

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

**ODNOS SLOVENSКИH UPORABNIKOV E-POŠTE
DO NEZAŽELENIH E-SPOROČIL**

Ljubljana, junij 2007

TINA ŠTUKELJ

IZJAVA

Študentka Tina Štukelj izjavljam, da sem avtorica tega diplomskega dela, ki sem ga napisala pod mentorstvom dr. Starman Danijela, in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne 1.6.2007

Podpis: _____

Kazalo

1.	UVOD.....	1
2.	OSNOVNE OPREDELITVE	1
3.	TRŽNO KOMUNICIRANJE	2
3.1.	SPLET TRŽNEGA KOMUNICIRANJA	3
4.	NEPOSREDNO TRŽENJE KOT DEL TRŽNEGA KOMUNICIRANJA	4
4.1.	OBLIKE NEPOSREDNEGA TRŽENJA	5
5.	ELEKTRONSKO OZ. E-TRŽENJE	6
5.1.	NAČINI KOMUNICIRANJA PRI ELEKTRONSKEM TRŽENJU.....	8
5.2.	ELEKTRONSKE OZ. E-FUNKCIJE V PODJETJU.....	9
5.3.	INTERNET	9
5.3.1.	Zgodovina interneta.....	10
5.3.2.	Internet v Sloveniji	11
5.3.3.	Zasebnost na internetu	11
5.4.	ELEKTRONSKO OZ. E-TRŽENJE	12
5.4.1.	Trženje preko svetovnega spleta.....	13
5.4.2.	Trženje preko elektronske oz. e-pošte	14
6.	E-POŠTA KOT DEL E-TRŽENJA.....	15
6.1.	ZGODOVINA NEZAŽELENIH E-SPOROČIL	16
6.2.	DELEŽ NEZAŽELENIH E-SPOROČIL	17
6.3.	PRIDOBIVANJE BAZE E-NASLOVOV	18
6.4.	ZAŠČITA IN ODGOVOR SPAMERJEV	19
6.5.	STRUKTURA E-SPOROČILA	23
6.6.	STROŠKI IN NEZAŽELENA E-SPOROČILA.....	24
7.	ZAKONODAJA IN E-POŠTA.....	26
8.	RAZISKAVA O ODNOSU SLOVENSКИH UPORABNIKOV ELEKTRONSKE POŠTE DO NEZAŽELENIH E-SPOROČIL	29
8.1.	OPREDELITEV NAMENA IN CILJEV RAZISKAVE	29
8.2.	METODOLOGIJA	30
8.3.	STRUKTURA VZORCA	31
8.3.1.	STRUKTURA VZORCA GLEDE NA SPOL	31
8.3.2.	Struktura vzorca glede na starost.....	31
8.3.3.	Struktura vzorca glede na status	32
8.3.4.	Struktura vzorca glede na izobrazbo.....	32
8.4.	NEZAŽELENA E-SPOROČILA IN SLOVENSKI UPORABNIKI E-POŠTE	33
8.4.1.	Razširjenost nezaželenih e-sporočil.....	33
8.4.2.	Vsebina in izvor prejetih nezaželenih e-sporočil.....	34
8.4.3.	Odnos potrošnikov do nezaželene elektronske pošte	35
8.4.4.	Seznanjenost z zakonodajo	37
8.4.5.	Vpliv pošiljanja nezaželenih e-sporočil na ugled podjetja	37
8.4.6.	Razlika v odzivu med starostnimi skupinami	37
8.4.7.	Povzetek raziskave	38
9.	SKLEP	39
	LITERATURA.....	40
	VIRI.....	41
	PRILOGE	

1. Uvod

Ker naj bi se vrednost izmenjanih informacij in posredovanih dobrin ter storitev preko interneta vsako leto podvojila, če ne celo potrojila, podjetja v prihodnosti ne bodo imela več izbire ali naj se odločijo za vstop na internetni trg ali ne, saj bi vsako izogibanje temu koraku peljalo podjetje v njegov propad. Vendar pa ne bo potrebno le vstopiti v svetovni splet, temveč pošteno premisliti, s katerim orodjem bi lahko dosegli svoje cilje. So orodja, ki te ne pripeljejo do cilja, temveč te pokopljejo, in takih se je potrebno izogibati. Je morda oglasno e-sporočilo eno izmed teh orodij?

Dnevno po svetovnem spletu kroži na milijone elektronskih oz. e-sporočil in vedno več je med njimi oglasnih. Nezaželena e-sporočila, imenovana tudi spam, so nadloga, s katero se morajo ubadati malone vsi uporabniki storitev interneta. Zanimalo me je ne le struktura nezaželenih e-sporočil, temveč predvsem kakšen je odnos uporabnikov elektronske pošte do prejemanja nezaželenih e-sporočil.

V prvem delu diplomske naloge sem opredelila teoretično in praktično stran oglasnih e-sporočil. Zanimalo me je, v kateri del tržnega komuniciranja sodijo oglasna e-sporočila, na kaj vse vplivajo, kakšne so prednosti in slabosti le-teh, ipd. Preučila sem tudi negativne posledice in stroške, ki jih nezaželena e-sporočila povzročajo ter na drugi strani tudi zakonodajo, ki naj bi pokrivala to področje.

V praktičnem delu sem se ukvarjala predvsem s tem, kako Slovenci sprejemajo nezaželena e-sporočila. Naokoli sem poslala e-sporočilo z internetnim naslovom do ankete in prejela precejšnje število odgovorov. Zanimalo me je, koliko je sploh nezaželenih e-sporočil med slovenskimi uporabniki interneta in kako se odzivajo nanje, pa tudi kakšne so razlike v sprejemanju in odzivanju.

2. Osnovne opredelitve

V nadaljevanju diplomske naloge bom uporabljala predvsem naslednje oznake:

- **Elektronsko oz. e-sporočilo** je vsako sporočilo v obliki besedila, glasu, zvoka ali slike, poslano po elektronskem komunikacijskem omrežju, ki se lahko shrani v tem omrežju ali v prejemnikovi terminalski opremi, dokler je prejemnik ne prevzame. Elektronsko sporočilo se po omrežju prenaša iz pošiljateljevega računalnika na prejemnikovega, vmes pa se lahko ustavi na strežniku (Zakon o elektronskih komunikacijah, 2004).

- **Elektronska oz. e-pošta** je način sestavljanja, pošiljanja in sprejemanja sporočil po elektronskih komunikacijskih sistemih. Večina sistemov e-pošte danes uporablja internet, po drugi strani pa je e-pošta eden najpogostejših uporab interneta (Wikipedia, 2006).
- **Spam oz. nezaželeno e-sporočilo** (tudi vsiljeno, nadležno ali nenaročeno) je pošiljanje enakih ali podobnih sporočil na veliko število naslovov. Spam največkrat vsebuje oglasna sporočila (Wikipedia, 2006).
- **Oglasno e-sporočilo** je sporočilo, ki vsebuje elemente oglasa oz. nas usmerja k določenemu izdelku ali storitvi. Oglasno e-sporočilo je lahko naročeno in v takem primeru ni nezaželeno e-sporočilo.
- **Spamer oz. pošiljatelj nezaželenih e-sporočil** je oseba, ki naokoli pošilja nezaželena e-sporočila.

3. Tržno komuniciranje

Z naraščanjem števila izdelkov v današnjem svetu je prišlo tudi do velike diferenciacije pri izdelkih. Lastnosti, cena in način dostave že dolgo niso edini dejavniki uspeha pri zagotavljanju prodaje.

V trženjskem spletu, ki ga sestavljajo izdelek, cena, tržne poti in tržno komuniciranje, je slednje najbolj viden element. Podjetja so strošek za tržno komuniciranje dolga leta videla kot nepotrebno razmetavanje denarja, skozi leta pa je dobilo svoje priznanje. Iz leta v leto so zneski, ki jih podjetja namenjajo svojim trženjskim akcijam večji in dosegajo vrtooglave višine. Trženjske aktivnosti se delijo na t.i. aktivnosti nad črto, ki se nanašajo na oglaševanje kot plačano obliko tržnega komuniciranja in na t.i. aktivnosti pod črto, kjer ne moremo spremljati izdatkov in je s tem tudi otežkočena merljivost oz. dokazljivost rezultatov. Bruto vrednost oglaševanja v Sloveniji je po podatkih Mediane (Setinšek, 2006) že drugo leto dosegla 8% rast in je v letu 2006 znašala 376,9 milijonov €. Neto vrednost oglaševanja je lani znašala 130 milijonov €, kar znaša 35% bruto vrednosti oglaševanja.

Vkolikor podjetje skrbno identificira svojo ciljno skupino, konkretno določi cilje komuniciranja, jasno oblikuje sporočilo, ki ga po pravih komunikacijskih kanalih prenese do potrošnika oz. naslovnika in pri tem realno določi finančna sredstva ter izbere najustreznejše instrumente komunikacijskega spleta, je uspeh tržnega komuniciranja neizbežen in prodaja steče.

3.1. Splet tržnega komuniciranja

Splet trženjskega komuniciranja je sestavljen iz petih poglavitnih načinov komuniciranja (Kotler, 2006, str. 555-556):

- **Oglaševanje**

American Marketing association je oglaševanje opredelila kot »vsaka plačana oblika neosebne predstavitve ali promocije idej, izdelkov ali storitev za znanega naročnika.«

Oglaševanje poteka na različne načine in preko različnih množičnih medijev, odvisno od tega, kje na krivulji življenjskega ciklusa se izdelek nahaja. Najpogosteje uporabljena orodja komuniciranja v oglaševanju so tiskani oglasi, oglasi na TV in radiu, embalaža in letaki v embalaži, brošure, plakati ipd.

Na slovenskih televizijskih programih se je v letu 2006 predvajalo kar za 2132 ur oglasov v vrednosti 194,5 milijonov €. Sledijo tiskani mediji, kjer je bruto vrednost oglaševanja v letu 2006 znašala 124,5 milijonov €. Medij, ki je dosegel v preteklem letu najvišjo rast bruto vrednosti (58%), pa je internet, kjer je skupna bruto vrednost oglaševanja znašala 7 milijonov € (Setinšek, 2006).

- **Pospeševanje prodaje**

Pri pospeševanju prodaje gre predvsem za spodbujanje k nakupu, pri čemer gre ponavadi za kratkoročno povečanje prodaje, ki pa zna v kombinaciji z ostalimi orodji prerasti tudi v dolgoročno izboljšanje prodajnih rezultatov.

Najpogostejša orodja komuniciranja so nagradna tekmovanja, žrebanja, vzorci, razstave, programi zvestobe...

- **Odnosi z javnostjo**

Namen odnosov z javnostjo je predvsem ustvarjanje nekega pozitivnega javnega mnenja o podjetju ali njegovih delih. Pri tem hočemo ustvariti vtis, da je podjetje aktiven član, ki deluje za dobro širše skupnosti.

Orodja komuniciranja, ki so najpogosteje uporabljena so govori, seminarji, konference, donatorstva, sponzoriranje, lobiranje...

