 25, jasno govorita o tem, da se zgoraj omenjena določba nanaša na uporabo piškotkov in podobnih programov, ki so nameščeni na opremi končnega uporabnika, z namenom zasledovanja in identificiranja.

Člen 13 zahteva od držav članic zagotovitev fizičnim osebam pravico vnaprejšnjega dovoljenja oz. izbire »opt-in« in pravi takole: *"Kjer pravna ali fizična oseba od svojih strank pridobi njihove natančne elektronske kontaktne podatke z namenom prodaje izdelka ali storitve v skladu z Direktivo 95/46/CE, lahko ista fizična ali pravna oseba te elektronske kontaktne podatke uporabi za neposredno trženje svojih lastnih podobnih izdelkov ali storitev. To se lahko izvede pod pogojem, da je stranka jasno in nedvoumno obveščena o možnosti ugovora glede takšne uporabe elektronskih kontaktnih podatkov, in sicer mora biti stranki ugovor omogočen brezplačno in na lahek način. Stranka lahko ugovarja, ko se ti podatki zbirajo"* (Directive on privacy and electronic communications, http:// www.spamlaws.com/docs/2002-58-ec.pdf).

Direktiva še določa, da e-pošta, poslana za namen direktnega marketinga, ne sme skrivati identitete pošiljatelja, ki je pobudnik komunikacije. Vsebovati mora veljavni e-naslov pošiljatelja, na katerega lahko prejemnik pošlje zahtevo o prenehanju pošiljanja takšne vrste sporočil[33]. Določbe se nanašajo na fizične osebe, direktiva pa državam članicam svetuje, da jih razširijo in aplicirajo tudi na pravne osebe.

Pravne osebe in ponudniki internetnih storitev ostajajo še vedno nezaščiteni. »Obstoječi odnosi« in »podobni izdelki« (člen 5.) sta zelo široka pojma, vendar jih direktiva ne opredeljuje natančneje ter s tem dopušča uporabnikom e-pošte pri opredelitvi uporabo »lastne

[32] Direktiva 95/46/EC: Podatkovni revizor predstavlja fizično ali pravno osebo, javna oblast, agencija ali katerokoli drugi organ, ki sam ali s pomočjo drugih določa predloge in pomene obedelave osebnih podatkov; kjer so predlogi in pomen obdelave določeni z zakonom ali regulativo, državni zakon sme določati tudi revizorja ali specifiče karakteristike za njegovo imenovanje (http://www.spamlaws.com/docs/95-46-ec.pdf).

domišljije« in seveda nemoč zakona v posameznih primerih. Kljub vsem naporom pri oblikovanju in sprejemanju direktiv je njihova veljavnost le na področju komercialnih e-sporočil (UCE), ki zagotovo predstavljajo večji del spamov, ne pa vseh. Množična e-sporočila (UBE), kot so ankete, verska sporočila, politični oglasi, vojna propaganda, legende, verižna pisma, prošnja za dobrodelne namene, bodo še vedno brez omejitev potovala po omrežju, saj jih niti direktiva niti nacionalni zakoni ne prepovedujejo. Izjema je le Avstrija, katere zakon prepoveduje pošiljanje kakršnihkoli množičnih e- sporočil (UBE) brez vnaprejšnje privolitve prejemnika.

»Opt-in« načelo je veljavno v Avstriji, Belgiji, Danski, Finski, Grčiji, Madžarski, Italiji, Norveški, Poljski, Španiji in Sloveniji. Švedska in Francija sta v postopku sprejemanja zakona. Vse države prepovedujejo pošiljanje e-pošte tretjim osebam brez vnaprejšnjega odnosa s prejemnikom in njihovega privoljenjem ter takšno kršitev kaznujejo z določenim zneskom za posamezen spam ali dnevno pošiljanje. V naštetih državah je znanih le malo primerov tožb spamerjev, čeprav gotovo prihaja do številnih kršitev in pritožb zaradi pošiljanja nenaprošenih e-pošt in obdelovanja osebnih podatkov, ki ni v skladu z zakonom.

Zakoni odvrnejo nekaj pošiljateljev od nezakonite uporabe e-pošte, še vedno pa je relativno visok delež spamov v celotni e-pošti. Torej so zanje odgovorni še drugi dejavniki, kot je nadzorni organ, dolgi postopki, neprimerni zakoni, neprepoznavnost pošiljatelja in različni posameznih skupin. Poznavalci namreč menijo, da bi popolno onemogočanje zbiranja podatkov precej zmanjšalo funkcionalnost spleta, verjetno pa tudi zaustavilo razvoj internetne ekonomije. Zato želijo z zakonodajo le vzpostaviti ravnotežje v sistemu, ki ne bi uničeval e-pošte kot orodja komunikacije, niti ne bi zatrl ekonomske rasti posameznih podjetij.

5.3.2 Regulacija spama v ZDA

Dolgoletne razprave o regulaciji spama v Ameriki so se lansko leto zaključile s prejetjem skupnega zakona, ki omejuje pošiljanje nanaprošenih komercialnih sporočil (UCE). Na nacionalni ravni so do sedaj spam omejili v 36 zveznih državah. Zakoni držav so osnovani na skupni osnovi. Razlikujejo se v posameznih določbah, ki so si v nekaterih primerih celo nasprotujoče.

[33] Člen 13 (4), Direktiva o zasebnosti v elektronski komunikaciji (http://www.spamlaws.com/docs/2002-58-ec.pdf).

5.3.2.1 Odstopanja pri definiranju spama

Neenotnost zakonov se kaže že v najpomembnejšemu sestavnemu delu zakona, v definiciji spama. Države so se pri opredelitvi predvsem omejile na regulacijo komercialnih e-sporočil. Zaradi tveganja poseganja na področje komunikacije, ki jo ščiti svoboda govora, se pri opredelitvi spama ne nanašajo na množična sporočila političnih, verskih in podobnih vsebin. Dejstvo je namreč, da komunikacijo z namenom oglaševanja, zakon o svobodi govora ščiti manj. Države, ki omejujejo pošiljanje množičnih sporočil zatorej poudarjajo, da velja to le v primerih, v katerih se e-pošta prenaša na neresnične informacije in so v nasprotju s pravili ponudnikov pošiljanja e-pošte. Nekatere države v zakonu spam opredelijo le kot e-pošto z eksplicitno seksualno vsebino.

Glede kršenja prvega ustavnega zakona »svobode govora« so borci za preprečitev spama na internetu slišali številne očitke podjetij in oglaševalcev. Trdijo, da preprečevanje pošiljanja kakršnekoli e-pošte izraža nespoštovanje ustave in nepošteno prepoved posameznih oblik komunikacije. Paul Graham odločno zanika takšne obtožbe, saj meni, da svoboda govora ne daje pravice nadlegovanja in sledenja drugim osebam. Dodaja še, da svoboda govora ni zaščitena od točke, od katere je govor za druge neprijeten in nadležen (Graham; www.paulgraha.com/spamdiff.html, 2).

Znotraj posameznih definicij UCE, UBE in e-sporočil s seksualno vsebino prihaja še do dodatnih razhajanj pri opredeljevanju pojmov[34]. UCE torej večina držav opiše kot e-pošto, ki jo pošlje pošiljatelj potrošnikom, s katerimi predhodno še ni vzpostavil poslovnega stika, niti nima njihovega dovoljenja za pošiljanje takšnih sporočil. Vsebina sporočila se navezuje na oglaševanje zakupa, prodaje, izposoje, menjave, ponudbe ali darovanja izdelkov in/ali storitev ter podaljševanja kredita in investiranja. Seveda pa tudi pri definiranju UCE prihaja do velikih razhajanj med državami. Države, kot je Connecticut, ki je zakon sprejela že leta 1999 in je do danes ostal nespremenjen, v njem sploh ne opredeljuje niti UCE niti UBE, medtem ko Kansas iz UCE izloča vsa sporočila, ki oglašujejo zaradi dobrodelnih namenov.

Zakoni različno opredeljujejo tudi predhodne poslovne stike. Večina jih definira kot odnose, ki so nastali pri poslovnih transakcijah ali komunikacijah. V Arkansasu takšnim odnosom določijo rok trajanja 5 let in se prekinejo, če je prejemnik v tem času zaprosil za izbris iz seznama prejemnikov.

Kljub raznolikosti zakonov, ki različno opredeljujejo posamezne določbe zakona, internetni ponudniki za filtriranje in blokiranje spamov zaenkrat še nimajo zakonske podpore. Kriterije zaprošene oz. nezaprošene e-pošte spuščajo le na nivo vpletenih prejemnikov sporočil.

5.3.2.2 Problem razdrobljenosti zakonov po posameznih državah

Internet je globalni fenomen, njegova regulacija pa se je do sedaj v Ameriki vršila le na nacionalni ravni. Odgovornost zakonov je bila geografsko omejena. Zakon je zadeval samo spamerje, ki pri pošiljanju e-pošte uporabljajo storitev internetnega ponudnika posamezne države ali so nezaprošeno e-pošto poslali njenim državljanom.

Podatek, da je 36 držav sprejelo zakon proti spamu in kar skoraj ena četrtina od teh v lanskem letu, kaže na resen problem in zaskrbljenost odgovornih v posameznih državah. Vsaka država je ne glede na druge sprejela zakon, ki naj bi optimalno omejeval pošiljanje spamov, dejansko pa raznolikosti in geografska omejenost delovanja zakona hromita njegovo moč. Kolikor je držav, toliko je variacij določb zakona, ki omejujejo pošiljanje UCE ali UBE ali e-pošte z eksplicitno seksualno vsebino.

Nobena organizacija, društvo ali država ne morejo reševati težav znotraj sebe brez usklajenosti in homogenega delovanja na vseh ravneh. Prav tako je nemogoče pri takšni zmedi prepovedi in zapovedi znotraj ZDA omejiti pošiljanje spama. Mogoče bo novo sprejeti zakon povezal razdrobljenost med posameznimi državami.

5.3.2.3 E-naslov ne pove veliko o izvoru sporočila

Izvor posamezne e-pošte je zelo težko določiti, največkrat to sploh ni mogoče. Skoraj nemogoče je, da prejemnik kot fizična oseba pride do vira e-pošte. Izurjeni in sofisticirani spamerji izkoriščajo odprte povezave in druga orodja, s katerimi zakrijejo vse sledi povezav med prejemnikom in pošiljateljem. Vedno bolj izpopolnjene tehnologije omogočajo spamerjem, da obidejo filtre in blokade ter ostanejo anonimni.

Za pošiljanje množične e-pošte spamerji največkrat uporabljajo storitve brezplačnih ponudnikov e-pošte, ki omogočajo odprtje enkratnega računa. E-naslov, iz katerega pošiljatelj

[34]Glej spam zakone v posameznih državah, www.spamlaws.com/state

pošlje več tisoč e-sporočil, se takoj po kliku na funkcijo »pošlji« zapre in ne obstaja več. Niti kanček upanja ni, da bi takšnemu pošiljatelju prepovedali nadaljnje pošiljanje nezaželenih sporočil, prepoznali njegovo identiteto, kaj šele ga zakonsko preganjali.

5.3.2.4 Antispam zakoni v posameznih državah

Raznolikost in hkrati podobnost ameriških zakonov na nacionalni ravni je privedla celo do nasprotovanj in nerazumljivosti določb posameznih držav. Večina držav ne prepoveduje spama kot takega, ampak ga le omejuje z določbami, ki narekujejo, v katerih primerih je njegovo pošiljanje prepovedano.

Spodaj opisane glavne določbe zakonov so v prilogi E povzete za vse države, ki imajo antispam zakon.

Pošiljanje resničnih informacij

Skoraj vse države, ki so sprejele antispam zakon, jasno prepovedujejo pošiljanje neresničnih informacij. Nekatere dodatno poudarjajo, da je prepovedano napačno navajanje e-naslova pošiljatelja in predmetne oznake sporočila, ki povzroča zavajanje prejemnikov.

Računalniške programe za ponarejanje informacij, ki krožijo med prejemniki, prepoveduje le ena tretjina držav. Zakoni držav označujejo distribucijo ali prodajo takšnih programov v določenih okoliščinah kot kriminalno dejanje.

Veljavnost e-mail naslovov

Zaradi ogorčenosti in posledičnih pritožb jeznih prejemnikov spamerji redkokdaj uporabljajo svoje resnične e-naslove. Neveljavni e-naslovi onemogočajo določitev vira e-pošte, od katerega bi prejemniki zahtevali izpis iz seznama in mu prepovedali nadaljnjo pošiljanje nezaželenih sporočil brez dovoljenja. »Opt-out« določbo, ki že sama po sebi zahteva veljaven naslov pošiljatelja, je uzakonilo dve tretjini držav.

»Opt-out« in »opt-in« predpis

Države, ki so sprejele »opt-out načelo«, omogočajo prejemnikom, da se sami odločajo o nadaljnjem prejemanju takšnih sporočil. Za izvedbo postopka skoraj vse države zahtevajo razkrito identiteto in veljaven naslov pošiljatelja, kontaktne informacije in jasna navodila za

brezplačen izpis iz seznama. Z izpisom prejemniki zavrnejo prejemanje e-sporočil v prihodnje.

»Opt-in« predpis sta do sedaj uzakonili le Kalifornija in Delaware in dopuščata pošiljanje e-pošte, če je to prejemnik vnaprej dovolil oz. se vpisal v seznam in s tem izrazil željo prejemanja sporočil.

Predmetne oznake sporočil prepoznavne filtrom

Skoraj dve tretjini držav predpisuje predmetno oznako e-pošte. Z »ADV« naj bi bila označena sporočila z oglaševalsko vsebino, z »ADLT« pa sporočila, katerih vsebina je namenjena odraslim. Oznake omogočajo prejemniku takojšno prepoznanje in ločevanje spamov od legitimne e-pošte. Z upoštevanjem teh dveh pravil bi bili filtri veliko bolj učinkoviti, vendar kot kaže FTC razikava, le 2 % spamov vsebuje oznako ADV ali ADLT. Očitno se spamerji ne zmenijo niti zanje niti za zakone.

Kljub pomanjkljivosti (opredeljeno ni niti množično pošiljanje niti nenaprošena e-pošta), poznavalci ocenjujejo, da je država Delaware sprejela najbolj restriktivni antispam zakon. Prepoveduje pošiljanje vsakršne množične komercialne e-pošte, ki krši računalniški zakon. Prepoveduje brezobzirno in brez namena in dovoljenja pošiljati e-pošto na katerikoli veljavni naslov v računalniškem sistemu. Kaznivo je pošiljanje neresničnih informacij in programov, ki spodbujajo kroženje takšnih informacij. Zakon zapoveduje tudi upoštevanje »opt-in« predpisa.

V posameznih državah so predlagali še nekatere druge rešitve, kot so centralni »opt-out« register, register domen za operaterja prejemnika, enkratni spam, ki se zaradi predvidene neučinkovitosti in/ali nesmiselnosti ali zaradi premajhnih ambicij odgovornih, še do danes niso uresničile.

5.3.2.5 Enotni antispam zakon v ZDA

Sprejemanje antispam zakonov na zvezni ravni je bilo do sedaj neuspešno. Vsako leto obravnavata senat in spodnji dom ameriškega kongresa številne osnutke zakonov, ki jih predlagajo posamezniki in organizacije iz obeh političnih struj. Prav tako kot nacionalni zakoni se tudi zvezni predlogi zakonov med seboj skoraj ne razlikujejo.

106. Kongres

Na 106. Kongresu je bilo predstavljenih 10 zakonskih osnutkov, ki se po vsebini skoraj ne razlikujejo od nacionalnih zakonov. Izjeme so le predlogi »Can spam act«, »Inbox privacy act« in »Unsolicited electronic mail act«. Za slednjega so napovedovali uspešno uzakonjene na 107. Kongresu, kar pa se ni zgodilo. Predlog zakona poleg že znanih omejitev, ki govorijo o označevanju UCE-jev z »ADV« in »ADUL«, o navodilih za »opt-out« in prepovedi kroženja neresničnih informacij, dodaja še prepoved kršenja pravil ponudnikov interneta, če so le-ta objavljena na spletni strani ali so na razpolago FTC-ju (glej http://www.spamlaws.com/federal/list106.html).

Tudi »Can spam act« poleg že znanih določb predlaga novo metodo kontroliranja z mehanizmom »no-spam« SMTP pasicami. Pasico naj bi administrator serverja oblikoval in jo poslal med vse ostale, od katerih prejema e-pošto.

»Inbox privacy act« med drugim predlaga FTC kot mehanizem oblikovanja pravil in nadzor za njihovo izpolnjevanje. Lastnikom domen naj bi bila dodeljena pravica »opt-out« vseh e-naslovov znotraj domene ob registraciji pri FTC.

Popolnoma nov je predlagani osnutek zakona, ki naj bi omejeval spam na področju mobilne telefonije, kjer se problem že pojavlja, a še ne povzroča večjih težav. Predlog prepoveduje pošiljanje tekstovnih, grafičnih ali slikovnih, kratkih in nezaprošenih sporočil s komercialno vsebino. Predlog vse do danes ostaja le predlog brez moči.