- **Osebna prodaja**

Osebna prodaja je pomembna predvsem pri izdelkih, kjer z ostalimi sredstvi potrošniku ne posredujemo dovolj informacij, da bi se odločil za nakup, bodisi ker gre za investicijske nakupe, kjer so potrebni tehtni premisleki, ali za nakupe kompleksnejših izdelkov, ki zahtevajo podrobnejšo predstavitev.

Najprimernejša orodja so prodajne predstavitve in srečanja, vzorci, sejemske predstavitve...

- **Neposredno trženje**

Neposredno trženje je novejša oblika tržnega komuniciranja, njegova uporaba pa se je v zadnjih letih močno razširila in odkriva vedno nove in nove medije, v katerih lahko na neoseben način pride neposredno do potrošnika. Ena od opredelitev neposrednega trženja pravi, da je neposredno trženje ciljno komuniciranje, ki nam omogoča vzpostaviti osebni odnos s stranko in predvsem takojšen in izmerljiv odziv. Je stroškovno učinkovito orodje ravno zaradi ciljnega komuniciranja s posameznimi ciljnim skupinami, ki jih družijo določene skupne značilnosti (PCMG, 2006).

Najpogostejše uporabljena orodja so katalogi, nenaslovljena pošta, trženje po telefonu, e-pošta...

4. Neposredno trženje kot del tržnega komuniciranja

Združenje za neposredno trženje (Direct Marketing association) je neposredno trženje opredelilo kot »interaktiven sistem trženja, ki uporablja enega ali več oglaševalskih medijev, da na katerikoli lokaciji pripelje do merljivega odziva in/ali transakcije« (Kotler, 1996, str. 665). Ena izmed bolj podrobnih opredelitev neposrednega trženja pravi, da je neposredno trženje »področje nauka o trženju, ki zajema takšen splet prodajnih metod, tržnega komuniciranja in prodajnih poti, kjer skuša tržnik vzpostaviti neposreden stik z neznanim potrošnikom, ga spoznati, oblikovati datoteko podatkov o njem in jo uporabiti za selekcioniran tržni pristop k tako segmentiranemu trgu, obenem pa vzpostaviti možnost merjenja uspešnosti oglaševalske in prodajne akcije. Končni cilj neposrednega trženja je vzpostavitev dvosmerne komunikacije med tržnikom in spoznanimi kupci, doseči trajnejši odnos, večji odziv na akcije, prilagojene ciljnim skupinam in povečati prodajo; vse to z neposrednim osebnim stikom, komuniciranjem po pošti, telefonu ali drugih elektronskih medijih« (Starman, 1996, str. 38).

Neposredno trženje se začne kot proces neposredne neosebne komunikacije med proizvajalcem oz. ponudnikom izdelka in neznanim potrošnikom. V večstopenjskem neposrednem trženju se ta komunikacija lahko nadgradi v dvostransko, pri čemer lahko

proizvajalec o potrošniku pridobi kopico koristnih podatkov za uspešno segmentacijo in proces se nadaljuje v obliki individualne komunikacije z znanimi potrošniki.

3 osnovne značilnosti neposrednega trženja (Kotler, 2006, str. 556):

- **Prilagojeno:** sporočilo je lahko naslovljeno na posameznika;
- **Sodobno, v koraku s časom:** sporočilo je lahko napisano v zelo kratkem času;
- **Interaktivno:** sporočilo je lahko prilagojeno/spremenjeno v skladu s posameznikovim odgovorom.

Uspešnost neposrednega trženja temelji predvsem na natančnosti in ažurnosti baze podatkov o kupcih in jasnosti samega sporočila, ki jim ga posredujemo. Bazo podatkov je potrebno neprenehoma preverjati in osveževati z novimi informacijami, saj na teh temelji celotna segmentacija, ki ima velik vpliv na doseganje naših ciljev, prav tako pa neustrezna oz. zastarela baza podatkov povzroči, da dosežemo le majhen del ciljnega občinstva.

Učinki neposrednega trženja so lahko merljivi. Stopnja odziva je glavno merilo za uspešnost akcij neposrednega trženja, izračunamo pa jo kot razmerje med številom nagovorjenih potrošnikov in številom potrošnikov, ki so se dejansko odzvali.

4.1. Oblike neposrednega trženja

Odvisno od tega, katere prodajne poti se poslužujemo, ločimo več oblik neposrednega trženja:

- **Prodaja po pošti**

Kanal, po katerem se prenašajo sporočila, je poštna dostava. Pošta Slovenije dostavi letno več kot 70 milijonov različne neposredne pošte v nabiralnike po celi Sloveniji (Pošta Slovenije, 2007).

Najbolj uporabljeni so prospekti za kratkotrajne ponudbe, prodajna pisma, oglasi s priloženimi naročilnicami, ipd. Še nekaj let nazaj je bila to zelo uspešna oblika komuniciranja s potrošniki, danes pa zaradi prenasičenosti v košu konča marsikateri od neprebranih katalogov, prospektov in ostalih neposrednih ponudb. Prav tako se je na trgu pojavila potreba, da se omeji možnost dostopa takemu promocijskemu materialu do vsakega nabiralnika, zato si potrošniki lahko kupijo »protireklamno nalepko« (Pošta Slovenije, 2006), ki stane 0,42 € in se jo nalepi na nabiralnik ter prepoveduje poštnim delavcem poleg poštnih pošiljk puščati tudi oglasna sporočila.

Kot vrsti medija, po kateri se lahko izvaja neposredno trženje, sta se pojavili tudi elektronska in glasovna pošta.

- **Prodaja po katalogu**

Prodaja po katalogu je za kupca precej udoben način seznanjanja s ponudbo podjetja, čeprav pride do težave pri izdelkih, kjer je zaželen neposreden stik z izdelkom.

Za podjetje ta oblika promocije ni tako stroškovno ugodna, saj izdelava in distribucija katalogov zahteva precej denarja, prav tako pa potrebujemo tudi večje število osebja, ki skrbi za nemoten potek naročil, embaliranja in distribucije izdelkov.

- **Prodaja od vrat do vrat**

Pri tej metodi gre za dvosmerno osebno komunikacijo med prodajalcem in potencialnim kupcem, pri čemer gre lahko za nenajavljen obisk, zmenjen obisk in predstavitev izdelka na domu potencialnega kupca ali pa predstavitevno srečanje oz. zabavo, kjer ima stranka poleg pridobivanja vseh pomembnih informacij o izdelku možnost tudi nakupa le-tega.

Stroški so zaradi visoke provizije in treninga prodajnega osebja pri tej metodi neposrednega trženja precej visoki.

- **Prodaja po telefonu**

Ločimo aktivno in pasivno prodajo po telefonu. Pri pasivni prodaji komunikacijo začne kupec, ki je zasledil neko informacijo o izdelku in se sedaj obrača neposredno na podjetje, da bi izvedel več podatkov ali celo naročil izdelek. Pri tej obliki se podjetja največkrat poslužujejo brezplačne linije 080.

Aktivna prodaja po telefonu lahko služi kot element za pridobivanje podatkov o kupcih, ki jih uporabimo pri ostalih vrstah prodajnih metod, ali pa gre za samostojno obliko, pri kateri prodajalec kontaktira potencialnega kupca z namenom, da mu kar preko telefona proda svoj izdelek ali posreduje informacije, s katerimi bi vzpodbudil nakup.

5. Elektronsko oz. e-trženje

Vsak nastanek novega medija pripelje oglaševalce do iskanja novih načinov trženja svojih izdelkov in storitev. Tudi nastanek interneta ni nobena izjema; v zadnjih 15 letih, odkar je internet širše dostopen tudi "navadnim" ljudem, je nastalo že kar nekaj novih načinov posredovanja informacij potrošnikom in oglaševanja izdelkov ter storitev. Prednost e-trženja

je predvsem v nizki ceni, hitri dosegljivosti želenih potrošnikov, možnosti hitrega odgovora in medsebojne komunikacije.

Hkrati je za to obliko trženja značilno, da vsebuje skoraj vse elemente tržnega komuniciranja, od neposrednega trženja do pospeševanja prodaje in odnosov z javnostjo. Z uporabo različnih orodij lahko dostopamo do večih tipov potrošnikov ali pa zgolj pustimo, da le-ti sami najdejo nas. Prav tako lahko elemente e-trženja uspešno kombiniramo z ostalimi elementi tržnega komuniciranja, s čimer lahko močno povečamo učinkovitost trženjskih aktivnosti.

Tabela 1: Primerjava tržnega komuniciranja pri tradicionalnem in e-trženju

Tradicionalno tržno komuniciranje	Elektronsko tržno komuniciranje
Množično komuniciranje.	Komunikacije so individualizirane in temeljijo na podrobnih informacijah o strankah.
Neosebni komunikacijski kanal brez interakcije; enosmerna komunikacija z relativno velikim tržiščem z različnimi nakupovalnimi navadami.	Možnost osebnega pristopa in dvosmerne medsebojne komunikacije s ciljno skupino, ki ima zelo podobne nakupovalne navade.
Odgovornost za uspešne odnose s strankami je na strani distributorjev, trgovcev na drobno in prodajnega osebja.	Tržniki se ukvarjajo neposredno s strankami.
Klasično oglaševanje: vsiljivi oglasi širši množici.	Stranka sama išče informacije in ima možnost, kaj si bo ogledala.

Vir: Skrt, 2001.

Ker je tudi e-trženje doživelo precej velik razmah in so potrošniki »napadeni« preko elektronskih kanalov iz vseh strani, je doseg trženjskih akcij vedno manjši. Pogosto gre za obratno sorazmerje – več, kot sprejmejo sporočil, manj jih potrošniki dejansko pogledajo.

Seth Godin¹ je uvedel izraz »permission« marketing oz. trženje z dovoljenjem (Kotler, 2003, str. 628), ki temelji na dejstvu, da potrošniki vplivajo na to, katere informacije so jim posredovane. Opredeli 5 stopenj takega trženja oz. odnosa, ki ga imajo potrošniki:

- **Stopnja NE**, pri kateri potrošnik noče imeti nobenega opravka s podjetjem;
- **Stopnja šibke odobritve/dovoljenja**, kjer potrošnik prizna, da ne ve veliko o podjetju, bi pa morda preveril njegovo ponudbo;
- **Stopnja srednje močne odobritve/dovoljenja**, pri kateri potrošnik pozna podjetje, vendar je do njega indiferenten; vkolikor bi podjetje do njega pristopilo na vljuden način, bi verjetno dovolil pošiljanje oglasov, sporočil;

¹ Bivši direktor Yoyodyne Inc, ki je danes del podjetja Yahoo!.

- **Stopnja močne odobritve/dovoljenja**, kjer potrošnik še ni posloval z podjetjem, vendar je prepričan, da le-to ponuja storitve oz. izdelke, ki jih potrebuje, zato je pripravljen posredovati veliko podatkov o sebi, da bi pridobil čim več informacij (katalogov, oglasov, akcij...) o omenjenih izdelkih ali storitvah;
- **Stopnja poslovanja**, kjer je potrošnik že tudi stranka podjetja in z njim redno posluje, ji zaupa in je z njim zadovoljen, zato mu podjetje ne pošilja več ogromnih količin nepotrebnih oglasov.

Glede na raziskavo, ki jo je izvedlo podjetje Jupiter Research (Jupiter Research, 2006), naj bi se izdatki namenjeni e-trženju povečali iz 885 milijonov USD v letu 2005 na kar 1100 milijard USD v letu 2010. David Schatsky, predsednik omenjene agencije, pravi, da bo trženjska arena v naslednjih 5 letih postala veliko bolj organizirano bojno polje. Tržniki se bodo morali pošteno potruditi, da bodo lahko ob naprednem filtriranju sporočil še naprej dosegali izjemne rezultate svojih akcij.

5.1. Načini komuniciranja pri elektronskem trženju

Internet je medij, ki omogoča več različnih načinov komunikacije. Skupna značilnost vseh spodaj omenjenih oblik je, da gre za dvostransko komunikacijo, ki pošiljatelju sporočila omogoča povratno informacijo.

- **En z enim**

Gre za osebno komunikacijo med dvema subjektoma. Osnovno orodje za tako vrsto komuniciranja pri e-trženju je e-sporočilo, pri čemer je tako sporočilo namenjeno le enemu sprejemniku.

- **En z mnogimi**

Pri tej vrsti je eno sporočilo namenjeno večim subjektom, zato lahko sem prištevamo tako vsa orodja, ki jih uporabljamo pri trženju preko svetovnega spleta (glej poglavje 5.4. Elektronsko oz. e-trženje), kot tudi e-sporočilo, ki je posredovana na več različnih naslovov.

- **Mnogi z mnogimi**

Kar nekaj strokovnjakov meni, da je to edina oblika komunikacije, ki je mogoča na internetu.

5.2. Elektronske oz. e-funkcije v podjetju

Elektronsko oz. e-poslovanje ni le vsaka poslovna transakcija, ki se odvija preko internetne mreže, temveč je okrepitev uspešnosti poslovnega delovanja in korak k boljši povezavi tako s partnerji, kot s kupci. E-poslovanje ni le delovanje na internetu, čeprav je res, da je večji del njegovega učinka viden prav tam. Gre za nov način posredovanja informacij, nakupa in plačila izdelkov, pa tudi medsebojne komunikacije med partnerji in kupci. Poleg zmanjševanja stroškov so glavne prednosti e-poslovanja tudi krajšanje reakcijskega časa z avtomatizacijo poslovnih procesov, razširjanje poslovnih možnosti in potencialnih trgov ter ažurno posredovanje informacij o zmožnostih in znanju podjetja partnerjem in kupcem.

E-poslovanje se nanaša tako na poslovanje med dvema pravnima subjektoma (B2B) kot tudi na poslovanje s končnimi kupci (B2C), pri čemer se njegova funkcija razlikuje med vrstama poslovanja. Pri B2B poslovanju gre bolj za utrditev vezi in olajšanje medsebojnega sodelovanja, medtem ko je pri B2C poslovanju poudarek v posredovanju informacij o nakupih in izvajanju same prodaje preko interneta končnim kupcem.

Pod pojmom e-trgovina razumemo v prvi vrsti opravljanje prodaje in ostalih poslovnih transakcij preko interneta. E-trženje poleg tega vsebuje še funkcijo informiranja strank ter oglaševanja podjetja in njegovih izdelkov oz. storitev.

Razmah e-poslovanja je sprožilo tudi ustanavljanje novih vrst podjetij, ki jih imenujemo »virtualna« podjetja. Ena od opredelitev opisuje virtuano podjetje kot začasno mrežo neodvisnih inštitucij, podjetij ali specializiranih posameznikov, ki se ob intenzivni uporabi informacijske in komunikacijske tehnologije spontano združujejo, da bi na trgu dosegli neko primerjalno prednost pred svojimi konkurenti (Bavec, 2002, str. 38). Svetovno najbolj znano virtualno podjetje je Amazon.com.

E-trženje je torej zgolj ena izmed funkcij, ki so se razvile z nastankom računalniške in internetne tehnologije. Med novejšimi »e-funkcijami« so tudi e-financiranje, e-nakupovanje (e-purchasing), e-izobraževanje, ipd.

5.3. Internet

Internet ni zgolj tehnologija, ki je prodrla v naša podjetja in domove, temveč je veliko več kot to. S pojavom klepetalnic, forumov in uvedbo interaktivnih iger je postal prostor za druženje. Za popestritev življenja ljudje ne potrebujejo več drugih ljudi, temveč se le vsedejo za svoj računalnik, priklopijo na mrežo in znajdejo se v novem svetu, obkroženi z novimi ljudmi, nenavadnimi idejami...

Internet je tudi trženjski medij, ki tržnikom ponuja obilico novih možnosti. Gre za enega najhitreje rastočih medijev, ki v sebi združuje tako sliko, zvok kot besedilo. Poleg tega pa tudi omogoča aktivno vključevanje potrošnika v sam proces prodaje. Če primerjamo internet z ostalimi mediji za množično komuniciranje, lahko opazimo, da ima internet daleč najhitrejšo rast dosega prebivalcev. Medtem ko je radio za doseg 50 mio ljudi potreboval kar 28 let, je TV dosegla enako število v 13 letih, internet pa je za tak doseg potreboval le 5 let.

Internet je omrežje, v katerega je povezano na tisoče računalnikov, ki se med seboj sporazumevajo s pomočjo TCP/IP protokola, ki zavzema tako protokol za nadzor prenosa kot tudi protokol za internet. Slednjega imenujejo tudi lepilo interneta, saj omogoča medsebojno komuniciranje računalnikov, ki so priključeni na internet. Podatki med računalniki potujejo preko različnih fizičnih nosilcev – od telefonske linije, satelitske ali radijske povezave do optičnega kabla ali žice lokalnega omrežja.

5.3.1. Zgodovina interneta

Začetki interneta segajo že v daljno leto 1960, ko je vlada ZDA začela vojaški projekt, imenovan ARPANET (Advanced Research Project Agency), ki je do leta 1973 potekal le v vojaške namene, po tem letu pa je kot raziskovalni projekt stekel tudi na ameriških univerzah. Po nastanku Bitneta (akademsko omrežje) je leta 1983 začel delovati internet, leto kasneje pa je ameriško obrambno ministrstvo le-tega prepustilo raziskovalcem, ki so do leta 1989 vzpostavili prvo komercialno omrežje Internet. Projekt ARPANET je prenehal delovati leta 1990, leto kasneje pa je ameriška vlada začela vlagati ogromne količine denarja v razvoj internetne "hrbtenice".

V letu 1991 je internet prišel tudi med "navadne" ljudi s pojavom www (World Wide Web). Istega leta je Anglež Tim Berner – Lee ustvaril HTML jezik (HyperText Markup Language) in internet, kot ga poznamo danes, je bil ustvarjen. Leto zatem sta bila ustanovljena Europanet (hrbtenica za evropska raziskovalna in akademska omrežja) in na slovenskem trgu tudi ARNES (akademsko omrežje).

Sledila so leta hitre rasti števila uporabnikov in nastanek novih načinov uporabe virtualnega spleta. Leta 1992 je Jean Polly uporabila izraz "surfanje na internetu", ki ga uporabljamo še danes. Začeli so se pojavljati iskalniki (yahoo.com, google.com...), sledilo je oglaševanje preko interneta, nakupovanje...

Leta 2000 je bil dostop do interneta že precej razširjen, pa vendar omogočen le 1/5 populaciji sveta. Danes do interneta dostopa že veliko več ljudi, pri čemer je največji delež uporabnikov v Severni Ameriki in Evropi.

5.3.2. Internet v Sloveniji

Tudi v Sloveniji je zabeležena konstantna rast dostopa do interneta. V poročilu Eurostat-a »Use of Internet among individuals and enterprises« lahko zasledimo, da v Sloveniji internet redno oz. vsaj 1-krat tedensko uporablja 40% populacije, od tega je rednih uporabnikov 43% moških in 39% žensk. Delež zaposlenih oseb, ki redno uporabljajo internet je 54%, kar je tik pod povprečjem za EU25, medtem ko je takih kar 75% študentov. Zanimiva je tudi ugotovitev, da kar 48% Slovencev še ni nikoli uporabilo interneta; za primerjavo naj povem, da je takih 43% prebivalcev EU25 in le 40% prebivalcev EU15. Tudi tukaj prihaja do razlik med spoloma, saj 50% Slovenk in le 45% Slovencev še ni nikoli uporabilo interneta. Delež zaposlenih ljudi, ki še niso uporabili interneta je 31%, kar je za 2% več kot v EU25 in kar za 5% več kot v EU15, medtem ko je študentov, ki še niso prišli v stik z internetom le 10%.

V letu 2005 je Statistični urad Republike Slovenije (SURS) izvedel obsežno raziskavo »Uporaba informacijsko-komunikacijske tehnologije (IKT) v podjetjih, Slovenija, 1. četrletje 2005«. Glede na to raziskavo naj bi v slovenskih podjetjih internet največ uporabljali za e-finančne storitve (87%), uporabo spletnih strani e-uprave (72%) in spremljanje razmer na trgu (70%). Slovenski trg je še vedno precej nezaupljiv do elektronskega poslovanja, saj je v letu 2004 le 27% podjetij z dostopom do interneta kupovalo preko interneta, še nižji pa je odstotek podjetij, ki so omogočala prodajo preko interneta, saj je takih le 9% podjetij z 10 ali več zaposlenimi. Glavne ovire za uvedbo e-prodaje naj bi bile varnostne težave glede plačil in tudi neprimernost blaga oz. storitve za e-prodajo. Kar 66% podjetij z dostopom do interneta ima svoje sisteme zaščitene s požarnim zidom, celo 99% jih ima poleg tega še zaščito s protivirusnimi programi. Kljub vsej tej zaščiti je kar 46% podjetij v letu 2004 naletelo na vsaj eno varnostno težavo (računalniški virus, nepooblaščen dostop do sistemov, spam...).

Glede na raziskavo "Special Eurobarometer 250 – Safer internet; May 2006" naj bi vsaj 1-krat mesečno internet v Sloveniji uporabljalo 50% ljudi.

5.3.3. Zasebnost na internetu

Pravica do zasebnosti je ena od najbolj osnovnih pravic v današnjem svetu, pa vendar je tudi ena izmed najbolj ogroženih. Glede na poročilo »Privacy and human rights« poznamo 4 vrste zasebnosti – informacijska zasebnost, zasebnost komunikacij, zasebnost telesa in prostorska zasebnost, pri čemer sta najbolj na udaru ravno prvi dve (Kovačič, 2003, str. 137). Večina držav priznava pravico do zasebnosti, prav tako kot tudi slovenska Ustava, ki v členih 35. do 38. opredeljuje varstvo pravic zasebnosti, kjer je med drugimi omenjeno tudi varstvo tajnosti pisem in drugih občil (sem spadajo tudi zvočne in digitalne komunikacije) ter varstvo osebnih podatkov.