107. Kongres

Na kongresu sta bila prestavljena dva nova zakona, ki se zavzemata za zaščito pravic otrok na internetu preko e-pošte. Predloga zahtevata označevanje vse e-pošte, posebno tiste s pornografsko vsebino, ter sprejetje enotnih pravil na vseh šolah in v knjižnicah, ki bi prepovedala anonimnost e-pošte. Tudi ta kongres se je končal brez korenitih sprememb in rešitev, ki si jih želimo vsi uporabniki e-pošte (glej http://www.spamlaws.com/federal/list107.html).

108. Kongres

Končno so ZDA dočakale prvi zakon, imenovan »CAN-SPAM ACT«, ki ureja področje pošiljanja nepovabljenih komercialnih sporočil na območju vseh Združenih Držav Amerike. Zakon, katerega snovatelj je Sen Burns, je kongres sprejel 22. oktobra 2003 in je enoten v vseh Združenih državah Amerike. V veljavo je stopil 1.januarja 2004 in opredeljuje »unsolicited commercial e-mail« (nepovabljeno komercialno e-sporočilo) kot katerokoli komercialno sporočilo, iz katerega ni razviden odnos ali dialog med pošiljateljem in prejemnikom in je poslano brez vnaprejšnjega dovoljenja prejemnika. Pošiljatelju, ki brez pooblastil uporablja dostop do zaščitenega računalnika, ponareja informacije v glavi dokumenta, se registrira z izmišljenimi identifikacijskimi podatki in se predstavlja z namišljenimi pravicami dostopanja do petih naslovov internetnih protokolov zaradi pošiljanja množičnih[35] komercialnih sporočil, zakon nalaga kazen od 25 dolarjev za posamezno sporočilo do ne več kot 1 milijon dolarjev in/ali do 5 let zapora. Zakon tudi ne dopušča pošiljanja zavajajočih in neresničnih informacij v besedilu in glavi e-sporočila, zahteva podatke, ki identificirajo e-sporočilo in pošiljatelja, veljavni e-naslov pošiljatelja in možnost izpisa iz seznama. Od pošiljatelja se pričakuje upoštevanje načela »opt-out« in pravilno označevanje predvsem tistih sporočil, ki imajo seksualno vsebino. Nelegalno je avtomatično pridobivanje e-naslovov in pošiljanje e-sporočil (glej Can Spam Act of 2003, http://www.spamlaws.com/federal/108s877.html).

Zakon pooblašča FTC za spremljanje nepravilnosti in poseganje v posamezne primere kršitve, za analiziranje učinkovitosti zakona v praksi in poročanje o morebitnih slabostih ter predlaganje izboljšav. Zaradi uspešnega »do-not call« registra, s katerim so zadovoljni tudi končni uporabniki, FTC-ju zakon dodeljuje odgovornost kreiranja in spremljanja delovanja »do-not-mail« registra.

Tudi Amerika je na področju spama stopila iz svoje apatičnosti in skuša z enotnim zakonom omejiti pošiljanje nezaželenih e-sporočil. Njegove določbe prepovedujejo in kaznujejo pošiljanje le nepovabljenih komercialnih e-sporočil, tako da je še vedno zagotovljena svoboda govora in dovoljeno pošiljanje sporočil z nekomercialno vsebino: ankete, peticije, politična in virska propaganda, sporočila dobrodelnih organizacij. Zakon izrecno prepoveduje pobiranje (ang. harvesting) e-naslovov iz različnih spletnih strani z računalniškimi programi in brez

dovoljenja potencialnih prejemnikov. Učinkovitosti zakona v tem trenutku še ni moč določiti, njegove lastnosti in uspešnost v praksi bo pokazal čas.

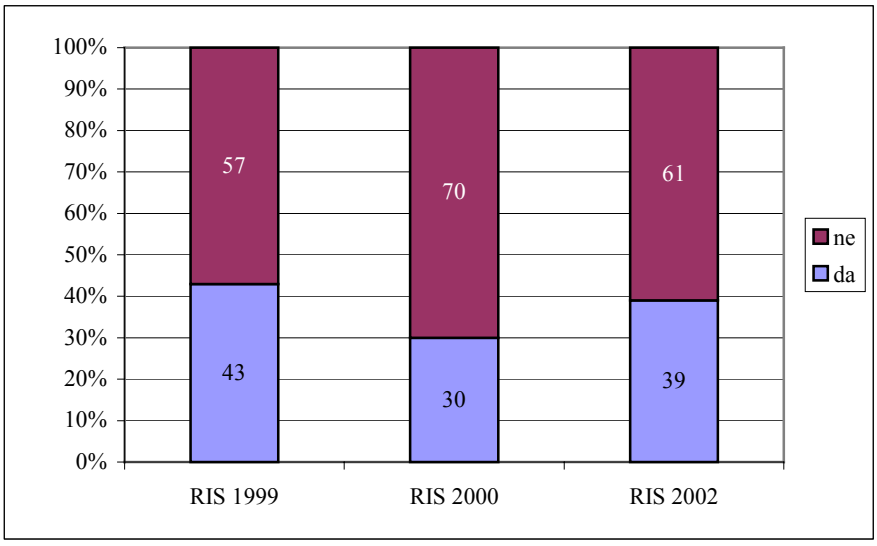
[35] »množično sporočilo« je sporočilo poslano na več kot 100 različnih e-naslovov v 24 urah ali na več kot 1000 e-naslovov v 30 dneh ali na več kot 10000 e-naslovov v času 1 leta

6 SPAM V SLOVENIJI

V Sloveniji v preteklih letih nismo doživeli večjih prelomnic v učinkovitosti spletnega trženja in uporabi sodobnejših računalniških orodij. Z naraščanjem internetne osveščenosti in s tem tudi števila njegovih uporabnikov, so se začele kazati prve smernice razvoja, ki so v zadnjem času vse bolj jasne. Opazen je večji razmah trženja z e-pošto, ki je v nekaterih primerih izveden celo legitimno in je v večini primerov povezan z izdajanjem e-publikacij, s katerimi podjetja ne le tržijo svojo ponudbo, temveč tudi izobražujejo svoje potencialne in obstoječe stranke.

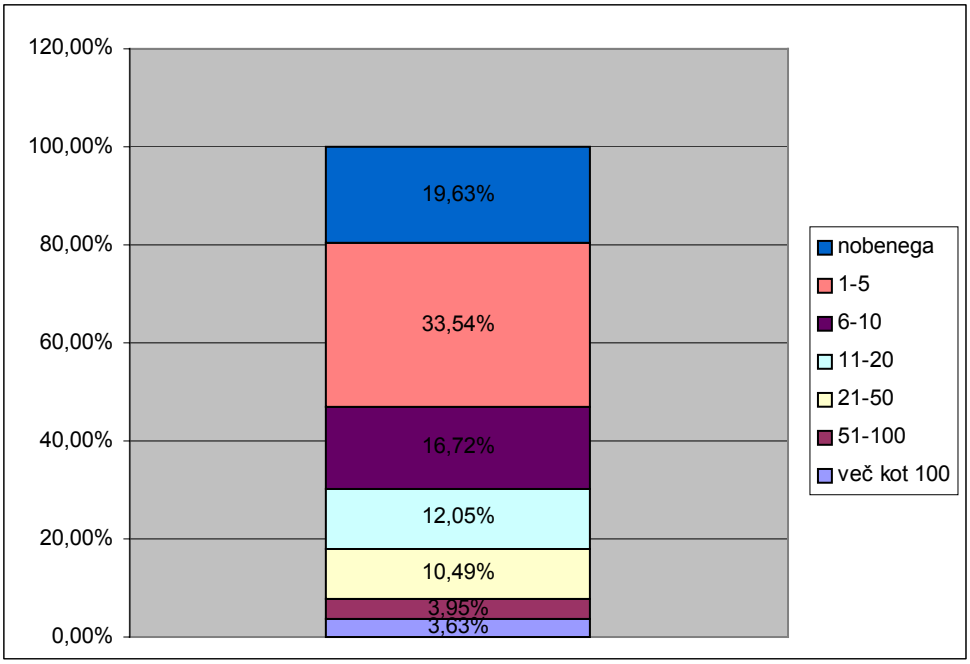
Problem nezaželene e-pošte je vsako leto izrazitejši in močnejši v zadnjem času. Tudi pri nas narašča število spamerjev, ki brez dovoljenj pošiljajo ponudbe, zgodbe, šale, slike in podobne vsebine na vse razpoložljive e-naslove. Potrošnike kot žrtve tovrstnih sporočil je država zaščitila z novim zakonom in z visokimi kaznimi spodbudila pošiljatelje k pridobitvi dovoljenj potencialnih prejemnikov.

Na temo spam je RIS junija 2002 izvedel telefonsko raziskavo. Njegove ugotovitve temeljijo na podatkih zbranih s telefonsko anketo med uporabniki interneta splošne populacije. Nekateri rezultati so pokazatelji trenda, ker so primerjani z ugotovitvami raziskav iz predhodnih let.



Slika 6.6: Ali ste že kdaj prejeli nezaželena komercialna e-mail sporočila oz. sporočila neznanih oseb, imenovana tudi spam? Vir: RIS 1999; RIS 2000; RIS 2002, n=234.

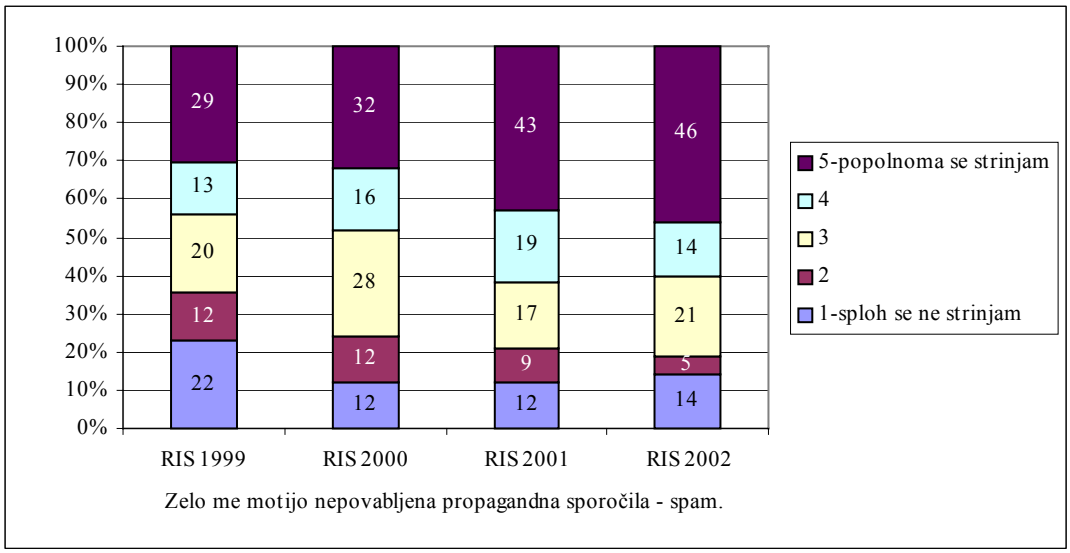
Rezultati kažejo, da v letu 2002 dobra tretjina (39 %) uporabnikov interneta prejema nezaželena komercialna e-sporočila. Odstotek prejemnikov, ki prejemajo takšna sporočila, se je v primerjavi z letom 2000 (30 %) povečal, v primerjavi z letom 1999 (43 %) pa se je zmanjšal. Nazadovanje v letu 2000 je mogoče pripisati hitri rasti uporabnikov interneta. Začetniki so načeloma manj intenzivni in redko uporabljajo e-naslov.



Slika 6.7: Koliko nezaželenih sporočil dnevno prejmete v svoj elektronski poštni nabiralnik? Vir: Siol v Skrt, september 2003, n=963.

Siolova anketa, izvedena na njihovi spletni strani, kaže, da je v letu 2003 delež prejemnikov nezaželenih sporočil zelo visok (80,37 %), od tega kar tretjina uporabnikov e-pošte prejme dnevno do 5 nezaželenih sporočil.

V primerjavi z rezultati RIS-ove raziskave iz leta 2002 je odstotek prejemnikov še enkrat večji. Število uporabnikov interneta narašča, vendar si tako velike razlike lahko razložimo z različnim načinom izvajanja anketiranja. Respondenti Siolovega vprašalnika so uporabniki interneta, ki so slučajno opazili in izpolnili vprašalnik. Respondenti RIS-ove ankete pa so mesečni uporabniki, tako začetniki kot vešči »deskarji« spletnih strani.



Slika 6.8: Odnos do nezaželenih komercialnih e-sporočil – primerjava, vir: RIS 1999, RIS 2000, RIS 2001, RIS 2002.

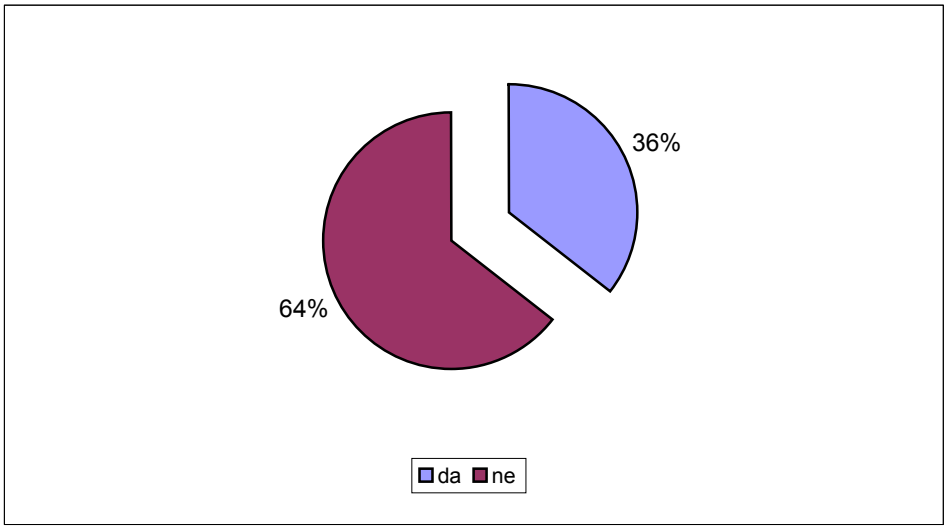
Skoraj polovica mesečnih uporabnikov se popolnoma strinja s trditvijo »*Zelo me motijo nepovabljena propagandna sporočila – spam*«. Nenaklonjenost do spama raste, saj mu nasprotuje že 60 % uporabnikov interneta. Povečanje nezaželenosti do spama na podlagi podatkov iz telefonskih anket si lahko razložimo s povečanjem števila takšnih množičnih oglasnih sporočil, saj so uporabniki, ki že več let uporabljajo internet, temu bolj izpostavljeni. Na velik porast spama v Sloveniji kaže tudi RIS-ova raziskava iz leta 2002, ki navaja, da spam zavzema kar 45 % celotne e-pošte. Glede na celotno populacijo mesečnih uporabnikov interneta - 570,000 (junij 2002), pa vsi uporabniki interneta mesečno prejmejo dobrih 11 milijonov spamov (RIS, 2003:3).

6.1 Raziskava o razširjenosti spama med študenti EF in FDV

V letu 2002 smo med študenti Ekonomske fakultete in Fakultete za družbene vede izvedli raziskavo. Želeli smo ugotoviti, kakšna je razširjenost spama med študenti, kako jih motijo tovrstna sporočila in kakšen odnos imajo do njih ter ali menijo, da bi bilo treba to področje zakonsko urediti. Vzorec ankete, ki je bil izbran kvotno, je obsegal 101 učenca EF in FDV. Ankete so študentje izpolnjevali sami v predavalnicah. Stopnja anketiranja je bila stoodstotna.

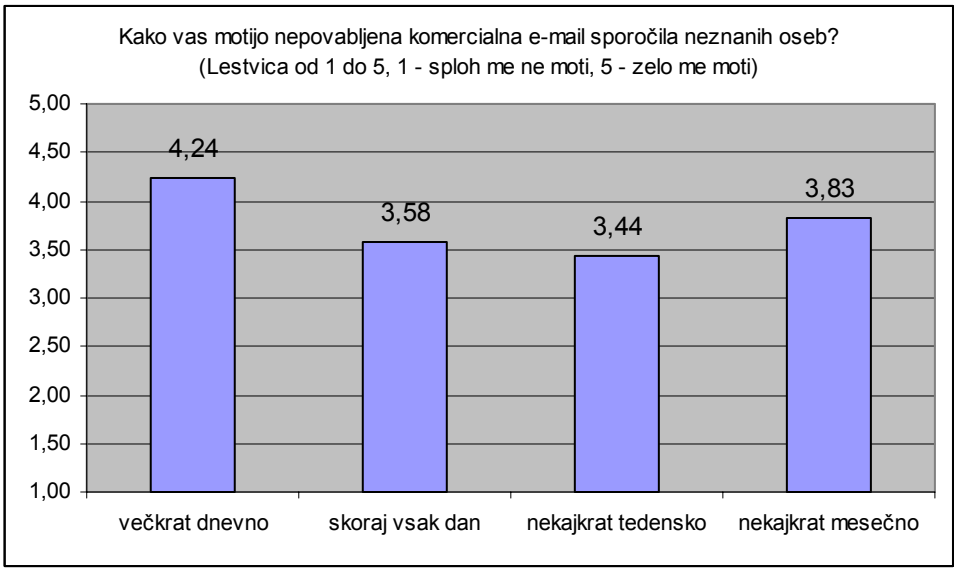
Tabela 6.2: Demografske značilnosti anketiranih oseb, Vir: Raziskava razširjenosti spam sporočil med študenti EF in FDV 2002, n=101.