Kazenski zakonik Republike Slovenije sankcionira posege v prostorsko zasebnost (149. in 152. člen), kamor bi lahko šteli tudi virtualni prostor (Kazenski zakonik Republike Slovenije, 2004). Zaenkrat je kazniv samo vdor pri gospodarskem poslovanju, vkolikor je pri tem povzročena premoženjska škoda oz. s strani storilca pridobljena premoženjska korist.

37. člen Ustave (Ustava Republike Slovenije, 2004) se nanaša na komunikacijsko zasebnost in s tem na tajnost pisem in drugih občil. Med ta občila lahko štejemo tudi telefonsko komunikacijo in elektronsko pošto, pri čemer je zasebnost varovana tako pri prenašanju sporočil preko javnih kot tudi zasebnih komunikacijskih sistemov (Šturm et al., 2002, 395).

Tudi informacijsko zasebnost pokrivata tako Ustava kot tudi Kazenski zakonik Republike Slovenije. 154. člen le-tega obravnava zlorabo osebnih podatkov s poudarkom na načinu pridobivanja osebnih podatkov, medtem ko 225. člen obravnava neupravičen vstop v zaščiteno bazo podatkov, kamor lahko štejemo tudi imenik e-naslovov (Kazenski zakonik Republike Slovenije, 2004).

Kljub zakonskim omejitvam pa nadzor nad dogajanjem na internetu vrši kar nekaj subjektov – od vlade, raznih podjetij, hekerjev in podobno. Obstajajo programi, vezani na spletne strani, ki zabeležijo iz katerega spletnega naslova je uporabnik prišel in tudi, katera je njegova naslednja “postaja”. Prav tako lahko ugotovijo, katero programsko opremo uporablja računalnik, kakšne so njegove nastavitve, ipd. Nekateri brskalniki samodejno pošiljajo spletnim stranem precej natančne podatke o okolju uporabnika, kar je označeno pod pojmom “klepetavost brskalnikov”.

Vsi ti podatki so zelo dobrodošli za podjetja pri raziskavah kupcev, saj lahko glede na njihove spletne “poti” ugotovijo marsikaj o njihovih interesih in željah ter kasneje ta podatek uporabijo za segmentiranje trga. Na drugi strani pa je to vdor v zasebnost potrošnika.

Tudi pri elektronski pošti je nadzor veliko večji, kot si mislimo. Elektronsko pošto je precej lahko prestreči, saj se le-ta po medmrežju prenaša nešifrirano. Upravitelji poštnih strežnikov imajo prost dostop do vseh sporočil, prav tako tudi upravitelji posredniških poštnih strežnikov.

Naj omenim, da 23. člen Zakona o slovenski obveščevalno-varnostni agenciji (2006) pravi, da »agencija lahko pod pogoji, določenimi s tem zakonom, izjemoma pridobiva podatke tudi s kontrolo pisem in drugih občil ter z nadzorovanjem in s snemanjem telekomunikacij«.

5.4. Elektronsko oz. e-trženje

Kotler opredeli e-trženje kot »obveščanje kupcev, komuniciranje, promocija in prodaja izdelkov in storitev preko interneta« (Kotler, 2006, str. G3). Rowley pa pravi, da e-trženje

predstavlja alternativno pot trženja oz. način približanja izdelkov in storitev kupcu, učenje v zvezi z željami in potrebami kupcev, vzpostavljanje stikov s kupci in komuniciranje z njimi ter prodajanje izdelkov in storitev (Rowley, 2001, str. 203).

Tabela 2: Delež posameznih oglasnih oblik od leta 1997 do 2004

	1997	1998	1999	2000	2001	2002	2003	2004
oglasne pasice	54%	56%	56%	48%	36%	29%	21%	19%
sponzorstva	41%	30%	27%	28%	26%	18%	10%	8%
mali oglasi (Classified)	/	/	/	7%	16%	15%	17%	18%
ključne besede			/	1%	4%	15%	35%	40%
vrinjene strani (Interstitial)	2%	5%	4%	4%	3%	5%	2%	/
oglaševanje prek e-pošte		1%	2%	3%	3%	4%	3%	1%
obogateni oglasi (Rich Media)	/	/	/	2%	2%	5%	8%	10%

Vir: Skrt, 2005.

Elektronsko tržno komuniciranje se deli na oglaševanje preko e-pošte in na oglaševanje na svetovnem spletu.

5.4.1. Trženje preko svetovnega spleta

Ker je svetovni splet zelo velik oglaševalski trg, kjer je na milijone in milijone različnih potencialnih kupcev, se je razvilo tudi več različnih oblik za dostopanje do njih.

- **Spletne pasice (bannerji)**

Gre za oglaševalsko sporočilo, ponavadi pravokotne oz. kvadratne oblike, na katerega lahko uporabnik klikne, s čimer aktivira povezavo do "domače" spletne strani oglaševanega izdelka/storitve. Pasice so najpogostejše nameščene na vrhu ali dnu spletne strani, pri čemer so lahko statične, animirane ali interaktivne.

- **Oglasni gumbki (buttons)**

So neke vrste manjše pasice, ravno tako pravokotne oz. kvadratne oblike, ki pa so za razliko od slednjih lahko nameščeni kjerkoli na www strani. Najpogostejše vodijo na strani s programsko opremo, ki jo lahko uporabnik brezplačno naloži na svoj računalnik.

- **Vmesni oglasi (pop-ups)**

Vmesni oglasi so najbolj moteča vrsta oglasov za uporabnike spleta, saj gre za oglase, ki se na ekranu pojavijo nenadoma in ponavadi zmotijo uporabnika pri delu oz. ogledovanju strani. Ti oglasi so različnih oblik in velikosti, prav tako pa so lahko statični ali animirani.

- **Sponzoriranje**

Gre za oglas, zraven katerega je ponavadi omenjeno, da gre za sponzorstvo, njegova funkcija pa je v večini primerov vzpostavljanje trdnejše povezave med izdelkom oz. blagovno znamko in vsebino spletne strani. Prav tako pa se ta možnost pojavlja na straneh iskalnikov, kjer podjetja uporabijo možnost sponzorstva zato, da se povezave na njihove spletne strani pojavijo na 1. mestu med zadetki iskanih strani.

5.4.2. Trženje preko elektronske oz. e-pošte

Zakon o elektronskih komunikacijah (2004) opredeli elektronsko pošto kot »vsako sporočilo v obliki besedila, glasu, zvoka ali slike, poslano po elektronskem komunikacijskem omrežju, ki se lahko shrani v tem omrežju ali v prejemnikovi terminalski opremi, dokler je prejemnik ne prevzame«. Elektronsko oz. e-sporočilo se po omrežju prenaša iz pošiljateljevega računalnika na prejemnikovega, vmes pa se lahko ustavi na strežniku.

Kadar elektronsko sporočilo vsebuje oglas za izdelek ali storitev, ga imenujemo oglasno elektronsko sporočilo. Na oglasna e-sporočila se lahko prejemnik naroči, kadar pa jih prejema nenaročeno, jih imenujemo nezaželena e-sporočila ali spam.

Poznamo naslednje vrste tržnega komuniciranja preko elektronske pošte (Central Iprom, 2006):

- **Sponzoriranje novic in liste razprav** preko elektronske pošte, pri čemer dosežemo točno določeno ciljno skupino, saj te razprave in novice ponavadi krožijo med ljudmi, ki imajo iste interese in razmišljanja;
- **Oglaševalsko podprta e-pošta** preko katere podjetja ponujajo brezplačne predale za elektronsko pošto (npr. Hotmail, Yahoo...), pri čemer jim v zameno lahko nemoteno pošiljajo svoje oglase, hkrati pa morajo za dostop do poštnega predala uporabniki preko "vhodne" strani, kjer ponudnik objavlja svoje in naročene oglase;
- **Sponzoriranje iger**, ki potekajo po elektronski pošti;
- **Neposredna e-pošta** s promocijskimi sporočili, ki prihaja neposredno v prejemnikov nabiralnik.

Duncan pa tržno komuniciranje preko e-pošte razdeli na sledeč način (Duncan, 2005, str. 396):

- **Oglasi**

Tako e-sporočilo je oblikovano kot golo besedilo (plain text) ali obogateno besedilo (rich media), ki podpira tudi avdio/video vložke, ki so prikazani v samem sporočilu in ne

priloženi kot priponka. Ta vrsta oglasnih sporočil je namenjena predvsem za privabljanje obiskovalcev na spletno stran. Ta način oglaševanja na spletno stran privabi veliko večje število ljudi, kot povezava preko oglasnih gumbkov oz. bannerjev.

- **Skupine razprav**

V določene razprave je vključenih na stotine ljudi, zato oglas na dnu sporočila lahko naenkrat pošljemo večjemu številu ljudi, pri čemer jih družijo isti oz. podobni interesi. Prejemniki lahko komunicirajo med seboj, zato lahko sporočilo z oglasom kroži dalj časa.

- **Obvestila oz. novice**

Na ta način podjetje posreduje novice o svojih izdelkih. Razlika med pošiljanjem novic in udeleževanjem v skupinah razprav je ta, da je v slednji omogočeno povratno komuniciranje, medtem ko gre tukaj le za obveščanje in prejemniki sporočil ne morejo komunicirati med seboj ali s pošiljateljem.

- **Publiciteta (publicity)**

Novice so poslane na vse naslove, ki bi lahko bili v povezavi s podjetjem ali poslovnim področjem, na katerem deluje podjetje.

6. E-pošta kot del e-trženja

E-pošta ima v primerjavi s klasičnimi poštnimi pošiljkami kar nekaj prednosti, zato se je njena uporaba v zadnjih letih tako razmahnila in izpodrinila sporočanje preko klasičnih pisem. Prva in najverjetneje največja prednost e-pošte je hitrost; sporočilo je dostavljeno v roku nekaj sekund, na drug konec sveta v roku nekaj minut, medtem ko standardna pisma za isto pot potrebujejo od enega dneva do večih tednov.

Prav tako gre za zelo ekonomičen način sporočanja informacij, tudi kadar moramo le-te prenesti večjemu številu ljudi. Potrebujemo le besedilo ali datoteko in naslove, medtem ko pri standardni pošti za vsako pismo potrebujemo še papir, kuverto in znamko, da ne omenim časa, ki ga porabimo pri tiskanju in kuvertiranju. Zelo uporabno je oblikovanje "mailing"list, na katerih so združeni uporabniki z istimi interesi, saj pri pošiljanju ni potrebno vnesti vsakega prejemnika posebej, temveč pošljemo sporočilo celotni skupini.

E-pošta ima visoko stopnjo zanesljivosti, saj v primeru neuspešne dostave (zaradi težav na strežniku ali napačnega naslova) dobimo obvestilo o tem v roku nekaj minut. Prav tako lahko takoj dobimo potrdilo, da je prejemnik prejel ali celo odprl pismo. Lahko zahtevamo tudi

neposreden odgovor in pri tem ne rabimo čakati, da poštar dostavi pismo in prejme odgovor ter ga potem pošlje nazaj nam, temveč je zopet govora o nekaj minutah.

Na povečano verodostojnost e-pošte vpliva tudi uporaba digitalnega podpisa, za katerega pravi Zakon o elektronskih komunikacijah, da je »Varen elektronski podpis, overjen s kvalificiranim potrdilom, glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu ter ima zato enako veljavnost in dokazno vrednost»(Zakon o elektronskih komunikacijah, 2004).

Prav gotovo je velika prednost e-pošte v pošiljanju dokumentov, ki obdržijo svojo kakovost oz. »tehnične« značilnost, kar omogoča prejemniku enostavno nadaljnjo uporabo.

6.1. Zgodovina nezaželenih e-sporočil

Izraz »spam« pravzaprav ne izhaja iz računalniškega sveta, temveč se je vse začelo s šunko oz. Letečim cirkusom Monty Pythona. V enem izmed skečev natakara neke restavracije streže gostom z raznovrstno hrano, pri čemer skoraj vse vsebujejo tudi šunko, zaradi česar natakara pri naštevanju oz. opisovanju jedi mnogokrat uporabi besedo spam (vrsta šunke). V nadaljevanju skeča besedo spam povzame še zborček, ki igra v ozadju, in na koncu se sliši le še spam, spam, spam...

Slika 1: Pločevinka SPAM šunke



Vir: Slo-Tech, 2005.

»Sending Persistent Annoying e-Mail« oz. vztrajno pošiljanje nadležnih e-sporočil je prevod, ki precej dobro opredeli nezaželena e-sporočila oz. spam (Smith, 2005, str. 137).

V računalniških oz. trženjskih vodah se je izraz spam prvič pojavil leta 1994, ko je nek ameriški programer po naročilu dveh odvetnikov sestavil oz. sprogramiral skripto, s pomočjo katere je poslal e-pošto na vse USE NET konference (skupine novic). Prvo masovno pošiljanje nezaželene elektronske pošte se je sicer začelo že veliko prej, okoli leta 1978, vendar je bila ta vrsta trženjske aktivnosti brez imena kar nekaj let.

Dejansko prvi trženjski napad s pomočjo e-pošte je izvedlo podjetje DEC, ki je oglas za svoj novi računalnik poslalo na vse tedaj znane elektronske naslove na ameriški zahodni obali. Če bi se vlada takrat zavedala, kakšna težava bo s takim početjem 20 let kasneje, bi to podjetje verjetno strožje kaznovala in postavila učinkovite ukrepe, da se to ne ponovi, tako pa je bilo omenjeno podjetje le lažje kaznovano zaradi kršitve pravil uporabe ARPA-NET-a (takrat je bil internet še vedno bolj domena akademskih in izobraževalnih institucij), ostala podjetja pa so bila opozorjena, naj takih akcij ne ponavljajo.

V 80-tih in 90-tih letih prejšnjega stoletja so po USE NET-u krožila razna standardna verižna pisma v stilu »Make money fast«, vendar pa te skupine novic še niso bile pripravljene na takšne napade. Zato je Richard Depew leta 1993 predlagal uvedbo t.i. moderiranih USE NET konferenc, pri katerih bi moderatorji preverili vsako sporočilo in ga v primeru neustreznosti zavrnili.

Januarja 1994 je po v vseh USE NET konferencah začel krožiti e-mail z naslovom »Global alert fo all: Jesus is coming soon«, par mesecev kasneje pa so ta sporočila prvič dobila tudi svoje ime: spam oz. nezaželena e-pošta.

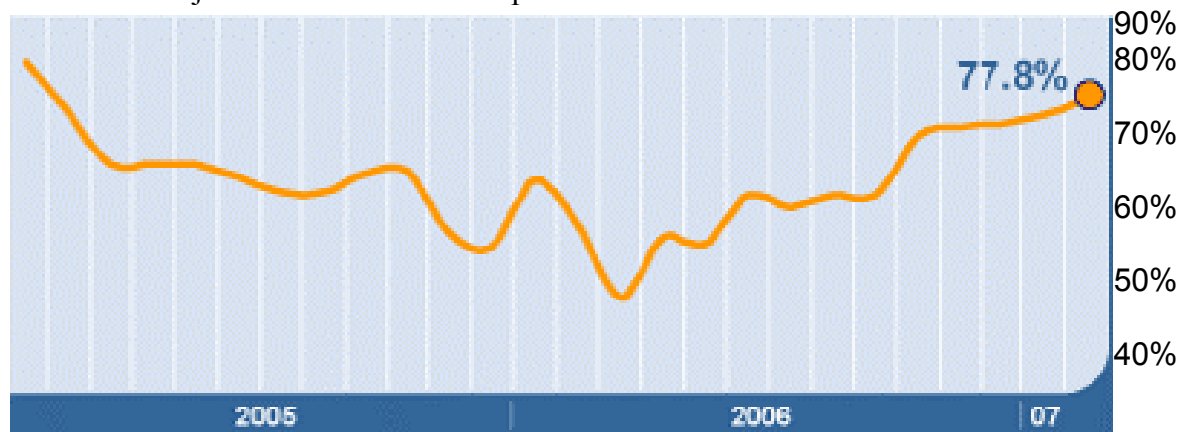
Z leti so USE NET konference izgubile na veljavi, saj so jih začeli izpodrivati razni forumi, zato so spamerji začeli pošiljati svoja sporočila neposredno na elektronske naslove. In od tu naprej so na udaru vsi, ki imajo elektronski naslov, in ne le tisti, ki sodelujejo v kateri od skupin novic.

6.2. Delež nezaželenih e-sporočil

Doma ali v službi naj bi nezaželena e-sporočila prejemale kar 56% vprašanih, ki uporabljajo e-pošto (Nezaželena e-pošta (spam), 2005). Glede na to raziskavo naj bi do 10 nezaželenih oglasnih sporočil dnevno na domači naslov prejemale 87% vprašanih, na službenega pa 76% vprašanih. 3% uporabnikov naj bi na službeni e-naslov prejemale več kot 50 spamov dnevno, medtem ko nad 50 nezaželenih e-sporočil dnevno na domači naslov prejme 1% vprašanih. Zaščito oz. programe za preprečevanje prejemanja nezaželenih e-sporočil naj bi glede na to raziskavo uporabljalo 32% vprašanih.

Podjetje MessageLabs redno raziskuje stanje na področju interneta in s tem tudi e-sporočil. Po nekajmesečnem padanju števila nezaželenih e-sporočil sredi leta 2006 se je začela nekaj mesečna rast števila nezaželenih e-sporočil. Aprila 2007 je bilo kar 77,8% vseh e-sporočil, poslanih preko interneta, nezaželenih e-sporočil.

Slika 2: Gibanje deleža nezaželenih e-sporočil



Vir: MessageLabs Intelligence, 2007.

6.3. Pridobivanje baze e-naslovov

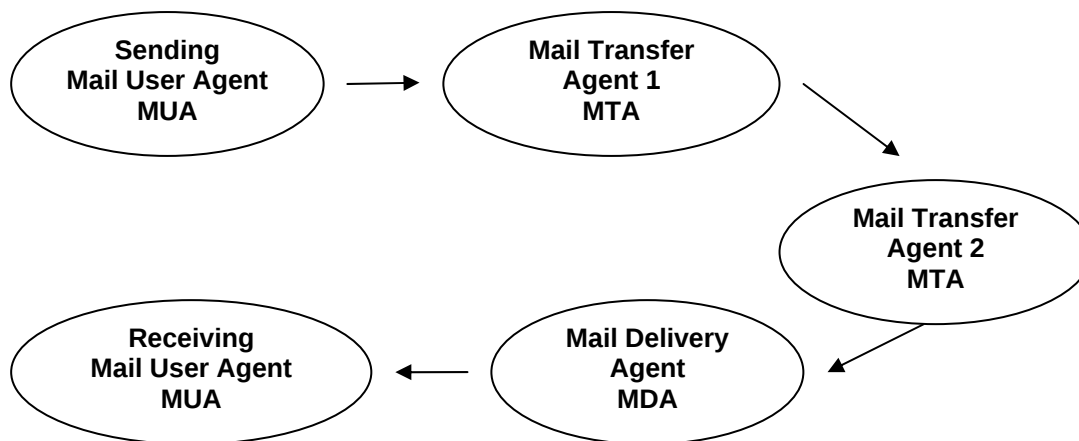
Pridobivanje e-naslovov je bilo včasih veliko lažje opravilo za vse pošiljatelje nadležnih masovnih sporočil. Vendar so se z razvojem raznih zaščitnih sistemov in načinov boja proti nezaželenim e-sporočilom razvijala tudi sama nezaželena e-sporočila. Spamerji oz. pošiljatelji nezaželene elektronske pošte morajo iz dneva v dan iskati nove načine, da lahko pridejo do e-naslovov in kar je še težje, da dejansko »dostavijo« e-sporočilo v poštni predal prejemnika. Zaenkrat so zelo uspešni pri tem in na vsak še tako učinkovit način zaščite najdejo protiudarec in spam je zopet v našem poštnem predalu.

Poglejmo si, kako e-pošta sploh potuje od pošiljatelja do prejemnika.

Prenos e-pošte vsebuje vsaj dva različna protokola, poljubno število strežnikov in programsko opremo tako na pošiljateljevi kot prejemnikovi strani. E-pošto v njeni vidni obliki ustvarimo na naši programski opremi (bodisi Microsoft Outlook, Netsape Messenger, itd.), kar imenujemo z Mail User Agent – MUA in je prvi igralec v igri prenašanja sporočila. Naslednji je Mail Transfer Agent - MTA, katerega naloga je preko drugih MTA-jev ali pa kar direktno prenesti sporočilo na strežnik, kjer ga bo prejemnik lahko prebral. Ta strežnik se imenuje Mail Delivery Agent – MDA. MTA in MDA sta lahko isti strežnik ali pa gre pri tem za dva različna strežnika. Vsi ti agenti delujejo s pomočjo protokolov, protokol za prenašanje sporočil pa se imenuje SMTP (Simple Mail Transfer Protocol). Prejemnik lahko ta sporočila prebere na več načinov: lahko se zgolj prijavi na strežnik in prebere vsebino svojega poštnega predala, lahko s pomočjo POP3 protokola (Post Office Protocol) »preloži« sporočila iz »virtualnega« poštnega predala na strežniku na svoj računalnik in jih tam prebere. Tretja možnost je protokol IMAP (Internet Message Access Protocol), ki prejemniku dovoli pregled in razvrstitev ter brisanje na samem strežniku, nato pa lahko, če želi, ta sporočila prenese na računalnik. Razlika med protokoloma POP3 in IMAP je torej v tem, da slednji ne zahteva predhodnega prenosa na računalnik, kot protokol POP3, temveč omogoča neposreden vpogled

na strežniku. Ta lastnost poveča tudi varnost sprejemanja sporočil, saj se marsikateri virus aktivira, ko je naložen na računalniku, v tem primeru pa ga zberemo preden pride do našega trdega diska.

Slika 3: Potovanje e-pošte od pošiljatelja do prejemnika



Vir: Baczewski, 2000, str. 7-9.