		Frekvence	%
Fakulteta	FDV	51	50,5
	EF	50	49,5
Spol	Moški	51	50,5
	Ženske	50	49,5
Starost	od 18 do 21	52	51,5
	od 22 do 27	49	48,5



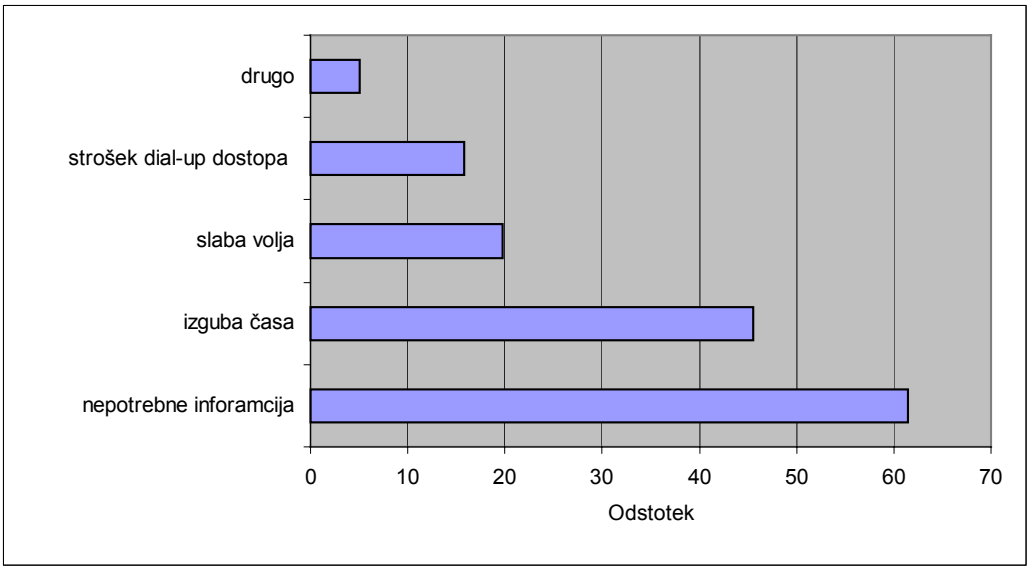
Slika 6.9: Porazdelitev odgovorov na trditev »Še nikoli nisem prejel spam sporočil.«, Vir: Raziskava razširjenosti spam sporočil med študenti EF in FDV, 2002.

Dobra tretjina (64 %) anketiranih študentov še ni prejela nezaželene e-pošte – spam.



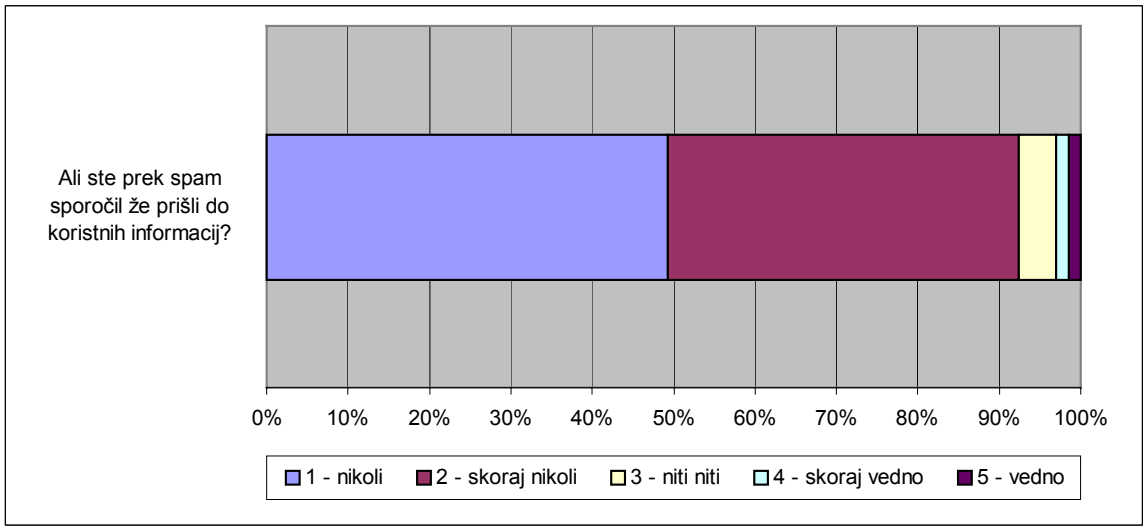
Slika 6.10: Ocene anketiranih študentov za obseg motnje spam sporočil glede na pogostost uporabe interneta, Vir: Raziskava razširjenosti spam sporočil med študenti, 2002.

Nepovabljena komercialna e-sporočila najbolj motijo tiste študente, ki uporabljajo internet večkrat dnevno in nekajkrat mesečno. Motečnost je nižja pri tistih, ki uporabljajo internet nekajkrat tedensko.



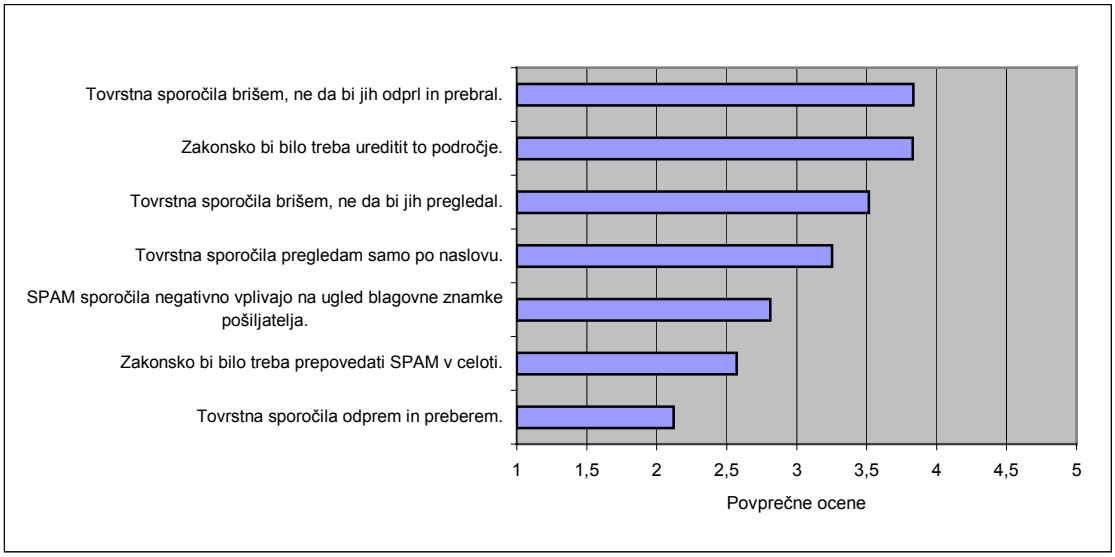
Slika 6.11: Porazdelitev odgovorov na vprašanje »Zakaj vas moti spam oz. bi vas motil, če bi ga prejeli (možnih več odgovorov)?«, Vir: Raziskava razširjenosti spam sporočil med študenti EF in FDV, 2002.

Spam sporočila več kot polovici študentov predstavlja nepotrebne informacije. Skoraj polovica meni, da z njimi izgubljajo čas, petini povzroča slabo voljo. Več kot desetina študentov se zaveda, da predstavljajo spam sporočila strošek dial-up dostopa.



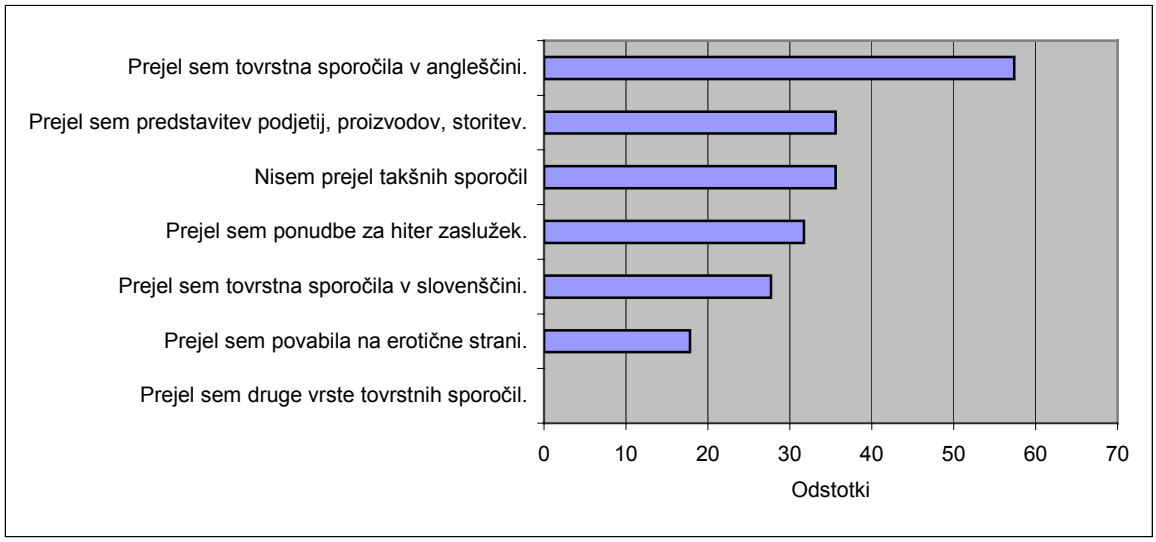
Slika 6.12: Porazdelitev odgovorov anketiranih študentov na vprašanje »Ali ste prek spamov že prišli do koristnih informacij?«, Vir: Anketa o spamu, december 2001.

Spam sporočila niso vir koristnih informacij po mnenju več kot 90 % študentov. To potrjuje tudi spodnja slika, ki kaže, da večina študentov do vsebinskega dela sploh ne pride, saj spam sporočila kategorično brišejo.



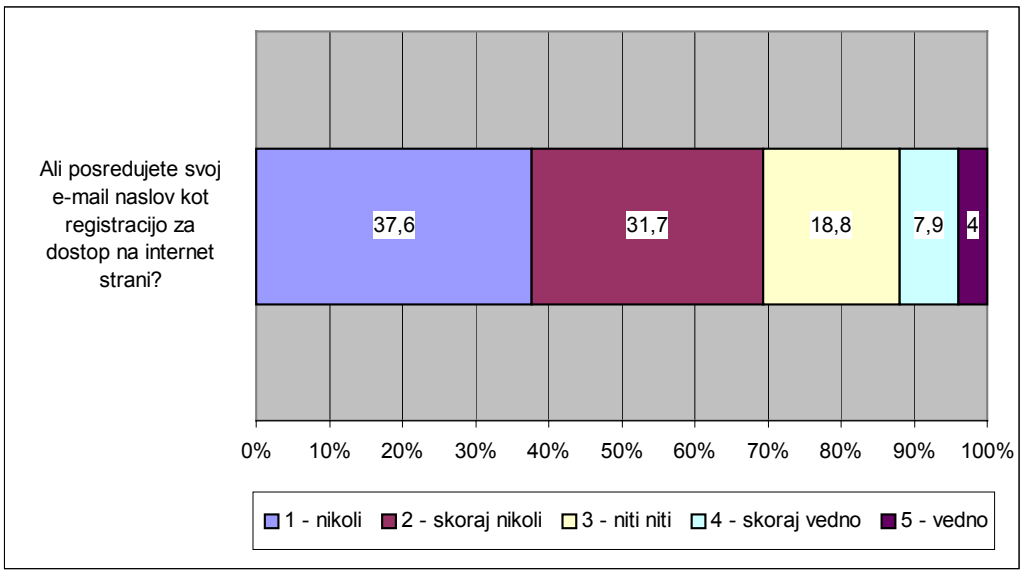
Slika 6.13: Povprečne ocene za nekaj trditev o problematiki v zvezi s spamom, Vir: Raziskava razširjenosti spam sporočil med študenti, 2002.

Respondnti se najbolj strinjajo s trditvama, da spam sporočila brišejo, ne da bi jih odprli in prebrali, ter da bi bilo treba to področje zakonsko urediti, najmanj pa, da tovrstna sporočila odprejo in preberejo.



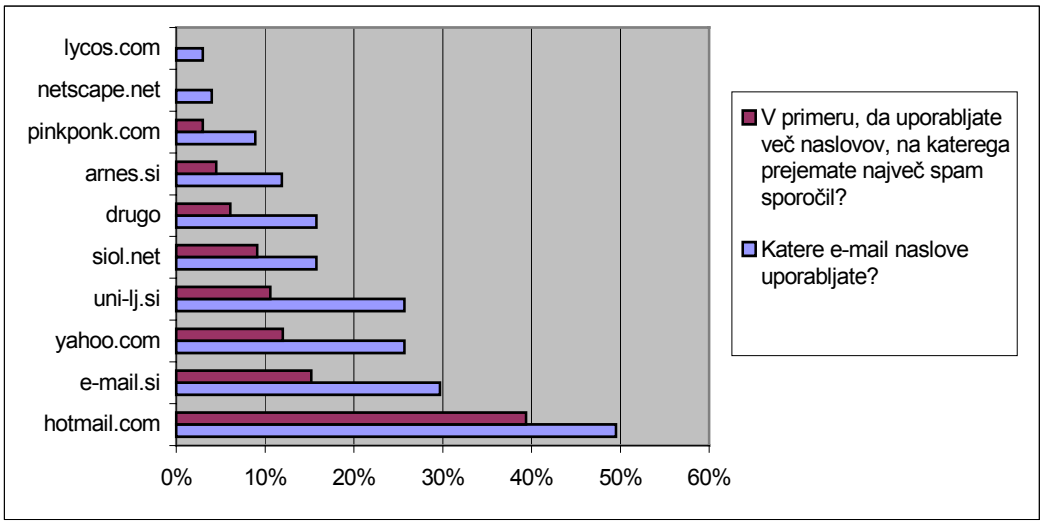
Slika 6.14: Porazdelitev odgovorov na vprašanje »Ali ste že kdaj prejeli spam?«, Vir: Raziskava razširjenosti spam sporočil med študenti, 2002.

Slika kaže, da je večina študentov prejela spam sporočila v angleščini, delež prejetih spamov v slovenščini je precej manjši. Dobra tretjina meni, da se vsebina spam sporočil nanaša na predstavitev podjetij, proizvodov in storitev.



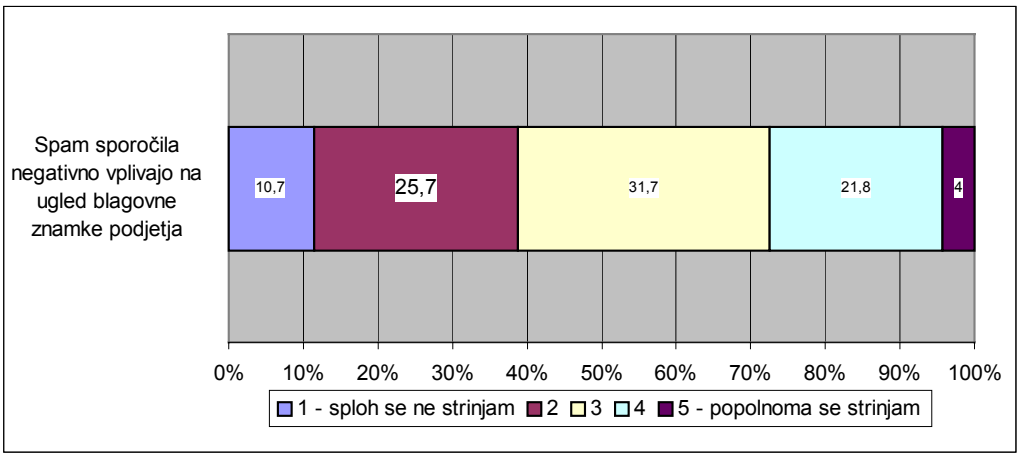
Slika 6.15: Porazdelitev odgovorov na vprašanje »Ali posredujete svoj e-mail naslov kot registracijo za vstop na internet strani?«, Vir: Raziskava razširjenosti spam sporočil med študenti, 2002.