Iz razčlenjene poti (Slika 3) lahko vidimo, da imajo spamerji kar nekaj možnosti, kjer lahko dobijo podatke tako o vsebini kot tudi naslovih pošiljatelja in prejemnika. Kot že omenjeno pri poglavju o zasebnosti na internetu, imajo upravljalci strežnikov neoviran dostop do pošte, ki se prenaša preko njih. Oseba, ki vdre v sistem podatkov upravljalca strežnika, tako lahko pridobi ogromno število delujočih e-naslovov.

Lahka tarča za spamerje so t.i. spiski prejemnikov elektronske pošte, ki so se sami odločili, da bodo prejeli določena obvestila. Ti spiski prejemnikov pošte so že urejeni glede na določene lastnosti prejemnikov, kar lahko jemljemo kot uspešno segmentiran trg in spamer ne potrebuje veliko dela, da pošlje sporočilo točno določenemu segmentu prejemnikov. Lahko le izbere vse, ki so npr. prijavljeni na novice iz področja zavarovalništva in jim pošilja ponudbe na to temo.

Primerna zbirka e-naslovov, v kateri lahko spamerji z malo računalniškega znanja pridobijo večje število e-naslovov, so tudi USE NET skupine, tako imenovani forumi ali skupine novic. Tudi tu je trg že precej segmentiran, kar je zopet prednost za spamerje.

6.4. Zaščita in odgovor spamerjev

Vsaka bitka zahteva prilagajanje in izumljanje novih načinov, kako poraziti nasprotnika. Spamerji v vsaki oviri, ki bi jim preprečila dostavo nezaželenih e-sporočil, najdejo luknjo, zato izgleda, kot da informatiki bijejo bitko brez konca.

Začelo se je s preprostim »ignoriranjem«. Prejemnik je pošiljatelja ali del njegovega e-naslova dodal na svojo »ignore« ali »black« listo in sistem je avtomatično vrnil ali izbrisal naslednje sporočilo iz tega e-naslova. Spamerji so zato začeli ustvarjati nove e-naslove ali spreminjati obstoječe, da so se tako izognili filtru.

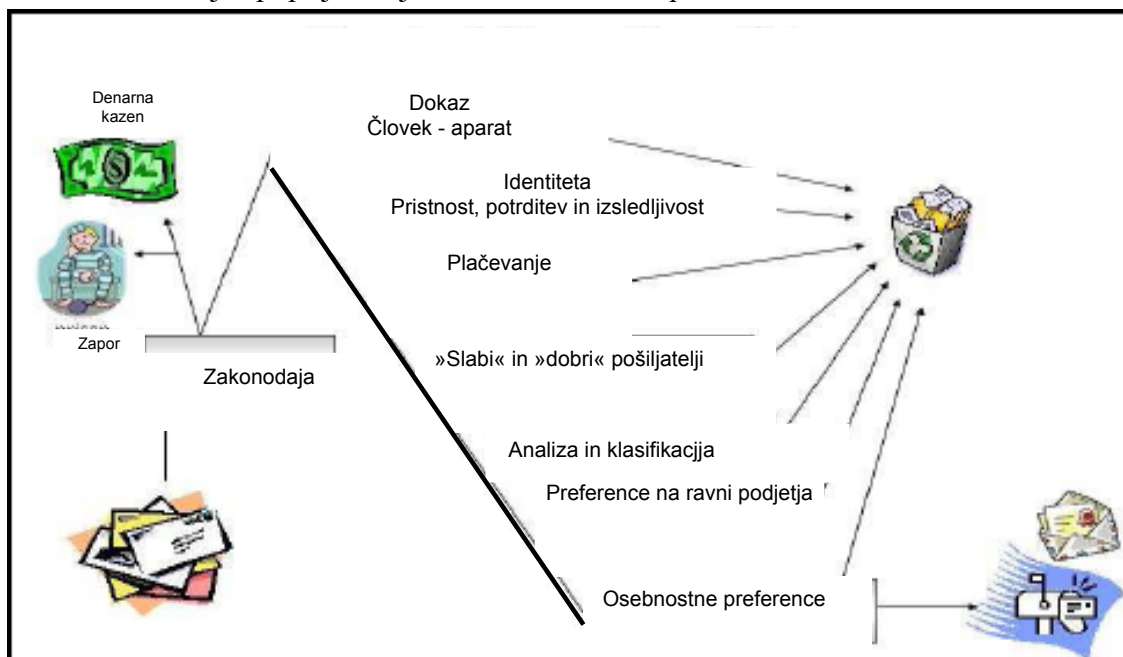
Nadaljevalo se je s preverjanjem naslovov (subject) teh sporočil. Program oz. filter je naslov (subject) sporočila primerjal s seznamom besed in fraz, ki so bili v močni povezavi s spam sporočili (npr. money, fast, sex, win...). Sporočilo, katerega naslov oz. del le-tega se je ujemal s seznamom, je bilo izbrisano. Osnovna težava tega filtra je, da je izbrisal tudi veliko sporočil, ki so imela v naslovu »kritične« fraze oz. besede, pa niso bili spam. Spamerji so našli rešitev: naslov so malenkost spremenili s krajšanjem besed, dodajanjem ločil, presledkov in podobno (m-a-k-e, m@ney, sxx...) in njihova e-sporočila so prišla čez filtre. Ko so bile tudi te besede in fraze dodane na »kritični« seznam, so spamerji spremenili vrstni red ali dodali nov znak (mon3y, fst...).

Obstajajo tudi filtri, ki sporočilo primerjajo s seznamom poznanih spamerjev in v primeru, da je pošiljatelj napisan tudi na seznamu, roma sporočilo v koš. Prav tako lahko ti filtri preverijo, kolikšnemu številu prejemnikov je bilo sporočilo poslano in v primeru velikega števila le-teh smatrajo sporočilo kot spam ter ga zbršejo. Nekateri filtri kot spam obravnavajo vsako sporočilo, ki pride iz brezplačnih e-naslovov (yahoo, hotmail...), zaradi česar je zmanjšana kredibilnost in funkcionalnost teh naslovov.

Obstajajo pa tudi oglasna e-sporočila, ki jih večina prejemnikov niti ne obravnava kot spam. Gre za šale, smešne in nenavadne kratke filmčke, prezentacije ipd., ki se v velikem številu prenašajo med uporabniki in vsebujejo prikrite oglase. Bodisi gre za sliko izdelka nekje v ozadju, oglas iz »tujine«, glasbo v ozadju, ki močno asociira na določeno blagovno znamko ali izdelek, itd...

Strokovnjaki iz podjetja SophosLab so odkrili, da se je razširilo pošiljanje oglasnih sporočil, ki vsebujejo subliminalna sporočila, kar so poimenovali kot »*pump-and-dump*« *stock spam campaign*. Ta oglasna sporočila vsebujejo animirane vložke, ki se za trenutek pojavijo na vsakih nekaj sekund. Ponavadi vsebujejo besedila oz. besede (buy!!!, free, ipd...), ki napeljujejo k nakupu, hkrati pa se na ta način sporočilo izogne spam filtru, ki bi prepoznal sporočilo kot spam in ga zavrnil, če bi se te besede pojavljale v osnovnem besedilu. Človeško oko sicer zazna »flash«, vendar ne prebere oz. prepozna sporočila, ki se skriva v ozadju, medtem ko sporočilo pride do naše podzvesti ter zaradi ponavljajočega pojavljanja vpliva na nakupno vedenje prejemnika. Sporočila so bila v večini primerov povezana z nakupom in prodajo delnic.

Slika 4: Področja spoprijemanja z nezaželenimi e-sporočili



Vir: Barry, 2000, str. 2.

Z analiziranjem in preprečevanjem škode, ki jo povzročajo spamerji, se ukvarjajo tudi malone vsa večja računalniška podjetja. Glede na članek podjetja IBM »A multifaced approach to spam reduction«, kjer opredelijo več nivojev bitke z nezaželeno elektronsko pošto, je govora o omejevanju nezaželene elektronske pošte in ne o eliminiranju, saj je le-to praktično nemogoče.

Vsak posameznik ima svojo predstavo o tem, kaj je in kaj ni spam, prav tako se med posamezniki tudi razlikuje meja tolerance pri sprejemanju oz. zavračanju takih sporočil. Dober sistem omejevanja nezaželene e-pošte bi torej moral vzeti v zakup tudi preference posameznika in mu dovoliti, da vpliva na delovanje sistema. Tu je govora predvsem o označevanju e-sporočila za spam, pa tudi pri nadaljnjem ukrepanju v zvezi z njim – ali se le-to takoj izbriše ali pa ima uporabnik možnost odločiti se, kaj bo naredil z njim. Večina podjetij ima vzpostavljen svoj sistem bojevanja z nezaželeno e-pošto, pri čemer posameznik nima vpliva na delovanje le-tega. Velika slabost takega sistema je seveda ta, da v koš roma marsikatero e-sporočilo, ki bi moralo priti do posameznika.

Analiziranje in kvalifikacija oz. filtriranje sporočil je eno najpomembnejših sestavin omejevanja dostopa nezeželeni e-pošti. Sistemi ponavadi preverijo naslov sporočila, pošiljatelja, samo vsebino ali zgradbo, največkrat pa kar vse skupaj. Prav tako lahko preučijo posamezno sporočilo kot celoto ali pa ga primerjajo z ostalimi sporočili. Velikokrat je v uporabi numerični sistem opredeljevanja »statusa« sporočila, pri čemer s pomočjo večih spremenljivk in ponderjev preučijo sporočilo ter se na podlagi doseženega števila točk odločijo o nadaljnjem postopku v zvezi z njim.

Seznami »dobrih«, večkrat tudi označenih kot »belih«, pošiljateljev in »slabih«, oz. »črnih« pošiljateljev so naslednja možnost v boju z nezaželenimi e-sporočili. Težava je, da tudi tu lahko napačna klasifikacija pošiljatelja povzroči veliko škode, saj je lahko onemogočeno sprejemanje pomembnih sporočil ne le iz enega naslova, temveč vseh naslovov iz ene domene. Naj tukaj omenim še t.i. »honeypot« e-naslove, katerih edina naloga je sprejemanje nezaželene e-pošte, ki se kasneje preuči, prav tako kot tudi pošiljatelj tega sporočila, in doda na že obstoječe sezname spamerjev.

Pošiljanje nezaželene e-pošte je tako razširjeno zato, ker je cenovno zelo ugodno in je potreben le majhen odziv, da se pokrijejo stroški, ki so nastali pri pošiljanju. Kot zanimivost naj omenim dejstvo, da zbiranje in urejanje baze terja več stroškov kot pošiljanje sporočil na tisoče naslovov. Pojavila se je težnja, da bi tudi pošiljanje e-sporočil bilo plačljivo, kar bi imelo velik vpliv na količino nezaželene e-pošte. Pojavi pa se vprašanje, komu bi se plačeval ta znesek poslanih sporočil. IBM je celo predlagal, da bi se ti zneski nakazovali dobrodelnim organizacijam, pri čemer bi vsak pošiljatelj po lastni presoji izbral organizacijo, kateri bi nakazal ta znesek. Vendar se seveda mnoga podjetja, ki masovno uporabljajo obveščanje preko e-pošte, borijo proti uvedbi te obveznosti.

Ena izmed največjih težav pri ravnanju z nezaželeno e-pošto je težko oz. včasih celo nemogoče natančno določanje pošiljatelja in po kakšni poti je sporočilo prišlo v naš e-poštni nabiralnik. Možnost, da bi lahko izsledili pravega pošiljatelja in natančno določili pot e-sporočila bi znatno izboljšala učinkovitost klasifikacije in s tem sistemov v boju z nezaželeno e-pošto. Sistem bi preveril pot in ozadje sporočila ter ob prikazu potrdil verodostojnost domene, jo ovrgel ali pa navedel, da podatek ni na voljo. Tako bi se lahko izognili zavajanju z napačnimi domenami. Naj tukaj omenim še eno orodje, s katerim lahko ugotovimo ali je sporočilo res prišlo iz »prave« domene – preprosta opcija odgovora oz. reply. Odgovor na sporočilo, ki nam kot pošiljatelja pokaže npr. »Citibank«, lahko vodi na naslov »citibank3741@collegeclub.com«, iz česar je jasno razvidno, da v ozadju ni podjetje Citibank, ki ima verjetno svojo lastno domeno in ne @collegeclub.com.

V zadnjem času so postali zelo popularni sistemi »izziv/odziv«. Sistem se uporabi za pošiljatelje, ki niso na našem seznamu »belih« pošiljateljev. Ob prejemu e-sporočila od takega pošiljatelja se avtomatično nazaj pošlje sporočilo z lahko nalogo (ponavadi je potrebno prepisati besedo, ki je napisana v vektorski obliki, da je avtomatski skenerji ne morejo prepoznati). Če sistem prejme pravilen odgovor, se sporočilo, ki nam ga je prvotno poslal pošiljatelj, dostavi v naš nabiralnik, v nasprotnem primeru ga označi za spam in zbriše. Ti izzivi so enostavni za človeka, medtem ko jih računalnik težko reši. Tak sistem zna povzročiti tudi nejevoljo pri pošiljatelju, kar lahko negativno vpliva na sodelovanje.

Kot orožje v spopadu z nezaželenimi e-sporočili pa IBM navaja zakonodajo; le-ta pa se sicer ne spopada s sporočili temveč s pošiljatelji.

Obstaja tudi mednarodni register spamerjev, imenovan »Rokso«² (Wells, 2006, str. 281) kjer so navedeni največji spamerji na svetu. Poleg seznama njihovih preteklih dejanj so zraven napisani tudi načini, ki jih posamezen spamerj uporablja in nasveti, kako se uspešno borovati proti njegovim nezaželenim e-sporočilom.

6.5. Struktura e-sporočila

Zaradi prevelikega števila prejetih e-sporočil se morajo spamerji pošteno potruditi, da naredijo tako sporočilo, da ta le-to pritegne potrošnikovo pozornost. Vse preveč e-sporočil roma neposredno v »koš«.

Kakor pri vseh oglasnih sporočilih je tudi tu potrebno upoštevati nekaj »standardnih« nasvetov. Naslov ima pri e-sporočilih verjetno še večjo pomembnost kot pri standardni pošti, saj pri kopici novih sporočil, ki pridejo v naš e-poštni nabiralnik naredimo prvo selekcijo že pri preletu naslovov oz. subjekta. Naslov »15% rast prodaje v tem četrtletju« bo verjetno pritegnil veliko več pogledov, kot npr. »Prodajna statistika«. Neprimerni oz. nezanimivi naslovi povzročijo, da potrošnik izbriše sporočilo, še preden ga sploh odpre in prebere. Naslovi morajo biti kratki in jedrnati, poleg tega naj bi bilo v njem čimbolj natančno opredeljeno, kateri interesni skupini je sporočilo namenjeno, npr. »Konferenca za prodajno osebje«, »Akcija za mlade«...

Dober naslov je torej prvi korak k uspešnemu oglasnemu e-sporočilu. Če potrošnik odpre sporočilo pomeni, da je le-to pritegnilo njegovo pozornost. Sedaj jo je potrebno še obdržati, kar naredi zanimiva vsebina in privlačna oblika. Stavki naj bodo kratki, poudarjene morajo biti glavne koristi ponujenega izdelka oz. storitve, vse skupaj je lahko podkrepljeno še s kakšno garancijo ali dokazom. Dobra besedila vsebujejo tako čustvene kot racionalne odgovore, pri čimer si le-ti sledijo po pomembnosti, od najpomembnejše do najmanj pomembne informacije.

Izbira pisave je naslednja pomembna točka. Ko je oglas natisnjen na papir, se njegova vsebina ne more več spreminjati in potrošnik vidi, kar mu pošljemo. Pri e-sporočilih ni vedno tako. Programska oprema prejemnika sporočil morda ne podpira pisave, s katero je napisano sporočilo, kar povzroči, da se določeni elementi (črke, znaki) spremenijo v kvadratke ali kakšne druge znake, s čimer je branje zelo otežkočano. Prav tako je težje branje besedil, v katerih so uporabljene samo velike črke, zato je priporočljiva uporaba malih in velikih črk. Tudi pri uporabi barv ni nujno, da bo potrošnik videl besedilo obarvano tako, kot ga vidi pošiljatelj. Kadar uporabnik poštnega predala do sporočil dostopa na strežniku, pri čemer si sporočil predhodno ne naloži na svoj računalnik, so le-ta velikokrat prikazana v črni barvi, ne glede na to, kakšen je original. Uporaba slik v e-sporočilih je lahko dvorezen meč. Dejstvo je, da slike lahko povečajo kredibilnost ali ponudijo še dodatne informacije, vendar pa so slike

² Register of Known Spam Operations.

ponavadi v visoko resolucijskih programih, ki zasedejo veliko prostora, zato niso primernejši element pri e-sporočilih. »Velika« sporočila pri prejemnikih povzročijo jezo, saj zmanjšajo hitrost prenosa podatkov in hitro zapolnijo poštni predal.

Enako kot s slikami je tudi s priponkami. V priponki lahko ponudimo še dodatne informacije, vendar velika priponka zopet lahko vodi v nezadovoljstvo prejemnika sporočila. Prednost priponke je tudi ta, da lahko vsebujejo datoteke v kateremkoli formatu, slabost pa, da so neuporabne, če tudi prejemnik nima nameščene programske opreme, ki omogoča upravljanje s tem formatom.

Na koncu sporočila naj bodo vedno kontaktni podatki o pošiljatelju in podjetju, na katerega se potrošnik lahko obrne. V elektronskem sporočilu je najlažje pripisati elektronski naslov strani, na kateri lahko potrošnik dobi še več informacij o ponujenem izdelku ali storitvi in morda celo opravi takojšen nakup.

Na koncu mora biti vedno ponujena možnost, da se prejemnik sporočila na enostaven način odjavi od prejemanja naših oglasnih e-sporočil. Najlažje je pripisati e-naslov, ki je ustvarjen z namenom sprejemanja odjav. Tako potrošnik enostavno klikne na ta naslov, pošlje sporočilo, hkrati pa se vsa ta »odjavna« sporočila sprejemajo in shranjujejo na enem samem mestu.

Pionirji trženja preko e-pošte navajajo naslednje napotke za povečanje uspešnosti trženja s pomočjo e-pošte (Kotler, 2006, str. 615):

- Ponudite potrošniku razlog, da se odzove na sporočilo.
- Naredite vaša sporočila osebna in potrošnikom posredujte le sporočila, ki sodijo v njihovo interesno območje.
- Ponudite informacije in možnosti, do katerih ne morejo dostopati po ostalih poteh.
- Olajšajte jim odjavo od prejemanja oglasnih sporočil.

6.6. Stroški in nezaželena e-sporočila

Stroški pošiljanja masovnih e-sporočil so za pošiljatelja resda nizki, vendar to ne pomeni, da so nizki tudi za prejemnika ali vmesne člene, ki poskrbijo za prenos e-pošte po medmrežju.

Stroški, ki nastanejo zaradi masovnih e-sporočil so zelo težko merljivi. Najlažje jih je preračunati s pomočjo časa, ki ga potrošnik porabi z branjem in/ali brisanjem teh sporočil. Na internetu lahko najdemo kopico pripomočkov, ki nam izračunajo stroške, ki jih nezaželena e-pošta povzroči v podjetju.

Tabela 3: Vpliv nezaželene elektronske pošte na različne subjekte

SUBJEKT V MEDMREŽJU	TEŽAVE, KI JIH POVZROČA SPAM
Prejemnik (stranka)	• Vtikanje v zasebnost posameznika. • E-sporočila velikokrat vsebujejo škodljive programske zapise, ki poškodujejo programsko opremo računalnika. • Obstaja možnost kraje »kritičnih« podatkov o uporabniku (razna gesla, številke kartic ipd.).
Prejemnik (zaposleni) in podjetje	• Porabljen delovni čas za branje in brisanje nezaželene elektronske pošte. • Dodatni stroški pri plačevanju internetne povezave, ki se zaračuna glede na porabljen čas. • Zmanjšana produktivnost.
Ponudniki dostopa do interneta (ISP)	• Stroški vzpostavitve anti-spam sistema. • Stroški dodatnega prostora na poštnih strežnikih zaradi zasedenosti poštnih predalov. • Slabša hitrost prenosa podatkov. • Večja možnost, da se bo sistem 'sesul' zaradi prevelikega števila sporočil. • Nezadovoljstvo uporabnikov.
Okolje e-poslovanja	• Negativen vpliv na zaupanje potrošnikov. • Pretirani zaslužki. • »Šušmarski« izdelki spoodkopavajo kredibilnost originalov. • Nelegalna uporaba programske in ostale digitalne opreme.
Država	• Etične kršitve. • Nezaželena oglasna sporočila so lahko žaljiva (pornografija) – kršitev zakonov.

Vir: Moustakos, 2004, str. 2.

Raziskava, ki jo je v mednarodnem okolju izvedla agencija Federal Trade Commission je pokazala, da kar 77% prejemnikov e-pošte dnevno porabi vsaj 10 minut za ukvarjanje (branje, brisanje) s temi sporočili. Raziskava, ki jo je na vzorcu 1000 odraslih oseb izvedlo podjetje Rockbridge Associates, Inc, skupaj s Smith School of Bussiness je pokazala, da je v ZDA zaradi nezaželene e-pošte tedensko izgubljenih kar 22,9 milijona delovnih ur. 78% odraslih dobiva nezaželeno e-pošto dnevno, pri čemer dobi vsaj 40 takih sporočil v enem dnevu. Le 14% prejemnikov nezaželene e-pošte je le-to tudi odprlo in pogledalo, za nakup oglaševanega izdelka pa se je glede na to raziskavo odločilo le 4 % prejemnikov.