Večina spletnih strani za dostop do informacij zahteva posredovanje e-naslova, ki ga pozneje koristijo za pošiljanje nezaželenih sporočil. Takšni načini so študentom dobro poznani, saj le dobra desetina (11,9 %) posreduje svoj e-naslov v te namene.



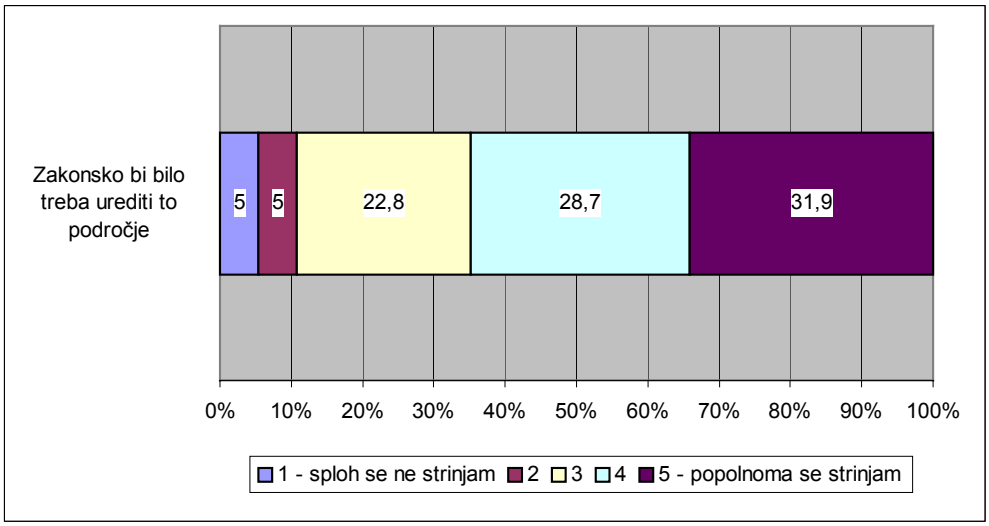
Slika 6.16: Primerjava porazdelitve odgovorov anketiranih študentov na vprašanji «Kateri e-mail naslove uporabljate?« in »V primeru, da uporabljate več e-mailov, na katerega prejemate največ spamov?«, Vir: Raziskava razširjenosti spam sporočil med študenti, 2002.

Najpogostejši e-naslov, ki ga uporabljajo, je »hotmail.com« (skoraj 50 % študentov), sledi mu »email.si« (slaba tretjina), tretje mesto najpogosteje uporabljenega e-naslova si delita »yahoo.com« in »uni-lj.si«, ki ju uporablja dobra četrtina. Študentje, ki imajo več e-naslovov, največ spam sporočil prejemajo na hotmail naslov.



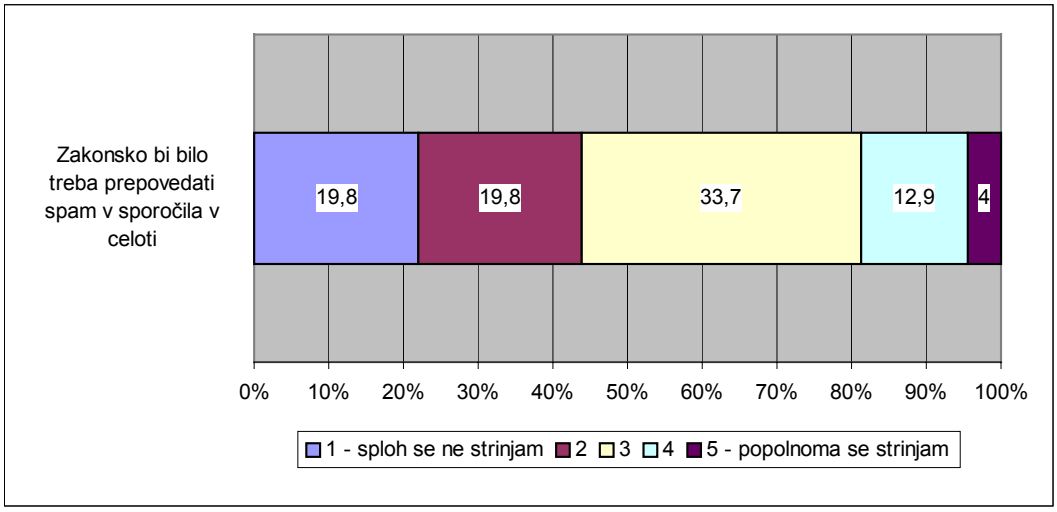
Slika 6.17: Porazdelitev odgovorov anketiranih študentov na trditev » Spam sporočila negativno vplivajo na ugled blagovne znamke pošiljatelja.«, Vir: Raziskava razširjenosti spam sporočil med študenti, 2002.

Prejeta sporočila očitno nimajo velikega vpliva na ugled blagovne znamke podjetja, saj manj kot tretjina študentov (25,8 %) meni, da imajo takšna sporočila negativen vpliv na blagovno znamko.



Slika 6.18: Porazdelitev odgovorov na trditev «Zakonsko bi bilo treba urediti področje spam sporočil«, Vir: Raziskava razširjenosti spam sporočil med študenti, 2002.

Velika večina študentov (60,4 %) se strinja, da bi morali področje spam sporočil zakonsko regulirati. Podatek je presenetljiv, glede na razmeroma majhen delež študentov, ki so že prejeli spam sporočila.



Slika 6.19: Porazdelitev odgovorov na trditev »Zakonsko bi bilo treba prepovedati spam sporočila v celoti.«, Vir: Raziskava razširjenosti spam sporočil med študenti, 2002.

Kljub temu, da se večina strinja, da je potrebna zakonska omejitev spam področja, se presenetljivo majhen delež (16,9 %) strinja s trditvijo, da bi bilo treba spam sporočila v celoti prepovedati.

V času raziskave je obstajal relativno visok delež študentov (64 %), ki spam sporočil še niso prejeli, kljub temu pa je njegova motečnost precej visoka. Prevladujejo spam sporočila v angleškem jeziku. Odnos do tovrstnih sporočil je precej slab, saj dobra polovica študenotv trdi, da njihova vsebina predstavlja le nepotrebne informacije, ravno toliko jih odobrava zakonsko ureditev tega področja. Kljub motečnosti spam sporočil le petina študentov meni, da bi jih bilo treba zakonsko prepovedati v celoti. Najbolj zanimivo pa je to, da le slaba tretjina respondetnov misli, da takšna sporočila negativno vplivajo na ugled blagovne znamke.

6.2 Motečnost spama pri ponudnikih interneta

Zaposleni na Arnesu in Voljatelu (priloga F) tarnajo, da se tedensko srečujejo z neprijetnostmi, ki jih povzročajo prevelike količine spama. Problemi se kažejo neposredno na preobremenjenosti poštnega strežnika, posredno pa na nezadovoljstvu uporabnikov, povišanih stroških delovanja in če je spam sredstvo prenosa nevarnih virusov, so posledice še hujše. Ponudniki interneta v ta namen uporabljajo filtre, ki najbolj ustrezajo njihovim potrebam. Na Arnesu menijo, da ne obstajajo 100-odstotno zanesljivi filtri. Tudi njihov sistem, ki temelji na odprti kodi in dopušča uporabniku možnost nastavitve filtracije in pregleda »spam mape«, v kateri so zbrane vse izločene e-pošte, ima nekaj pomanjkljivosti, skupne vsem filtrirnim sistemom: nezanesljivost, obremenitev strežnika in dodatno vzdrževanje.

Tudi internetni ponudniki so nemočni v boju proti spamerjem, ki pošiljajo nezaželeno e-pošto iz tujine. V takšni situaciji lahko le opomnijo spamerja preko ponudnika, ki mu je omogočil pošiljanje tovrstnih e-sporočil. Ponudniki so bolj uspešni v boju s slovenskimi spamerji, saj lahko sprožijo postopek pri tržnemu inšpektoratu, ki pošiljatelju na podlagi dokazov izreče visoko denarno kazen.

Oba ponudnika trdita, da vešči pošiljatelji spretno ohranjajo svojo anonimnost z uporabo odprtih povezav in proksi strežnikov, neobstoječih domen in neresničnih podatkov v glavi sporočil. Na Arnesu menijo, da so neosveščenost uporabnikov, dostopnost in zmožnost

tehnologij ter pomanjkanje regulacije glavni dejavniki, ki spodbujajo obseg takšnih sporočil. Na Voljatelu pa krivdo pripisujejo odzivnosti prejemnikov.

Kot pomanjkljivosti učinkovite regulacije spam sporočil oba ponudnika navajata neosveščenost uporabnikov in neusklajenost na vseh področjih. Na Arnesu so prepričani, da že sam koncept interneta onemogoča kakršnokoli »dokončno« rešitev.

Spam v Sloveniji po oceni obeh ponudnikov interneta zavzema od 30 % do 40 % delež med e-pošto. Ponudniki so seznanjeni z novim slovenskim antispam zakonom in močno dvomijo v njegovo visoko učinkovitost. Arnes mu pripisuje slabost, ker je pošiljatelj odgovoren za svoja dejanja le v primeru, da pošilja e-sporočila na osebne naslove. Zakon o varstvu potrošnikov v 45.a členu ne omejujeje e-pošte, poslane na generične naslove (npr. mojepodjetje.si). Oba ponudnika pa se strinjata, da je učinkovitost odvisna predvsem od izvajanja in pristojnosti inšpekcije, ki nadzoruje to področje.

6.3 Zakonska ureditev spama

V letu 2003 je tudi Slovenija naredila prve korake na področju spama in tako zaščitila zasebnost potrošnikov pred vdorom nezaželenih, oglaševalskih e-sporočil. Po zgledu direktiv Evropske unije je pri nas v veljavi zakon, ki omejuje pošiljanje nezaželene e-pošte. Glede na to, da je spam področje močno povezano z varstvom osebnih podatkov, je treba omeniti, da že naša ustava v 38. členu prepoveduje zlorabo osebnih podatkov (glej Ustava RS, http://www.us-rs.si/si/basisfr.html).

Zakon o varstvu potrošnikov, ki v 45.a členu regulira področje spama, je stopil v veljavo 17. januarja 2003. Pri oblikovanju zakona je bila upoštevana in povzeta direktiva EU, in sicer 2000/31 EC (člen 6 in 7) in 97/7 EC (člen 10). Zakon določa, da lahko podjetje uporablja e-pošto samo *z vnaprejšnjim soglasjem* posameznega potrošnika, ki mu je sporočilo namenjeno. Pri tem gre za načelo »opt-in«, ki velja kot izjema. Splošno »opt-out« načelo določa, da je uporaba individualnih komunikacijskih sredstev dovoljena, če se potrošnik s tem strinja. V primeru, da ne želi več prejemati sporočil, ki so namenjena sklenitvi pogodbe za dobavo kateregakoli blaga ali storitve, mora podjetje upoštevati njegovo željo in ne sme več pošiljati sporočil (glej Uradni list, člen 45a, http://objave.uradni-list.si/bazeul/URED/2003/014/B/525663109.htm). Sankcije za nespoštovanja zakona so

precej stroge, saj se lahko posameznika kaznuje z denarno kaznijo najmanj milijon tolarjev, pravno osebo pa z najmanj tremi milijoni tolarjev (Uradni list, člen 77, http://objave.uradni-list.si/bazeul/URED/2003/014/B/525663109.htm). Tretji odstavek 45.a člena uveljavlja splošno načelo »opt-out« za vsa komunikacijska sredstva, ki omogočajo osebna sporočila, se pravi, da zakon preventivno sega tudi na področje mobilne telefonije in SMS sporočil.

Pri snovanju zakona so bili dejavni predvsem predstavniki gospodarstva: Ministrstvo za gospodarstvo, Urad za varstvo potrošnikov, Gospodarska zbornica Slovenije, posamezne potrošniške organizacije in Tržni inšpektorat RS (TIRS), ki skrbi tudi za nadzor in uresničevanje zakona. Minimalna je bila udeležba stroke - poznavalci delovanja e-sporočil in sistemov, ki podpirajo e-komunikacijo. To je verjetno tudi razlog, da iz njihovih krogov izhaja največ pomislekov glede nedodelane zakonodaje, dolgotrajnih postopkov iskanja primernega dokaznega gradiva in problema izvajanja sankcij. Suhadolnik meni, da se učinek zakona ne bo kaj veliko poznal, saj večina nezaželene e-pošte izvira iz tujine in še dodaja, da je zelo enostavno e-sporočilo poslati v imenu nekoga drugega in prekriti pravega pošiljatelja (Suhadolnik v Skrt, 2003: 57).

Ključni snovatelji zakona so želeli zaščititi le potrošnika, zato je zakon precej ozko oblikovan in ne deluje na celotnem področju spama. V njem je veliko vrzeli, ki se bodo verjetno pokazale v praksi. Zakon ne definira nezaželenih e-sporočil, niti e-sporočil, ki jih zakon omejuje. Menijo, da za varstvo potrošnika opredelitev ni relevantna, saj želijo z zakonom preprečiti le prejemanje spama potrošnikov. Velja pa pravilo, da količina ni odločilnega pomena, saj že eno samo sporočilo lahko krši zakon. (priloga G). Nikjer niso navedena pravila soglašanja s prejemanjem e-pošte in koliko časa naj bi soglasje veljalo. Opisan ni niti način izvajanja »opt-out« funkcije ali mora pošiljatelj to omogočati brezplačno ali je za storitev dovoljeno zaračunati. Zapletlo se bo verjetno tudi pri dokazovanju kršitve zakona, predvsem pa je vprašanje ali imamo učinkovit organ, ki bo ugotavljal krivdo, zagotovil vsem udeleženim pravičnost in kaznoval krivce. Zaradi dolgotrajnih postopkov ugotavljanja kršitve zakona potekajo le zbiranja dokaznih gradiv za domnevne kšitelje, kazen pa še ni bila izrečena niti fizični niti pravni osebi. O učkonkovitosti zakona torej še ne moremo govoriti. Zagotov pa je, da kljub prizadevanjem proti spamu ostajamo še vedno poraženi pred spami iz tujine, ki še polnijo naše e-poštne predale.

7 OMEJITVE POSAMEZNIH REGULACIJ

Z uvajanjem novih tehnoloških, zakonskih in socialnih rešitev ter drugih destimulativnih ukrepov proti spamerjem lahko izboljšamo problem spama. Večina poznavalcev dvomi v učinkovitost posameznih pristopov in jih kritizira zaradi premajhne transparentnosti, ki bi omogočala boljše poznavanje in medsebojno povezovanje. Burr in podporniki njegovega predloga zakona zavzemajo stališče, da so pristopi proti spamu multiformni in ne vključujejo le zakonodaje, ampak tudi uveljavljanje zakonov, tehnološke rešitve, pristope ponudnikov interneta in izobraževanje uporabnikov e-pošte (Burr v Kajzer; http://www.techweb.com/wire/story/TWB20030710S0008).

Socialni pritisk oz. etična pravila na internetu, pravila posameznih spletnih strani in različni načini samoregulacije so popolnoma nemočni proti pojavom, ki v družbi delujejo deviantno. Samoregulacija se vrši le na nivoju posameznika in mu omogoča zaščito pred prejemanjem neželenih sporočil, vendar je takšen pristop reševanja popolnoma neučinkovit in ne pripomore k preprečevanju globalnega problema, niti ne ovira pošiljanja tovrstnih sporočil.

Nekoliko bolj uspešni so filtrirni sistemi, ki za svoje delovanje zahtevajo visoke vložke in večkratno nadgradnjo sistema. Zaradi fleksibilne narave jim spamerji neprestano sledijo in prilagajajo svojo tehnologijo, ki omogoča izogib tudi najnovejšim filtrom. Večina strokovnjakov je precej skeptičnih glede tehnoloških pristopov, saj meni, da bo tehnologija zaenkrat ostala še vedno poražena. Deloma zaradi časa, virov in dobička, s katerim razpolagajo spamerji, deloma zaradi odprte narave interneta in e-mail protokolov. Nezadovoljstvo s filtrirnimi sistemi narašča tudi med ameriškimi podjetji, ki menijo, da spam postaja čedalje hujši problem, filtrirni sistemi pa so neučinkoviti (Spam Getting Worse: Filters Aren't effective, http://emailuniverse.com/list-news/2002/07/29.html).

Na pravnem področju se tudi pojavljajo posamezne omejitve, ki slabijo moč zakonodaje. Geografske meje, ki ločujejo nacionalne zakonodaje, različne načine uvajanja zakonov in preprečevanja pošiljanja spamov so najpomembnejše omejitve. Samoumevno je, da se globalnega problema ne da rešiti na nacionalni ravni ali z razpršeno zakonodajo, ki na različne načine opredeljuje, omejuje ali prepoveduje spam in kaznuje kršitelje. Naslednji problem, ki slabi zakonodajo, je njena togost. Počasni procesi sprejemanja zakonov ne morejo slediti hitro se spreminjajoči tehnologiji, tako da so novi zakoni zaradi zastarelosti precej neučinkoviti.

Dodatno antispam zakone posameznih držav, predvsem v Ameriki, bremenijo še posamezne klavzule.

Večina uporabnikov si veliko obeta od novosprejetega skupnega antispam zakona v Ameriki, čeprav mu poznavalci ne pripisujejo večjega pomena. Muris, predsednik FTC-ja, ni navdušen nad »do-not-spam« registrom, saj naj bi po njegovem mnenju napravil več škode kot koristi in v končni fazi privedel do še večjih zlorab osebnih podatkov uporabnikov (FTC chairman takes road less traveled, http://www.ohio.com/mld/beaconjournal/6667210.htm). Skeptično je tudi mišljenje Mozene, ki je prepričan, da odprta narava interneta in e-pošiljanja sporočil onemogočata učinkovitost kakršne koli antispam politike. Trdi še, da veliko število spamov izvira iz Amerike in da je za uspešno preprečitev spama potreben skupen boj zakonodaje in tehnologije. “Edini način, da se znebimo spamov je, da se borimo, proti profitu spamerjev”.

SKLEP

Prvotna oblika marketinga je bila neposredna. Čisto na začetku so ljudje poznali le direkten stik s kupci oz. so z njimi menjali za dobrine, ki so jih sami potrebovali. S spreminjanjem življenjskega stila, mišljenja in družbenih ureditev, se je spreminjala tudi oblika marketinga. Vse bolj se je začel uveljavljati in uspevati posredni marketing. Že eno samo sporočilo je prepričalo množico potrošnikov, jim vzbudilo potrebo in razmišljanje o načinu njene zadovoljitve. Posredni marketing je postal množičen. Za širjenje svojih sporočil je uporabil tiskane medije, radio, letake, plakate in pozneje tudi televizijo. V zadnjem desetletju se spet pojavijo nove spremembe tako na področju tehnologije kot tudi družbe. Individualističen potrošnik in nove oblike medijev ponovno težijo k neposrednemu stiku med prodajalcem in kupcem.

Nova oblika neposrednega marketinga se zaradi novih medijev in hitrega razvoja tehnologije vse bolj nagiba k osebnemu pristopu. Orodja, ki omogočajo graditev podatkovnih baz in prepoznavanje potrošniških navad in želja, počasi zbujajo občutke nelagodja in zaskrbljenosti. Številni vdori v potrošnikovo zasebnost ogrožajo potrošnike in zmanjšujejo njihovo zaupanje v komunikacijo posameznih medijev.

Glede na opisane razmere in trende v marketingu lahko sklepam, da bo neposredni marketing v dobi e-poslovanja pridobival na pomenu. Podjetja bodo začela opuščati stare oblike množičnega marketinga in jih nadomeščati z novimi oblikami neposrednega oz. osebnega marketinga. Oglaševanje prek e-pošte med podjetji postaja vse bolj priljubljeno predvsem zaradi majhnih stroškov, preproste uporabe in možnosti hitrega obveščanja velikega števila potrošnikov ter oblikovanja sporočil, prilagojenih vsakemu posamezniku. Ravno te prednosti pa so žal privedle do vsiljivosti oglaševalcev, ki pošiljajo e-pošto tudi tistim, ki njihovih sporočil ne želijo prejemati. E-pošta in SMS-sporočila, ki jih pošiljajo bolj ali manj neznani pošiljatelji brez naše privolitve, resnično predstavljajo vsak dan večji problem. Nadloge e-pošte odvračajo podjetja, da bi se v večji meri odločala za e-mail marketing.

Zaradi strmega vzpona števila spamov, ki potuje po e-mail protokolih, je vsak dan več nezadovoljnih in nezaupljivih uporabnikov. Spam je nadloga svetovnega spleta tako v Ameriki in Evropi kot tudi v Sloveniji, zato menim, da bi morali na globalni ravni reševati tudi težave,

ki jih povzroča. Prepričana sem, da bi že enotna opredelitev spama kot takega bistveno pripomogla k zaustavitvi in zmanjšanju problemov.

Naslednji problem se pojavlja tudi v sami zasnovi interneta in e-mail protokolov, ki kljub hitremu razvoju tehnologije še vedno ostajajo skoraj nespremenjeni. Še vedno ostajajo odprte številne povezave, ki so imele na začetku vlogo pridobivanja novih uporabnikov, sedaj, ko je število teh močno naraslo, pa predvsem služijo le množičnemu pošiljanju spama in zabrisanju sledi pošiljatelja.

Antispam aktivnosti se sicer hitro širijo, zakonodaje posameznih držav sprejemajo nove zakone, uporabniki in ponudniki interneta kupujemo vedno nove antispam zaščite, obseg spama pa je kljub temu že presegel delež legalnih sporočil v naših e-poštnih predalih in še vedno raste. Kdo oz. kaj je tisto (tisti), ki lahko zaustavi internetno nadlogo – spam? Mislim, da rešitev ne obstaja v posameznem pristopu, ampak v podpori in dopolnjevanju vseh področij. Najbolj perspektivne se mi zdijo metode, ki bi spremenile zastarele protokole in s tem tudi način pošiljanja e-pošte. Za spamerje bi bilo povsem nesprejemljivo, da bi na primer ciljni strežnik od pošiljatelja zahteval potrdilo za vsako poslano pošto, za končne uporabnike in delovanje poštnih strežnikov pa bi bil takšen način povsem nemoteč. Na področju tehnologije bi morali seveda zapreti tudi vse odprte povezave, ki so eden glavnih krivcev za množičnost spama. Tudi na področju zakonodaje so potrebne spremembe. Kot prvo, sem mnenja, da je nujna enotnost pri opredelitvi spama in njegovi omejitvi oz. prepovedi. Razdrobljenost zakonov in geografska omejenost delovanja še dodatno slabita njihovo uspešnost. Prepričana sem, da bi omenjene spremembe in adekvatnost tehnologije, zakonodaje in drugih družbenih ukrepov ustavile zaskrbljujočo rast spama in ga deloma omejile. Močno pa dvomim, da obstaja način, ki bi povsem uničil spam. Verjetno se bomo morali v realnem življenju sprijazniti z delnimi rešitvami, tako kot na drugih področjih, in si pojav razložiti kot del sodobne, demokatične in civilizirane družbe in visoke tehnologije.

Glede na opisane razmere menim, da se razvoj nagiba v dve smeri, ki bosta v prihodnje zaznamovali tako neposredni kot tudi spletni marketing. Prva smer, imenovana marketing s privolitvijo, temelji na zaupanju, legalnem pridobivanju podatkov potrošnikov, osebni in nevsiljivi komunikaciji ter spoštovanju potrošnikov. Takšen odnos, ki ga vodijo potrošniki, je običajno dolgoročen in prinaša obojestransko zadovoljstvo in uspešno poslovanje ponudnika. Pravo nasprotje predstavlja druga smer, ki z agresijo gradi kratkoročne odnose in ogroža

potrošnike in njihovo zasebnost. Osnova so jim ogromne podatkovne baze, pridobljene na nelegalen način, ki jim omogočajo precej natančno opredelitev ciljne skupine in ceneno pošiljanje sporočil številnim potrošnikom.

Neposredni marketing bi se zaradi nizkih stroškov in številnih možnosti, ki jih nudi internet, še bolj intenzivno razvijal v smeri spletnega marketinga, če ne bi vse večji obseg spama, virusov in parazitskih programov povzročal toliko nezaupanja in strahu uporabnikov. Zaradi hitrih sprememb na tem področju in gibanja trenda v smeri elektronskega poslovanja, lahko kmalu pričakujemo nove spremembe.

Naj zaključim še z mislijo, da internet postaja vedno bolj kritičen način globalne komunikacije, hkrati pa predstavlja tudi izjemno priložnost za razvoj globalnega trga ter enotno svetovno gospodarstvo, ki mora enotno obravnavati tudi motnje, ki se pri tem pojavljajo.

LITERATURA

Knjige:

Bird, Drayton (1990): Commonsense direct marketing. Lincolnwood, NTC Business Books

Blois, Keith; Sargeant Adrian (2000): The Oxford textbook of marketing: Direct marketing. Oxford University Press str.: 591-617

Chaffey, Dave et al. (2000): Internet Marketing. Trowbridge, Pearson Education Limited

Leskovšek, Marjeta, Lobe, Bojana, Novak, Marjeta (2002): Raziskava razširjenosti spam sporočil med študenti EF in FDV, Ljubljana, Fakulteta za družbene vede

Korper, Stefano in Ellis, Juanita (2001): E-Commerce Book. San Diego, Academec Press

Kotler, Philip (1996): Marketing Management – Trženjsko upravljanje: analiza, načrtovanje, izvajanje in nazdor. Ljubljana, Slovenska knjiga

Kovačič, Matej (2003): Zasebnost na internetu. Ljubljana, Mirovni inštitut

Meše, Pavel (2003): Varnost v elektronskih komunikacijah in informacijski tehnologiji: pojmovnik, angleško-slovenski slovar, kratice, Ljubljana, Elektrotehniška zveza Slovenije

Reitman, Jerry I. (1995):Beyond 2000 The Future of Direct Marketing. Lincolnwood, NTC Business Book

Roberts, Stevan et al. (2001): Internet Direct Mail. Lincolnwood, NTC Business Books

Schwartz, Alan and Garfinkel, Simson (1998): Stopping spam. Sebastopol, O'Reilly & Associates, Inc.

Stone, Bob (1994): Successful Direct Marketing Methods.Lincolnwood, NTC Business Books

Članki:

Bogataj, Maja (2003): "Avtorsko pravo v obdobju digitalnih tehnologij". GV-konferenca: Poslovna raba interneta, Portorož, januar 2003.

Božič, Gorazd (2003): "Kaj se dogaja na omrežju?". Zbornik referatov štirinajste delavnice

R. B. (2003): "Oglaševanje z SMS sporočili". Delo, XLV, 232, str.13.

VITEL, maj 2003, str. 33-35.

Ocvirk, Vasja (2003): "Veliko več kot tehnološko vprašanje". Moj mikro, 19, 9, str. 54-55.

Oseli, Petra (2003): "Učinkovitost internetnega oglaševanja". GV-konferneca: Poslovna raba interneta, Portorož, januar 2003.

Skrt, Radoš (2003): "In vendar se premika". Moj mikro, 19, 9, str. 56-58.

Skrt, Radoš (2003): "Zakonito do e-naslovov". Moj mikro, 19, 9, str. 58-59.

Skrt, Radoš (2003): "Velik učinek za malo denarja". Moj mikro, 19, 9, str. 60-59.

Zmagaj, Peter (2003): “Kako se zaščitimo pred SMS spamom”. Finance, 154/1582, str. 7.

Internet naslovi:

Direct marketing association guidelines
http://www.the-dma.org/guidelines/ethicalguidelines.pdf
DMA census of the direct marketing industry
http://www.dma.org.uk/_public/dma_census2001-2002_short.pdf
Email Address Harvesting: How Spammers Reap What You Sow
ttp://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm)
False Claims in Spam
http://www.ftc.gov/reports/spam/030429spamreport.pdf
Filters vs. Blacklist
www.paulgraham.com/falsepositives.html
FTC Unveils "Dirty Dozen Spam Scams"
http://www.ftc.gov
House argues over competing spam bills
http://www.techweb.com/wire/story/TWB20030710S0008
Industry, politicians, user groups call for national spam-killing measures
http://www.internetweek.com/story/showArticle.jhtml?articleID=10100104
Information about hoaxes and Chain letters
http://hoaxbusters.ciac.org
Make spammers pay before you do
http://www.clickz.com/feedback/buzz/article.php/1432751
Official journal of the European Communities; Directive 95/46/EC of the European Parlament and of the Council of 24 October 1995
http://www.spamlaws.com/docs/95-46-ec.pdf
Official journal of the European Communities; Directive 97/7/EC of the European Parlament and of the Council of 20 May 1997
http://www.spamlaws.com/docs/97-7-ec.pdf
Official journal of the European Communities; Directive 97/66/EC of the European Parlament and of the Council of 15 December 1997
http://www.spamlaws.com/docs/97-66-ec.pdf
Official journal of the European Communities; Directive 2002/58/EC of the European Parlament and of the Council of 12 July 2002

http://www.spamlaws.com/docs/2002-58-ec.pdf
Official journal of the European Communities; Directive 2000/31/EC of the European Parlament and of the Council of 8 June 2000
http://www.spamlaws.com/docs/2000-31-ec.pdf
Parazitni programi; Adware, Spyware in prikrita omrežja
http://www.arnes.si
Pismo predsedništvu spodnjega doma ameriškega kongresa
http://www.eff.org/Spam_cybersquatting_abuse/Spam/HTML/19980729_eff_hr3888_letter.html
Privacy & Human Rights 1999
www.privacyinternational.org/survey/index99.html
Searching for a Definition for Spam
http://www.clickz.com/em_mkt/em_mkt/article.php/1492521
Size and cost of the problem
http://www.ietf.org/proceedings/03mar/slides/asrg-1/index.html
Spam Abuse
http://spam.abuse.net
Spam Getting Worse: Filters Aren't effective
http://emailuniverse.com/list-news/2002/07/29.html
Spam is different
http://www.paulgraham.com
Technical and Legal Approaches to Unsolicited Electronic Mail
http://www.spamlaws.com
Terminološki slovar informatike
http://www.ef.uni-lj.si/terminoloskislovar/index.asp
The impact of data restrictions on consumer distance shopping (2001)
http://www.the-dma.org/isec/9.pdf
The problem
http://www.cauce.org
The spam police
http://www.nwfusion.com/research/2001/0910feat.html
The Spam Problem and Brightmail's solution
http://www.brihtmail.com
Unsolicited Commercial Communications and Data Protection

http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamstudy_en.pdf
Why was I referred to this website?
http://www.mail-abuse.org
Ustava Republike Slovenije
www.us-rs.si/si/basisfr.html
The Bloor Perspective: SMS spam, go phish and Windows Media Center
http://www.silicon.com/software/security/0,39024655,10006191,00.htm
SIBIS Slovenia, Country report No. 10
http://www.sisplet.org/ris/uploads/publikacije/2003/slovenia_cremonti.pdf
Brightmail Hails Passing of U.S. Senate Bill 877
http://www.brightmail.com/pressreleases/102203_senate_bill_877.html
Privacy and Human Rights 2003: Threats to Privacy
http://www.zentek-international.com/mirrors/privacyinternational/survey/phr2003/threats.htm

PRILOGE

PRILOGA A: DIRECT MARKETING ASSOCIATION GUIDELINES

For Ethical Business Practice

The Direct Marketing Association's Guidelines for Ethical Business Practice are intended to provide individuals and organizations involved in direct marketing in all media with generally accepted principles of conduct. These guidelines reflect The DMA's long-standing policy of high levels of ethics and the responsibility of the Association, its members, and all marketers to maintain consumer and community relationships that are based on fair and ethical principles. In addition to providing general guidance to the industry, the Guidelines for Ethical Business Practice are used by The DMA's Committee on Ethical Business Practice and the Teleservices Ethics Committee, industry peer review committees, as the standard to which direct marketing promotions that are the subject of complaint to The DMA are compared.

These self-regulatory guidelines are intended to be honored in light of their aims and principles. All marketers should support the guidelines in spirit and not treat their provisions as obstacles to be circumvented by legal ingenuity.
These guidelines also represent The DMA's general philosophy that self-regulatory measures are preferable to governmental mandates. Self-regulatory actions are more readily adaptable to changing techniques and economic and social conditions. They encourage widespread use of sound business practices.
Because dishonest, misleading or offensive communications discredit all means of advertising and marketing, including direct marketing, observance of these guidelines by all concerned is expected. All persons involved in direct marketing should take reasonable steps to encourage other industry members to follow these guidelines as well.

HONESTY AND CLARITY OF OFFER
Article #1

All offers should be clear, honest and complete so that the consumer may know the exact nature of what is being offered, the price, the terms of payment (including all extra charges) and the commitment involved in the placing of an order. Before publication of an offer, marketers should be prepared to substantiate any claims or offers made. Advertisements or specific claims that are untrue, misleading, deceptive or fraudulent should not be used.

ACCURACY AND CONSISTENCY
Article #2

Simple and consistent statements or representations of all the essential points of the offer should appear in the promotional material. The overall impression of an offer should not be contradicted by individual statements, representations or disclaimers.

CLARITY OF REPRESENTATIONS
Article #3

Representations which, by their size, placement, duration or other characteristics are unlikely to be noticed or are difficult to understand should not be used if they are material to the offer.

ACTUAL CONDITIONS
Article #4

All descriptions, promises and claims of limitation should be in accordance with actual conditions, situations and circumstances existing at the time of the promotion.

DISPARAGEMENT
Article #5
Disparagement of any person or group on grounds addressed by federal or state laws that prohibit discrimination is unacceptable.

DECENCY
Article #6

Solicitations should not be sent to consumers who have indicated to the marketer that they consider those solicitations to be vulgar, immoral, profane, pornographic or offensive in any way and who do not want to receive them.

PHOTOGRAPHS AND ART WORK
Article #7

Photographs, illustrations, artwork and the situations they describe should be accurate portrayals and current reproductions of the products, services or other subjects they represent.

DISCLOSURE OF SPONSOR AND INTENT
Article #8

All marketing contacts should disclose the name of the sponsor and each purpose of the contact. No one should make offers or solicitations in the guise of one purpose when the intent is a different purpose.

ACCESSIBILITY
Article #9

Every offer and shipment should clearly identify the marketer's name and postal address or telephone number, or both, at which the consumer may obtain service. If an offer is made online, an e-mail address should also be identified.

SOLICITATION IN THE GUISE OF AN INVOICE OR GOVERNMENTAL

NOTIFICATION
Article #10

Offers that are likely to be mistaken for bills, invoices, or notices from public utilities or governmental agencies should not be used.

POSTAGE, SHIPPING OR HANDLING CHARGES
Article #11

Postage, shipping or handling charges, if any, should bear a reasonable relationship to actual costs incurred.

Advance Consent Marketing

Article #12

These guidelines address marketing plans where the consumer gives consent to receive and pay for goods or services in the future on a continuing or periodic basis unless and until the consumer cancels the plan.

The following principles apply to all advance consent marketing plans:

* Marketers should have the consumer’s informed consent to participate in any advance consent marketing plan before the consumer is billed or charged. In telephone sales where the consumer pays in a way other than by credit or debit card, this consent must be written or audio recorded.

* Marketers may provide products or services and bills concurrently; however, consumers should not be obligated to pay bills prior to the expiration of any trial period.

* Marketers should inform consumers in the initial offer and in renewal reminders of their right to cancel their participation in the plan.

* Marketers should provide renewal reminders at the frequency specified in the initial offer. Marketers should allow consumers a reasonable length of time between receipt of renewal reminders and the renewal date, before which consumers can cancel the plan.

* Marketers should promptly honor requests for refunds due upon consumers' cancellation of the plan.

Marketers should clearly and conspicuously disclose material terms and conditions before obtaining the consumer's consent, including:

* a description of the goods or services being offered
* the identity of the marketer and contact information for service or cancellation
* the interval between shipments or services to be provided
* the price or the range of prices of the goods or services purchased by the consumer, including whether there are any additional charges
* whether the consumer will be billed or automatically charged
* when and how frequently the consumer will be billed or charged
* the fact that the consumer must take affirmative action to cancel in order to avoid future billing or charges
* the specific and easy steps that consumers should follow to cancel the plan and avoid the charges, and
* the time period if any within which the consumer must cancel

When applicable, the following terms and conditions should also be clearly and conspicuously disclosed in the initial offer:

* that the current plan or renewal prices of the goods or services are subject to change
* the length of any free, trial, or approval period in time or quantity
* the length of any membership period, and the length of subsequent renewal or billing periods
* the fact that goods or services will continue after the free period unless the consumer cancels
* any minimum purchase obligations, and
* terms and conditions of any refund policy

In telephone sales where the marketer uses pre-acquired account information under a free-to-pay conversion plan, the marketer should:

* obtain from the consumer the last 4 digits of the account to be charged
* obtain consent from the consumer to charge such account, and
* audio record the entire transaction

In telephone sales where the marketer uses pre-acquired account information but does not engage in a free-to-pay conversion plan, the marketer should:

* identify with specificity the account that will be charged, and
* obtain consent from the consumer to charge such account

All marketing partners or service providers should comply with these guidelines.

Marketing to Children

MARKETING TO CHILDREN

Article #13

Offers and the manner in which they are presented that are suitable for adults only should not be made to children. In determining the suitability of a communication with children online or in any other medium, marketers should address the age range, knowledge, sophistication and maturity of their intended audience.

PARENTAL RESPONSIBILITY AND CHOICE

Article #14

Marketers should provide notice and an opportunity to opt out of the marketing process so that parents have the ability to limit the collection, use and disclosure of their children's names, addresses or other personally identifiable information.

INFORMATION FROM OR ABOUT CHILDREN

Article #15

Marketers should take into account the age range, knowledge, sophistication and maturity of children when collecting information from them. Marketers should limit the collection, use and dissemination of information collected from or about children to information required for the promotion, sale and delivery of goods and services, provision of customer services, conducting market research and engaging in other appropriate marketing activities.
Marketers should effectively explain that the information is being requested for marketing purposes. Information not appropriate for marketing purposes should not be collected.
Upon request from a parent, marketers should promptly provide the source and general nature of information maintained about a child. Marketers should implement strict security measures to ensure against unauthorized access, alteration or dissemination of the data collected from or about children.

MARKETING ONLINE TO

CHILDREN UNDER 13 YEARS OF AGE

Article #16

Marketers should not collect personally identifiable information online from a child under 13 without prior parental consent or direct parental notification of the nature and intended use of such information online and an opportunity for the parent to prevent such use and participation in the activity. Online contact information should only be used to directly respond to an activity initiated by a child and not to recontact a child for other purposes without prior parental consent. However, a marketer may contact and get information from a child for the purpose of obtaining parental consent.
Marketers should not collect, without prior parental consent, personally identifiable information online from children that would permit any off-line contact with the child.
Marketers should not distribute to third parties, without prior parental consent, information collected from a child that would permit any contact with that child.
Marketers should take reasonable steps to prevent the online publication or posting of information that would allow a third party to contact a child off-line unless the marketer has prior parental consent.

Marketers should not entice a child to divulge personally identifiable information by the prospect of a special game, prize or other offer.
Marketers should not make a child's access to a Web site contingent on the collection of personally identifiable information. Only online contact information used to enhance the interactivity of the site is permitted.
The following assumptions underlie these online guidelines:

* When a marketer directs a site at a certain age group, it can expect that the visitors to that site are in that age range; and

* When a marketer asks the age of the child, the marketer can assume the answer to be truthful.

Special Offers and Claims

USE OF THE WORD "FREE" AND OTHER SIMILAR REPRESENTATIONS
Article #17

A product or service that is offered without cost or obligation to the recipient may be unqualifiedly described as "free."
If a product or service is offered as "free," all qualifications and conditions should be clearly and conspicuously disclosed, in close conjunction with the use of the term "free" or other similar phrase. When the term "free" or other similar representations are made (for example, 2-for-1, half-price or 1-cent offers), the product or service required to be purchased should not have been increased in price or decreased in quality or quantity.

PRICE COMPARISONS
Article #18

Price comparisons including those between a marketer's current price and a former, future or suggested price, or between a marketer's price and the price of a competitor's comparable product should be fair and accurate.
In each case of comparison to a former, manufacturer's suggested or competitor's comparable product price, recent substantial sales should have been made at that price in the same trade area.
For comparisons with a future price, there should be a reasonable expectation that the new price will be charged in the foreseeable future.

GUARANTEES
Article #19

If a product or service is offered with a guarantee or a warranty, either the terms and conditions should be set forth in full in the promotion, or the promotion should state how the consumer may obtain a copy. The guarantee should clearly state the name and address of the guarantor and the duration of the guarantee.
Any requests for repair, replacement or refund under the terms of a guarantee or warranty should be honored promptly. In an unqualified offer of refund, repair or replacement, the customer's preference should prevail.

USE OF TEST OR SURVEY DATA
Article #20

All test or survey data referred to in advertising should be valid and reliable as to source and methodology, and should support the specific claim for which it is cited. Advertising claims should not distort test or survey results or take them out of context.

TESTIMONIALS AND ENDORSEMENTS
Article #21

Testimonials and endorsements should be used only if they are:

1. Authorized by the person quoted;
2. Genuine and related to the experience of the person giving them both at the time made and at the time of the promotion; and
3. Not taken out of context so as to distort the endorser's opinion or experience with the product.

Sweepstakes

USE OF THE TERM "SWEEPSTAKES"
Article #22

Sweepstakes are promotional devices by which items of value (prizes) are awarded to participants by chance without the promoter's requiring the participants to render something of value (consideration) to be eligible to participate. The co-

existence of all three elements - prize, chance and consideration - in the same promotion constitutes a lottery. It is illegal for any private enterprise to run a lottery without specific governmental authorization.
When skill replaces chance, the promotion becomes a skill contest. When gifts (premiums or other items of value) are given to all participants independent of the element of chance, the promotion is not a sweepstakes. Promotions that are not sweepstakes should not be held out as such.
Only those promotional devices that satisfy the definition stated above should be called or held out to be a sweepstakes.

NO PURCHASE OPTION
Article #23

Promotions should clearly state that no purchase is required to win sweepstakes prizes. They should not represent that those who make a purchase or otherwise render consideration with their entry will have a better chance of winning or will be eligible to win more or larger prizes than those who do not make a purchase or otherwise render consideration. The method for entering without ordering should be easy to find, read and understand. When response devices used only for entering the sweepstakes are provided, they should be as easy to find as those utilized for ordering the product or service.

CHANCES OF WINNING
Article #24

No sweepstakes promotion, or any of its parts, should represent that a recipient or entrant has won a prize or that any entry stands a greater chance of winning a prize than any other entry when this is not the case. Winners should be selected in a manner that ensures fair application of the laws of chance.

PRIZES
Article #25

Sweepstakes prizes should be advertised in a manner that is clear, honest and complete so that the consumer may know the exact nature of what is being offered. For prizes paid over time, the annual payment schedule and number of years should be clearly disclosed.
Photographs, illustrations, artwork and the situations they represent should be accurate portrayals of the prizes listed in the promotion.
No award or prize should be held forth directly or by implication as having substantial monetary value if it is of nominal worth. The value of a non-cash prize should be stated at regular retail value, whether actual cost to the sponsor is greater or less.
All prizes should be awarded and delivered without cost to the participant. If there are certain conditions under which a prize or prizes will not be awarded, that fact should be disclosed in a manner that is easy to find, read and understand.

PREMIUMS
Article #26

Premiums should be advertised in a manner that is clear, honest and complete so that the consumer may know the exact nature of what is being offered.
A premium, gift or item should not be called or held out to be a "prize" if it is offered to every recipient of or participant in a promotion. If all participants will receive a premium, gift or item, that fact should be clearly disclosed.

DISCLOSURE OF RULES
Article #27

All terms and conditions of the sweepstakes, including entry procedures and rules, should be easy to find, read and understand. Disclosures set out in the rules section concerning no purchase option, prizes and chances of winning should not contradict the overall impression created by the promotion.
The following should be set forth clearly in the rules:

* No purchase of the advertised product or service is required in order to win a prize.
* A purchase will not improve the chances of winning.
* Procedures for entry.
* If applicable, disclosure that a facsimile of the entry blank or other alternate means (such as a 3"x 5" card) may be used to enter the sweepstakes.
* The termination date for eligibility in the sweepstakes. The termination date should specify whether it is a date of mailing or receipt of entry deadline.
* The number, retail value (of non-cash prizes) and complete description of all prizes offered, and whether cash may be awarded instead of merchandise. If a cash prize is to be awarded by installment payments, that fact should be clearly disclosed, along with the nature and timing of the payments.
* The estimated odds of winning each prize. If the odds depend upon the number of entries, the stated odds should be based on an estimate of the number of entries.
* The method by which winners will be selected.
* The geographic area covered by the sweepstakes and those areas in which the offer is void.

* All eligibility requirements, if any.
* Approximate dates when winners will be selected and notified.
* Publicity rights regarding the use of winner's name.
* Taxes are the responsibility of the winner.
* Provision of a mailing address to allow consumers to receive a list of winners of prizes over $25.00 in value.

Fulfillment

UNORDERED MERCHANDISE OR SERVICE
Article #28

Merchandise or services should not be provided without having first received the customer's permission. The exceptions are samples or gifts clearly marked as such, and merchandise mailed by a charitable organization soliciting contributions, as long as all items are sent with a clear and conspicuous statement informing the recipient of an unqualified right to treat the product as a gift and to do with it as the recipient sees fit, at no cost or obligation to the recipient.

PRODUCT AVAILABILITY AND SHIPMENT
Article #29

Direct marketers should offer merchandise only when it is on hand or when there is a reasonable expectation of its timely receipt.
Direct marketers should ship all orders according to the terms of the offer or within 30 days where there is no promised shipping date, unless otherwise directed by the consumer, and should promptly notify consumers of any delays.

DRY TESTING
Article #30

Direct marketers should engage in dry testing only when the special nature of the offer is made clear in the promotion.
Collection, Use and Maintenance of Marketing Data

COLLECTION, USE AND TRANSFER OF PERSONALLY IDENTIFIABLE DATA
Article #31

Consumers who provide data that may be rented, sold or exchanged for marketing purposes should be informed periodically by marketers of their policy concerning the rental, sale or exchange of such data and of the opportunity to opt out of the marketing process. Should that policy substantially change, marketers have an obligation to inform consumers of that change prior to the rental, sale or exchange of such data, and to offer consumers an opportunity to opt out of the marketing process at that time. All individual opt-out requests should be honored. Marketers should maintain and use their own systems, policies and procedures including in-house suppression and opt-out lists, and at no cost to consumers refrain from using or transferring such data, as the case may be, as requested by consumers.
List compilers should maintain and use their own systems, policies and procedures, and at no cost to consumers refrain from using or transferring data, as the case may be, as requested by consumers.
For each list that is rented, sold or exchanged, the applicable DMA Preference Service name removal list (e.g., Mail Preference Service, Telephone Preference Service and E-mail Preference Service) should be employed prior to use.
Data about consumers who have opted out of use, including a request not to be contacted, or transfer should not, per their requests, be used, rented, sold or exchanged.
In addition to adhering to these guidelines, marketers should cooperate with The DMA when requested in demonstrating compliance with the "Privacy Promise".

Upon request by a consumer, marketers should disclose the source from which they obtained personally identifiable data about that consumer.

PERSONAL DATA
Article #32

Marketers should be sensitive to the issue of consumer privacy and should only collect, combine, rent, sell, exchange or use marketing data. Marketing data should be used only for marketing purposes.
Data and selection criteria that by reasonable standards may be considered sensitive and/or intimate should not be disclosed, displayed or provide the basis for lists made available for rental, sale or exchange when there is a reasonable expectation by the consumer that the information will be kept confidential.
Credit card numbers, checking account numbers and debit account numbers are considered to be personal information and therefore should not be transferred, rented, sold or exchanged when there is a reasonable expectation by the consumer that the information will be kept confidential. Because of the confidential nature of such personally identifying numbers, they should not be publicly displayed on direct marketing promotions or otherwise made public by direct marketers.
Social Security numbers are also considered to be personal information and therefore should not be transferred, rented, sold or exchanged for use by a third party when there is a reasonable expectation by the consumer that the information will be

kept confidential. Because of the confidential nature of Social Security numbers, they should not be publicly displayed on direct marketing promotions or otherwise made public by direct marketers. Social Security numbers, however, are used by direct marketers as part of the process of extending credit to consumers or for matching or verification purposes.

COLLECTION, USE AND TRANSFER OF HEALTH-RELATED DATA

Article #33

Health-related data constitute information related to consumers':

* Illnesses or conditions;
* Treatments for those illnesses or conditions, such as prescription drugs, medical procedures, devices or supplies; or
* Treatments received from doctors (or other health care providers), at hospitals, at clinics or at other medical treatment facilities.

These fair information practices and principles apply to any individual or entity that collects, maintains, uses and/or transfers health-related data for marketing purposes, whether or not marketing is a primary purpose. These principles are applicable to nonprofit as well as for-profit entities.

1. Personally identifiable health-related data gained in the context of a relationship between consumers and health or medical care providers or medical treatment facilities should not be transferred for marketing purposes without the specific prior consent of those consumers. Health or medical care providers include licensed health care practitioners, such as doctors, nurses, psychologists, pharmacists and counselors, and those who support health care providers and therefore have access to personally identifiable information, such as insurance companies, pharmacy benefits managers or other business partners, and businesses that sell prescription drugs.
2. Personally identifiable health-related data, including the occurrence of childbirth, gained in the context of a relationship between consumers and health or medical care providers or medical treatment facilities (as defined in #1) should not be used to contact those consumers for marketing purposes without giving consumers a clear notice of the marketer's intended uses of the data and the opportunity to request not to be so contacted.
3. Personally identifiable health-related data volunteered by consumers, and gathered outside of the relationship between consumers and health care providers, should also be considered sensitive and personal in nature. Such data should not be collected, maintained, used and/or transferred for marketing purposes unless those consumers receive, at the time the data are collected, a clear notice of the marketer's intended uses of the data, whether the marketer will transfer the data to third parties for further use, the name of the collecting organization, and the opportunity to opt out of transfer of the data. Such data include, but are not limited to, data volunteered by consumers when responding to surveys and questionnaires. Clear notice should be easy to find, read and understand.
4. Personally identifiable health-related data inferred about consumers, and gathered outside of the relationship between consumers and health care providers, should also be considered sensitive and personal in nature. These are data based on consumers' purchasing behavior. Such data include, but are not limited to, data captured by inquiries, donations, purchases, frequent shopper programs, advertised toll-free telephone numbers, or other consumer response devices. Any entity, including a seller of over-the-counter drugs, which uses inferred health-related data should, per The DMA's Privacy Promise, promptly provide notice and the opportunity to opt out of any transfer of the data for marketing purposes.
5. Marketers using personally identifiable health-related data should provide both the source and the nature of the information they have about that consumer, upon request of that consumer and receipt of that consumer's proper identification.
6. Consumers should not be required to release personally identifiable health-related information about themselves to be used for marketing purposes as a condition of receiving insurance coverage, treatment or information, or otherwise completing their health care-related transaction.
7. The text, appearance and nature of solicitations directed to consumers on the basis of health-related data should take into account the sensitive nature of such data.
8. Marketers should ensure that safeguards are built into their systems to protect personally identifiable health-related data from unauthorized access, alteration, abuse, theft or misappropriation. Employees who have access to personally identifiable health-related data should agree in advance to use those data only in an authorized manner.

If personally identifiable health-related data are transferred from one direct marketer to another for a marketing purpose, the transferor should arrange strict security measures to assure that unauthorized access to the data is not likely during the transfer process. Transfers of personally identifiable health-related data should not be permitted for any marketing uses that are in violation of any of The DMA's Guidelines for Ethical Business Practice.

Nothing in these guidelines is meant to prohibit research, marketing or other uses of health-related data which are not personally identifiable, and which are used in the aggregate.

PROMOTION OF MARKETING LISTS

Article #34

Any advertising or promotion for marketing lists being offered for rental, sale or exchange should reflect the fact that a marketing list is an aggregate collection of marketing data. Such promotions should also reflect a sensitivity for the consumers on those lists.

MARKETING LIST USAGE

Article #35

List owners, brokers, managers, compilers and users of marketing lists should ascertain the nature of the list's intended usage for each materially different marketing use prior to rental, sale, exchange, transfer or use of the list. List owners, brokers, managers and compilers should not permit the rental, sale, exchange or transfer of their marketing lists, nor should users use any marketing lists for an offer that is in violation of these guidelines.

INFORMATION SECURITY

Article #36

The protection of personally identifiable information is the responsibility of all marketers. Therefore, marketing companies should assume the following responsibilities to provide secure transactions for consumers and to protect databases containing consumers' personally identifiable information against unauthorized access, alteration, or dissemination of data:

* Marketers should establish information security policies and practices that assure the uninterrupted security of information systems.
* Marketers should create and implement staff policies, procedures, training and responsiveness measures to protect personally identifiable information handled in the everyday performance of duties.
* Marketers should employ and routinely reassess protective physical safeguards and technological measures in support of information security policies.
* Marketers should inform all business partners and service providers that handle personally identifiable information of their responsibility to ensure that their policies, procedures and practices maintain a level of security consistent with the marketer's applicable information security policies.

Online Marketing

ONLINE INFORMATION

Article #37

Notice to Online Visitors

If your organization operates an online site, you should make your information practices available to visitors in a prominent place on your Web site's home page or in a place that is easily accessible from the home page. The notice about information practices on your Web site should be easy to find, read, and understand so that a visitor is able to comprehend the scope of the notice. The notice should be available prior to or at the time personally identifiable information is collected.
Your organization and its postal address, and the Web site(s) to which the notice applies should be identified so the visitor knows who is responsible for the Web site. You also should provide specific contact information so the visitor can contact your organization for service or information.

If your organization collects personally identifiable information from visitors, your notice should include:

* The nature of personally identifiable information collected about individual visitors online, and the types of uses you make of such information, including marketing uses that you may make of that information.
* Whether you transfer personally identifiable information to third parties for use by them for their own marketing and the mechanism by which the visitor can exercise choice not to have such information transferred.
* Whether personally identifiable information is collected by, used by or transferred to agents (entities working on your behalf) as part of the business activities related to the visitor's actions on the site, including to fulfill orders or to provide information or requested services.
* Whether you use cookies or other passive means of data collection, and whether such data collected are for internal purposes or transferred to third parties for marketing purposes.
* What procedures your organization has put in place for accountability and enforcement purposes.
* That your organization keeps personally identifiable information secure.

If you knowingly permit network advertisers to collect information on their own behalf or on behalf of their clients on your Web site, you should also provide notice of the network advertisers that collect information from your site and a mechanism by which a visitor can find those network advertisers to obtain their privacy statements and to exercise the choice of not having such information collected. (Network advertisers are third parties that attempt to target online advertising and make it more relevant to visitors based on Web traffic information collected over time across Web sites of others.)
If your organization's policy changes materially with respect to the sharing of personally identifiable information with third parties for marketing purposes, you will update your policy and give consumers conspicuous notice to that effect, offering an opportunity to opt out.

Honoring Choice

You should honor a visitor's choice regarding use and transfer of personally identifiable information made in accordance with your stated policy. If you have promised to honor the visitor's choice for a specific time period, and if that time period subsequently expires, then you should provide that visitor with a new notice and choice. You should provide choices of opting out online. You may also offer opt-out options by mail or telephone.

Providing Access

You should honor any representations made in your online policy notice regarding access.

Data Security

Your organization should use security technologies and methods to guard against unauthorized access, alteration, or dissemination of personally identifiable information during transfer and storage. Your procedures should require that employees and agents of your organization who have access to personally identifiable information use and disclose that information only in a lawful and authorized manner.

Visitors Under 13 Years of Age

If your organization has a site directed to children under the age of 13 or collects personally identifiable information from visitors known to be under 13 years of age, your Web site should take the additional steps required by Article #16 of the Guidelines for Ethical Business Practice and inform visitors that your disclosures and practices are subject to compliance with the Children's Online Privacy Protection Act.

Accountability

There should be a meaningful, timely, and effective procedure through which your organization can demonstrate adherence to your stated online information practices. Such a procedure may include: 1) self or third party verification and monitoring, 2) complaint resolution and 3) education and outreach. This can be accomplished by an independent auditor, public self-certification, a third party privacy seal program, a licensing program, membership in a trade, professional or other membership association or self-regulatory program, or being subject to government regulation.

COMMERCIAL SOLICITATIONS ONLINE

Article #38

Marketers may send commercial solicitations online under the following circumstances:

* The solicitations are sent to the marketers' own customers, or
* Individuals have given their affirmative consent to the marketer to receive solicitations online, or
* Individuals did not opt out after the marketer has given notice of the opportunity to opt out from solicitations online, or
* The marketer has received assurance from the third party list provider that the individuals whose e-mail addresses appear on that list
    - o have already provided affirmative consent to receive solicitations online, or
    - o have already received notice of the opportunity to have their e-mail addresses removed and have not opted out.

In each solicitation sent online, marketers should furnish individuals with a link or notice they can use to:

- o request that the marketer not send them future solicitations online, and
- o request that the marketer not rent, sell, or exchange their e-mail addresses for online solicitation purposes.

The above requests should be honored in a timely manner.

Only those marketers that rent, sell, or exchange information need to provide notice of a mechanism to opt out of information transfer to third-party marketers.

Marketers should process commercial e-mail lists obtained from third parties using The DMA's E-mail Preference Service suppression file. E-MPS need not be used on one's own customer lists, or when individuals have given affirmative consent to the marketer directly.

Solicitations sent online should disclose the marketer's identity, and the subject line should be clear, honest, and not misleading. A marketer should also provide specific contact information at which the individual can obtain service or information. The marketer's street address should be made available in the e-mail solicitation or by a link to the marketer's Web site.

ONLINE REFERRAL MARKETING

Article #39

Online referral marketing is a technique marketers use to get new marketing leads. Typically, the online marketer:

1. encourages an individual to forward a marketing piece on to another individual (personally identifiable information is not collected), or
2. asks an individual to provide the marketer with personally identifiable information about another individual so the marketer may contact that person directly.

This guideline relates only to the second type of online referral marketing above, where personal information about a prospect is given to the marketer.

A marketer should not use personally identifiable information about a prospect provided online by another individual unless:

* the marketer has first clearly disclosed to the referring individual the intended uses of the information;

* the marketer has disclosed to the referring individual that their own contact information will be provided to those they have referred to the marketer;

* the marketer discloses to the referred person the fact that their contact information was obtained from another individual. The marketer should make the referring person's information available in the first e-mail communication to the prospect. Or, the marketer can tell the prospect how to get the referring person's contact information at no cost; and

* the marketer provides, in the first and any subsequent e-mail communications, the ability to remove the referred person's name from future contact.

Marketers should not sell, rent, share, transfer or exchange a referred e-mail address unless they receive prior permission from the referred person to do so.

Telephone Marketing

REASONABLE HOURS

Article #40

Telephone contacts should be made during reasonable hours as specified by federal and state laws and regulations.

TAPING OF CONVERSATIONS

Article #41

Taping of telephone conversations by telephone marketers should only be conducted with notice to or consent of all parties, or the use of a beeping device, as required by applicable federal and state laws and regulations.

RESTRICTED CONTACTS

Article #42

A marketer should not knowingly call or send a voice solicitation message to a consumer who has an unlisted or unpublished telephone number except in instances where the number was provided by the consumer to that marketer for that purpose. A marketer should not call consumers who are on the marketer's in-house Do-Not-Call list. A marketer should not knowingly place a call or send a voice or text message to a wireless telephone number for which the called party must pay the charge, in either business-to-consumer or business-to business marketing, except in instances where the number was provided by the consumer or business to that marketer for that purpose. A marketer should also use the DMA's Wireless Suppression Service or another comprehensive wireless suppression service prior to calling or sending text solicitation messages.

A marketer should use the DMA's Telephone Preference Service as required in Article #31 and must use the federal Do-Not-Call registry and state Do-Not-Call lists when applicable prior to using any outbound calling list. Individuals with whom the marketer has an established business relationship do not need to be suppressed even if they are on the national registry. An established business relationship is defined as those persons with whom the marketer has had a transaction/received a payment within the last 18 months or those persons who have inquired about the marketer's products/services within the last 3 months. (Note: State laws may vary. The DMA's Web site at: www.the-dma.org/government/donotcalllists.shtml attempts to provide current information on state Do-Not-Call lists.) Consumers who have given written permission to the marketer do not need to be suppressed by any Do-Not-Call list. Individuals can add or remove themselves from company-specific Do-Not-Call lists either orally or in writing.

Marketers should not use randomly or sequentially generated numbers in sales or marketing solicitations.

CALLER-ID / AUTOMATIC NUMBER IDENTIFICATION REQUIREMENTS

Article #43

Wherever the technology is available marketers should:

* transmit a telephone number such as the telephone number of the seller, service bureau or customer service department that the consumer can call back during normal business hours to ask questions and/or to request not to receive future calls, and

* transmit the name of the seller or service bureau.

Marketers should not block transmission of caller identification or transmit a false name or telephone number.

Telephone marketers using automatic number identification (ANI) should not rent, sell, transfer or exchange, without customer consent, telephone numbers gained from ANI except where a prior business relationship exists for the sale of directly related goods or services.

USE OF AUTOMATED DIALING EQUIPMENT

Article #44

Marketers using automated dialing equipment should allow 15 seconds or 4 rings before disconnecting an unanswered call.

Marketers should connect calls to live representatives within 2 seconds of the consumer's completed greeting. If the connection does not occur within the 2-second period, then the call is considered abandoned whether or not the call is eventually connected.
For any abandoned calls, the marketer should play a prerecorded message that includes the seller's name, telephone number, states the purpose of the call, and provides a telephone number at which the consumer can request not to receive future marketing calls.
Repeated abandoned or "hang up" calls to consumers' residential telephone numbers should be minimized. In no case should calls be abandoned more than:

* 3% of answered calls within a 30-day period (unless a more restrictive state law applies), or
* twice to the same telephone number within a 48-hour time period.

Marketers should only use automated dialing equipment which allows the telephone to immediately release the line when the called party terminates the connection.
When using any automated dialing equipment to reach a multi-line location, whether for business-to-consumer or business-to-business marketing, the equipment should release each line used before connecting to another.
Companies that manufacture and/or sell automated dialing equipment should design the software with the goal of minimizing abandoned calls to consumers. The software should be delivered to the user set as close to 0% as possible. Manufacturers should distribute these Guidelines for Automated Dialing Equipment to purchasers of dialing equipment and recommend that they be followed.

The dialers' software should be capable of generating a report that permits the user of the equipment to substantiate compliance with the guideline.

USE OF PRERECORDED VOICE MESSAGING

Article #45

Marketers who use prerecorded voice messaging should not automatically terminate calls or provide misleading or inaccurate information when a live consumer answers the telephone.

Prerecorded solicitations should include the name and telephone number of the seller, service bureau or customer service department where the consumer can call back during normal business hours to request not to receive future calls, ask questions or get service.

USE OF TELEPHONE FACSIMILE MACHINES

Article #46

Unless there is an established business relationship with the recipient, or unless the recipient has given prior permission, advertisements, whether sent to a consumer or a business, should not be transmitted to a facsimile machine, including computer fax machines. An established business relationship is defined as those persons with whom the marketer has had a transaction/received a payment within the last 18 months or those persons who have inquired about the marketer's products/services/causes within the last 3 months.

Each permitted transmission to a fax machine must clearly contain on the first page, the date and time the transmission is sent, the identity of the sender which is registered as a business with a State and the telephone number of the sender or the sending machine.

PROMOTIONS FOR RESPONSE BY TOLL-FREE AND PAY-PER-CALL NUMBERS

Article #47

Promotions for response by 800 or other toll-free numbers should be used only when there is no charge to the consumer for the call itself and when there is no transfer from a toll-free number to a pay call.
Promotions for response by using 900 numbers or any other type of pay-per-call programs should clearly and conspicuously disclose all charges for the call. A preamble at the beginning of the 900 or other pay-per-call should include the nature of the service or program, charge per minute and the total estimated charge for the call, as well as the name, address and telephone number of the sponsor. The caller should be given the option to disconnect the call at any time during the preamble without incurring any charge. The 900 number or other pay-per-call should only use equipment that ceases accumulating time and charges immediately upon disconnection by the caller.

DISCLOSURE AND TACTICS

Article #48

Prior to asking consumers for payment authorization, telephone marketers should disclose the cost of the merchandise or service and all terms and conditions, including payment plans, whether or not there is a no refund or a no cancellation policy in place, limitations, and the amount or existence of any extra charges such as shipping and handling and insurance. At no time should high pressure tactics be utilized.

Fund-Raising

Article #49

In addition to compliance with these guidelines, fund-raisers and other charitable solicitors should, whenever requested by donors or potential donors, provide financial information regarding use of funds.

Laws, Codes, and Regulations

Article #50

Direct marketers should operate in accordance with laws and regulations of the United States Postal Service, the Federal Trade Commission, the Federal Communications Commission, the Federal Reserve Board, and other applicable federal, state and local laws governing advertising, marketing practices and the transaction of business.

PRILOGA B: Primer verižnega pisma in njegovi sestavni deli

1. Zavajajoč predmet pisma

Predmet:Subject: Make A Wish Foundation (fwd)

2. Prepričevanje prejemnika

A pleas from a sick little girl,

Little Kimberly Anne is dying of a horrible tropical disease. Her goal, before she passes into the Great Beyond, is to collect as many free America Online disks as she can, to make the Guiness Book of Records. Her project is being sponsored by the Wish-Upon-a-Star Foundation, which specializes in fulfilling the final wishes of such sick little girls.

3. Prošnja

So, next time you get an unwanted AOL disk in the mail, don't throw it away! Think of the sparkle it will bring to the eye of a dying child. Write on the package:

Please copy this message and circulate it to your friends, neighbors, and co-workers. Only you can child's wish reality! God bless you from the Wish-Upon-a-Star Foundation!</h3>

PRILOGA C: Promocijska spletna stran INETGIANT

"Auto-mail 75 Million Targeted Opt-In Prospects Every Month
Using The Worlds Most Astonishing "Set And Forget" Technology!!"
Email 75 million TARGETED prospects every month!

No software to download, no specific expertise required. All from our servers!

Our membership offers you AUTOMATIC mailings to selected email groups. Subscribers of these groups have requested to be included in groups for people interested in new business opportunities, products or services.
Type your ad on your browser and click 'Send'. You are done.

Put your website promotion on autopilot!

Email 2.5 million safelist recipients at the press of a button spam free!

Got Questions???
Want to see even more features? click here!

InetGiant.com will skyrocket your traffic!

Our service is 100% spam free as we are only using targeted opt-in email lists and are mailing people that asked for your ads!

Send 2.5+ Million Emails Per Day

Easily and quickly send email from your browser to our
own opt-in email lists with 1-click! No special software required!

(100% opt-in, Send mail instantly from your browser!)

Rated #1 in Online Resources and Marketing Tools!

All mail is sent from our own servers.

100% Automated!!!

Powerful and easy to use!

You do not need set up any email software or anything else!

Drive targeted traffic to your Site!

Do you have an online Business or Product that just hasn't taken off like You thought it should? Or like You were Told it Would?

We can Dramatically IMPROVE Any Business!

Targeted email is the most direct and powerful method of marketing on the Internet today.

There are potentially millions of targeted buyers willing to purchase your product / service.

Do You Think You can Make more MONEY if You only had more Prospects? Our System can increase Your sales by 1200% overnight! Get ready to literally launch your Cash Flow into ORBIT!

Got Questions???
100% SPAM FREE Emails!

Are you Paying up to $20 per month subscribing to a FFA Site to draw email addresses from? 500 email addresses a day for $20 a month! You can email at least 2.5 Million a day for your whole lifetime for less when you use our system!

How can you get so many targeted leads?

Our opt-in email safe-lists are 100% opt-in and 100% legal. Your ad will reach ONLY those prospects who have asked to be included in opt-in safe-lists for people interested in new business opportunities, products or services. Each safelist has several thousand members that will be mailed each time you hit the send button. We are cooperating with several online companies to provide you with so many targeted leads every day!

And what are safe-lists?

Safe-lists are discussion groups of mutual interest through which subscribers can exchange information. Whenever you send a message to a safe-list, it is distributed to all the members. We individually qualify EACH safe-list for you to ensure TOP QUALITY.

Our safe-lists are 100% deliverable right to the prospects' mailboxes every day.

All it takes is one click through our incredible online blaster and you will be reaching a 100% opt-in audience that are of the highest response anywhere on the internet!!

You will be 100% targeting your services at individuals interested in Business Opportunities, Internet Marketing and Ordinary Products which means your product/service will convert at an astonishing RATIO and shoot your profits through the roof!!

Send your ad to 2.5 Million recipients each day with just a few clicks in your browser!

You Know People are Making Money ONLINE!
You've Tried and Typed and Tried and Typed! You've bought some things you didn't need! That All Stops Today! You Make Money Selling the Things You have, Not Falling for Every "Opportunity" Pops into your email "inbox"!

The Internet is Huge and growing every day!
Your Market is Growing every Day!

PRILOGA D: Tehnike filtriranja

TEHNIKA FILTRIRANJA	NAČIN DELOVANJA	ARGUMENTI ZA	ARGUMENTI PROTI
filtriranje po ključni besedi	e-pošta je sprejeta, če izpolnjuje specifičen, določen pogoj	enostavna implementacija, na voljo pri številnih ponudnikih e-pošte	slaba natančnost, pogoste pozitivne napake
filtriranje na osnovi pravil	e-pošta je filtrirana in izločena na podlagi ključnih besed, ki so povezane s skupkom pravil	lahko je zelo natančno	zahteva nenehno ažuriranje pravil, nenatančno, ker izpušča negativne napake
filtriranje bayesian	primerja analize preteklih spamov s statistično verjetnostjo, izhaja iz bayesian logike – je način umetne inteligence	lahko je zelo natančno, iz predhodnih spamov se uči prepoznavati sedanji spam,	natančnost je odvisna od kvalitete preteklih spamov, potrebna je prilagoditev posameznemu uporabniku
črni seznami	seznam, ki s prepoznavanjem IP naslovov loči spame od legitimne e-pošte	učinkovito blokirajo že znane vire spamov	zahteva nenehno ažuriranje, izpusti spame, katerih vir je nepoznan
prstni odtis	prepoznavanje spama deluje na podobnosti nazadnje prejetih sporočil	hitro prepoznavanje spama z visoko stopnjo natančnosti	ne prepozna novih spamov, zahteva nenehno posodabljanje iz centralnega vira
odgovor oporekanja	poziv pošiljatelja k izboljšanju prepoznavnosti njegove identitete predenj je e-pošta dostavljena	visoka stopnja zavrnitve spamov	poveča se število e-pošte, blokirajo se veljavne e-pošte poslane avtomatsko, zahteva večjezično podporo
varovano pošiljanje	poslana e-pošta mora imeti skrivnostno ID, ki jo filter prepozna in dokaže pošiljateljev obstoj	visoka stopnja zavrnitve spama, zanesljiva identifikacja vira e-pošte	zahteva splošno standardizacijo in podporo digitalne identitete, deluje le ob podpori zelo drage infrastrukture

Vir: www.informationweek.com/shared/printableArticle.jhtml?articleID=13101046

PRILOGA E: Antispam zakoni v posameznih državah Amerike

št.	država	leto	oznaka predmeta	opt-out	opt-in	veljaven naslov pošiljatelja	kroženje resničnih informacij	uporaba e-naslova tretjih oseb	uporaba domene tretjih oseb	UCE	UBE	e-pošta s porno vsebino	kršenje pravilnika ISP	programza prevare	omejena količina
1	Alaska	2003	adv:adlt							¤		¤			
2	Arizona	2003	adv	¤			¤	¤	¤	¤					
3	Arkansas	2001/2003	adv:adlt	¤		¤	¤		¤	¤		¤			
4	California	2003		¤	¤	¤			¤	¤	¤				
5	Colorado	2000	adv	¤		¤	¤	¤	¤	¤					
6	Connecticut	1999					¤				¤		¤	¤	
7	Delaware	1999			¤		¤			¤	¤			¤	
8	Idaho	2000		¤		¤	¤	¤		¤	¤				podobna vsebina, istočasno, min. 2
9	Illinois	1999/2003	adv:adlt	¤		¤	¤	¤	¤	¤	¤			¤	
10	Indiana	2003	adv:adlt	¤			¤		¤	¤					
11	Iowa	1999		¤		¤	¤	¤		¤	¤				
12	Kansas	2000	adv:adlt	¤			¤		¤	¤	¤			¤	> 500

št.	država	leto	oznaka predmeta	opt-out	opt-in	veljaven naslov pošiljatelja	kroženje resničnih informacij	uporaba e-naslova tretjih oseb	uporaba domene tretjih oseb	UCE	UBE	e-pošta s porno vsebino	kršenje pravilnika ISP	programza prevare	omejena količina
13	Louisiana	1999/2003	adv:adlt				¤				¤		¤	¤	> 1000
14	Maine	2003	adv:adlt	¤		¤	¤	¤	¤	¤					
15	Maryland	2002					¤		¤	¤					
16	Michigan		adv	¤		¤	¤			¤				¤	
17	Minnesota	2002	adv:adlt	¤			¤		¤	¤					
18	Missouri	2000	adv:adlt	¤			¤			¤					
19	Nevada	1997, 2001,2003	adv	¤		¤	¤			¤					
20	New Mexico	2003	adv:adlt	¤						¤					
21	North Carolina	1999					¤				¤		¤		
22	North Dacota	2003	adv:adlt	¤			¤		¤	¤					
23	Ohio	2002		¤		¤	¤			¤			¤		
24	Oklahoma	1999, 2003	adv:adlt	¤			¤	¤	¤	¤				¤	
25	Oregon	2003	adv					¤			¤		¤		

št.	država	leto	oznaka predmeta	opt-out	opt-in	veljaven naslov pošiljatelja	kroženje resničnih informacij	uporaba e-naslova tretjih oseb	uporaba domene tretjih oseb	UCE	UBE	e-pošta s porno vsebino	kršenje pravilnika ISP	programza prevare	omejena količina
26	Pennsylvania	2000, 2002	adv:adlt	¤		¤	¤		¤	¤				¤	
27	Rhode Island	1999		¤			¤		¤	¤	¤		¤	¤	
28	South Dakota	2002	adv:adlt				¤			¤					
29	Tennessee	1999	adv:adlt	¤			¤				¤		¤	¤	
30	Texas	2003	adv:adlt	¤		¤	¤			¤					
31	Utah	2002	adv:adlt	¤		¤	¤			¤					
32	Virginia	1999, 2003					¤				¤		¤	¤	
33	Washington	1998, 1999					¤		¤	¤					
34	West Viriginia	1999				¤	¤		¤		¤		¤	¤	kršenje pravil ISP
35	Wisconsin	2001	adult advertisment							¤					
36	Wyoming	2003					¤		¤	¤					
1	Kentucky	nimata anti spam zakona, ampak pravilo vrhovnega sodišča je: če napisani oglas potuje preko elektronske komunikacije, mora imeti oznako "THIS IS AN ADVERTISMENT"													
2	Florida														
Kršitve zakonov se različno kaznujejo: od 10 $ na posamezno e-pošto pa do 100.000 $ na posamezen primer pošiljanja in/ali povrnitev stroškov za nastalo škodo prejemniku ali ISP-ju,															

PRILOGA F: Mnenje Urada za varstvo potrošnikov; ga. Zupan

1. Kdo je sodeloval pri oblikovanju zakona?

Zakon smo sestavili: Ministrstvo za gospodarstvo, Urad za varstvo potrošnikov, Tržni inšpektorat RS, Gospodarska zbornica Slovenije, in posamezne potrošniške organizacije.

2. Zakaj zakon ne opredeljuje spama?

Zakon spama ne opredeljuje, ker je za varstvo potrošnikov relevantno zgolj to, da se prepreči njihovo nadlegovanje z nezaželenimi sporočili. Vsako komercialno e-sporočilo ne glede na poslano število kopij je lahko označeno kot spam. Pri oblikovanju pravil smo upoštevali direktivi Evropske Unije 2000/31/EC in 97/7/EC . Po zgledu EU direktiv tudi naš zakon v 2. členu zakona o varstvu potrošnikov določa glavne sestavine e-pošte, ki so potrebne za jasno prepoznavnost e-pošte.

3. Glede na to, da spam ni opredeljen prosim, razvrstite našteta e-sporočila s katerimi bi kršili zakon, če bi jih poslali brez dovoljenja?

Z njimi kršimo zakon	**Z njimi ne kršimo zakona**
Oglas za izdelek ali storitev	
Anketa	
Pismo, ki spodbuja k dobrodelnosti	
Vabilo na prireditev	
Proti spam sporočilo	
Sporočilo zaradi profitne dejavnosti	

Spam je vsako e-sporočilo, ki ga podjetje pošlje potrošniku brez njegovega dovoljenja. Že prvo e-sporočilo, ki prosi za dovoljenje pošiljanja je v nasprotju z zakonom.

4. Ali zakon določa kako naj se vrši opt-out funkcija?

Zakon ne opredeljuje načina izvajanja izpisa iz seznama, niti ni določeno, da mora pošiljatelj omogočati izpis iz seznama brezplačno.

5. Ali že imate prve informacije o izvajanju zakona in kdo so prvi kršitelji?

Do sedaj kazen kršiteljem še ni bila izrečena kljub temu,da smo že prejeli kar nekaj prijav nespoštovanja zakona. Zakon velja za vsa podjetja, ki poslujejo na našem trgu, tako na področju mobilne telefonije kot na področju interneta, vendar o posameznih kršiteljih v tem trenutku še ne moremo govoriti.

6. Menite, da bo zakon v Sloveniji omejil pošiljanje spama?

Novi zakon bo gotovo ustavil rast nezaželene e-pošte. Visoke kazni bodo odvrnile podjetja od takšnega načina izvajanja direktnega marketinga – od pošiljanja spamov.

PRILOGA G: Mnenje slovenskih ponudnikov interneta: Arnes, Voljatel

1. Se tudi vi kot ponudnik interneta srečujete s problemi spama?

Arnes
Velika količina nezaželene pošte tedenjsko ovira delovanje našega pštnega strežnika. Sorazmerno s količino spama se povečuje nezadovoljstvo uporabnikov. Pravtako spam posredno in neposredno vpliva na finčne učinke. Pogosto pa je tudi metoda za razširanjanje virusov.

Voljatel
Tudi pri nas se vsaj enkrat tedensko srečujemo s težavami, ki jih povzroča spam.

2. Kako se borite proti spamu?

Arnes
Spamu se upiramo z osveščanjem naših uporabnikov, s primerno programsko opremo, ki omogoča filtriranje in s posredovanjem pritožb uporabnikov tržni inšpekciji.

Voljatel
Z uporabo antispam programov želimo omejiti spam sporočila in njihove negativne učinke.

3. Kakšen filtrirni sistem uporabljate in ali ste zadovoljni z njim?

Arnes
Uporabljamo sistem, ki temelji na odprti kodi. Uporabniku dopuščamo možnost samoodločitve o filtriranju oz. moči filtriranja e-pošt. Izbrana pošta se znajde v posebni mapi »spam« , ki jo uporabnik lahko še pregleda. Po enem mesecu pa se podatki v njej izbrišejo. Sistem odprte kode smo izbrali zaradi primernosti, načela odprte kode, znanja, s katerim razpolagamo in zaradi tega, ker sistem deloma deluje na »učenju« razpoznavnosti odpadne pošte.

Voljatel
Mi smo se odločili za spam-killer. Sistem deluje na osnovi določenih besed in skupin. S filtrom smo zelo zadovoljni in se nam zdi trenutno eden najboljših.

4. Ali poznate bayesian filtre in kaj menite o njihovi učinkovitosti?

Arnes
Bayesian filtre poznamo in menimo, da je njihova učinkovitost boljša v primerjavi z drugimi filtri

Voljatel
Jih ne poznamo.

5. Podpirate filtriranje na osnovi RBL in če ne, zakaj ne?

Arnes
Mi nasprotujemo filtriranju na osnovi RBL, saj se pri takemu načinu filtriranja zavrne veliko legitimne e-pošte.

Voljatel
Filtriranje na osnovi RBL je uspešno.

6. Kako ocenjujete učinkovitost filtrov v primerjavi z drugimi regulacijami in samoregulacijo v primerjavi s filtri?

Arnes
Filtre obidejo številni spami in zavrnejo številne legalne pošte, zato menimo, da je njihova učinkovitost nizka. Lahko rečemo, da je samoregulacija veliko bolj uspešna.

Voljatel
Filtri so ena najbolj učinkovitih sredstev za regulacijo spama. Samoregulacija je po našem mnenju še najmanj učinkovita.

7. Ali ste že prejeli pritožbe uporabnikov zaradi spamov in če ste, kako ste ravnali v takšnem primeru?

Arnes
Vse več dobivamo pritožb naših uporabnikov. Posredujemo jih tržni inšpekciji ali direktno posvarimo pošiljatelja, če je le ta znan. Večji problem je pri pošti, ki je prispela iz tujine, saj ne moremo direktno kontaktirati s pošiljateljem.

Voljatel
Prejeli smo že kar nekaj pritožb uporabnikov. Če je mogoče prepoznati identiteto pošiljatelja, ga opomnimo.

8. Ali je pošiljatelj e-pošte vedno prepoznaven?

Arnes
Pošiljatelji spama večkrat skrijejo svojo identiteto. To dosežejo z uporabo odprtih povezav, neobstoječih domeni in potvarjanjem glave sporočila.

Voljatel
Proxy – multiple omogočajo spamerjem zakritje sledi in njihove identitete.

9. Kako bi definirali spam in kateri so glavni dejavniki, ki pospešujejo njegovo rast?

Arnes
Definicija: za spam sporočilo lahko smatramo vsako sporočilo, ki je poslano večjemu številu naslovnikov, z namenom vsiljevanja vsebine, ki se je naslovniki sami ne bi odločili prejemati. Rast spam sporočil pospešujejo predvsem trije dejavniki: neosveščenost uporabnikov, dostopnost in zmnožnost tehnologije, pomanjkanje regulacije.

Voljatel
Spam je nezaželenana pošta. Glavni vzrok večanja obsega spam sporočil pa je neosveščenost uporabnikov.

10. Kaj po vašem mnenju ovira učinkovitost regulacij?

Arnes
Sam koncept interneta onemogoča kakršnekoli dokončne rešitve. Učinkovitost reguliranja količine spama zavirajo naslednji dejavniki: neosveščenost uporabnikov, nedodelanost zakonodaje, različne odpredelitve, neusklajenost zakonov po državah in zapoznela zakonodaja.

Voljatel
Pomanjkljivosti regulacij so: neosveščenost uporabnikov, različne opredelitve spama in nedodelanost zakonodaje.

11. Kako bi vi rešili problem spama?

Arnes
- z osvešanjem uporabnikov in opozarjanjem na problem povezan z virusi,
- z izboljševanjem filtrirnih sistemov, prilaganjem novim metodam spama,
- z odpravljanjem odprtih povezav,
- z zakonodajo, ki bi kaznovala vsaj hude kršitelje, ki bi bili prepoznavni,
- z usklajeno mednarodno zakonodajo in protokoli sodelovanja med ponudniki storitev.
-

Voljatel

12. Ali poznate slovenski antispam zakon in kaj menite o njem?

Arnes
Naš zakon ne bo dovolj učinkovit, ker je pošiljatelj odgovoren le, če pošilja e-pošto na osebne naslove in ne tudi na generične naslove (npr. @podjetje.si). sicer pa bo učinkovitost kot vedno odvisna od učinkovitosti in pristojnosti inšpekcije in tržnega inšpektorata.

Voljatel
Slovenski zakon nam je znan in menimo, da bo precej neučinkovit in težko izvedljiv.