Potrošnik naj bi za brisanje enega samega sporočila porabil 3 do 6 sekund. Če dnevno v poštni predal prejme le 10 nezaželenih e-sporočil, znese to od 0,5 do 1 minute. V tednu za brisanje porabi 2,5 do 5 minut, kar na letni ravni znese 2 do 4 ure. Če uporabimo podatek iz

raziskave Federal Trade Commission-a, da potrošnik porabi vsaj 10 minut dnevno z nezaželenimi e-sporočili, potem na letni ravni en sam potrošnik izgubi kar 43 ur zaradi tega. V podjetju z 10 zaposlenimi to znese 430 ur, kar je enako, kot če bi en zaposleni skoraj 3 mesece »gledal v zrak«.

Stroški nastanejo tudi z nakupom t.i. »anti-spam« opreme in z odpravljanjem posledic, ki jih povzročijo virusi, ki se prenašajo z e-pošto. Anti-spam programi so sicer zelo napredni, pa vendar so spamerji vedno bolj iznajdljivi, zato najdejo vedno nove in nove poti, da se izognejo barikadam in nezaželena e-sporočila dostavijo v poštne nabiralnike širom po medmrežju.

Težava nastane, kadar anti-spam program prepozna kot spam neko navadno sporočilo, ki lahko vsebuje pomembne podatke za naše poslovanje. Glede na to, da se v podjetjih nihče ne ukvarja z natančnim pregledovanjem sporočil, ki jih je zaščitni program označil kot spam, je težko izvedeti, kolikšen je ta del napačno opredeljenih sporočil in kolikšna škoda lahko nastane zaradi tega.

Podjetje Jupiter Research v svoji raziskavi predvideva, da bo zaradi anti-spam filtrov število nezaželene elektronske pošte upadalo za 13 % letno. S tem naj bi se povprečno število prejetih spamov na potrošnika znižalo iz 3.253 v letu 2005 na zgolj 1.640 v letu 2010.

BBC News je objavil članek, v katerem piše, da imajo lahko pošiljatelji nezeželenih e-sporočil velik vpliv tudi na cene delnic podjetij, pri čemer lahko pri tem pridejo do precejšnjega dobička. Pošiljatelj pošlje naokoli sporočilo z informacijami, ki napeljujejo k nakupu določenih delnic. Zaradi povečanega povpraševanja se cena tem delnicam zviša, vendar gre pri tem le za kratkoročen učinek. Pošiljatelju elektronskega sporočila, ki kupi delnice pred povečanjem cene in jih proda, ko se le-te zvišajo, to lahko prinese dobiček tudi do 6%, medtem ko ima oseba, ki se odzove na tako sporočilo lahko tudi 8% izgubo (Spammers manipulate stock market, 2006).

7. Zakonodaja in e-pošta

Približno 10 let nazaj je Ted Alspach³ zaprosil neko organizacijo, ki mu je po elektronski pošti masovno pošiljala oglasna e-sporočila, naj odstrani njegov e-naslov iz svojega seznama in dobil odgovor, da le-to na žalost ni možno. Čez nekaj časa, ko je Ted vsakodnevno tej organizaciji pošiljal več »prošenj« dnevno, so njegovo ime le odstranili iz seznama prejemnikov novic.

³ Avtor priročnika »E-pošta na internetu«.

Razmere naj bi bile danes drugačne, glede na to da je to področje tudi zakonodajno urejeno, vendar se še vedno najde veliko število kršiteljev in pa tudi tistih, ki najdejo luknje v zakonodaji in se spretno izognejo kazni.

Večina svetovnih zakonodaj glede pošiljanja elektronske pošte temelji na 2 načelih: »opt-in« in »opt out«. Pri »opt-out« načelu se mora potrošnik opredeliti, ali želi sprejemati oglasna sporočila preko e-pošte ali ne, zato mu podjetja oz. posamezniki lahko pošiljajo nezaželeno oglasno e-pošto vse dokler ne dobijo zahteve oz. izražene želje po prenehanju pošiljanja teh sporočil. »Opt-in« načelo pa ščiti potrošnika veliko bolj, saj mora potrošnik vnaprej privoliti v prejemanje ponudb ali oglasov s strani določenega podjetja. Večina podjetij, ki se ukvarja z »legalnim« pošiljanjem e-oglasov to področje ureja s pomočjo telemarketinga, s katerim od osebe dobi ustno privolitev za pošiljanje in pa velikokrat tudi aktualen elektronski naslov. Potrošniki se lahko tudi sami prijavijo za dobivanje oglasnih sporočil nekega podjetja preko spletnih strani ali »prijavnih« pisem.

Slovenska zakonodaja to področje pokriva z Zakonom o varstvu osebnih podatkov in Zakonom o varstvu potrošnikov.

45. a člen Zakona o varstvu potrošnikov (2006) navaja da »podjetje lahko uporablja sistem klicev brez posredovanja človeka, faksimile napravo in elektronsko pošto samo z vnaprejšnjim soglasjem posameznega potrošnika, ki mu je sporočilo namenjeno«, prav tako pa tudi »če potrošnik pri kateremkoli stiku, vzpostavljenim s sredstvom za komunikacijo, ki omogoča osebna sporočila, izjavi, da ne želi več prejemati sporočil na takšen način, mu podjetje ne sme več pošiljati nobenih sporočil, ki so namenjena sklenitvi pogodbe za dobavo kateregakoli blaga ali katerekoli storitve«.

77. člen tega zakona opredeljuje kazen za kršitev zgornjih dveh odstavkov 45. a člena kazen v višini najmanj 1.000.000,00 SIT za posameznika in najmanj 3.000.000,00 SIT za pravne osebe.

Zakon o varovanju osebnih podatkov (2005) se na večih mestih dotika področja nezaželene e-pošte. V prvem delu, ki obravnava obdelavo osebnih podatkov, je navedeno, da se le-to lahko izvaja le ob osebni privolitvi posameznika. Osebna privolitev je lahko dana v pisni, ustni ali kakšni drugi obliki. Za zavarovanje osebnih podatkov naj bi bilo poskrbljeno tudi s preprečevanjem nepooblaščenega dostopa do osebnih podatkov pri njihovem prenosu, kar naj bi veljalo tudi za prenos po telekomunikacijskih sredstvih in omrežjih. Na zahtevo posameznika, na katerega se osebni podatki nanašajo, mora upravljavec osebnih podatkov le-te zbrisati ali prenehati z njihovo obdelavo.

Cel VI. del tega zakona je posvečen neposrednemu trženju, kamor uvrščamo tudi nezaželeno e-pošto. 72. člen tega zakona obravnava pravice in dolžnosti upravljavca osebnih podatkov. Le-ta lahko uporablja oz. obdeluje določene osebne podatke, ki jih je dobil iz javno dostopnih

virov ali v okviru zakonitega opravljanja dolžnosti. Med osebnimi podatki, ki jih lahko obdeluje, je tudi naslov e-pošte posameznika; ob obdelavi je dolžan obvestiti posameznika, na katerega se osebni podatki nanašajo, na njegove pravice.

73. člen tega zakona pokriva pravice posameznika in pravi, da lahko posameznik na upravljalčeve stroške kadarkoli zahteva prenehanje obdelave osebnih podatkov, ki se nanašajo nanj.

Zagrožene so tudi kazni za kršitve določb tega zakona. Tako je za kršitev določb o obdelavi osebnih podatkov zagrožena kazen od 50.000,00 do 3.000.000,00 SIT, ki jo morajo plačati pravne oz. fizične osebe, odgovorne osebe in osebe, ki so kršitev dejansko izvedle. Prav tako je zagrožena kazen od 50.000,00 do 3.000.000,00 SIT za kršitev določb o zavarovanju osebnih podatkov, ki ravno tako zadeva vse 3 akterje – pravno oz. fizično osebo, odgovorno osebo in storilca dejanja. Za vse 3 osebe je zagrožena tudi kazen od 50.000,00 do 1.000.000,00 SIT za kršitev določb o neposrednem trženju.

Zakon o elektronskem poslovanju in elektronskem podpisu zaenkrat še ne obravnava nezaželene elektronske pošte.

Na oblikovanje slovenske zakonodaje imajo precejšen vpliv tudi direktive Evropske unije. Najpomembnejši za to področje sta:

- direktiva 2002/58/EC (E-privacy directive) s poudarkom na posredovanju osebnih podatkov in varstvu zasebnosti pri e-komunikacijah
- direktiva 2000/31/EC (E-commerce directive), ki pokriva pravne poglede na informacijsko tehnologijo, posebej elektronsko poslovanje

V primeru, da je podjetje obtoženo pošiljanja nezaželene e-pošte, mora dokazati, da je predhodno dobilo dovoljenje potrošnika za pošiljanje e-pošte na njegov naslov. To pomeni, da naj bi imela podjetja arhivirano kdaj in kako so dobila to soglasje. Preverjanje le-tega ni težavno v primeru pismenih dovoljenj, težava se pojavi pri dokazovanju dovoljenja, ki je bilo prejeto ustno, bodisi preko telefona ali osebno.

Kršitelje oz. pošiljatelje nadležne nezaželene e-pošte lahko potrošniki v Sloveniji prijavijo na Tržni inšpektorat Republike Slovenije, prav tako pa tudi ponudniku dostopa do interneta, preko katerega je pošta prišla. Naj omenim, da obstajajo tudi organizacije, ki se ukvarjajo z bojem proti nezaželenim e-sporočilom in spamerjem (npr. Spam recycling center, Spamcop, Mail Abuse Prevention System...), vendar je verjetno pot do njihove pomoči precej dolgotrajna, glede na to, da so to organizacije, ki delujejo na svetovni ravni in se morajo vsakodnevno ukvarjati z milijoni in milijoni nezaželenih e-sporočil.

Največjo oviro pri preganjanju in kaznovanju spamerjev bi lahko našli v načelu teritorialne pristojnosti v pravu. To načelo omejuje inšpektorje na kaznovanje pošiljateljev, ki prihajajo iz

območja Slovenije, ostali pa so pravno nedotakljivi. Vkolikor bi imele vse države urejeno področje kaznovanja pošiljateljev nezaželenih e-sporočil, to ne bi predstavljalo problema, saj bi vsaka država poskrbela za svoje kršitelje, žal pa večina teh sporočil prihaja ravno iz držav, ki imajo to področje zelo slabo urejeno.

Večina ponudnikov dostopa do interneta ne podpira pošiljanja masovnih oglasnih sporočil uporabnikom, kar je omenjeno tudi v pogodbi med ponudnikom in uporabnikom, vendar le-to pravzaprav nima velikega vpliva na kršitelje. Na podlagi prejete in upravičene pritožbe zaradi pošiljanja nezaželenih oglasnih sporočil sicer ponudnik dostopa lahko zaradi kršenja pogodbeno določenih obveznosti prekine spamerju dostop do interneta, kar pa gledano iz poslovnega vidika ni najprimernejša rešitev za poslovanje ponudnika. V marsikaterem primeru je spamer le prejel le obvestilo, oseba, ki ga je prijavila pa je bila obveščena, da so bili sprejeti ukrepi proti kršilcu in tu se zgodba konča.

8. Raziskava o odnosu slovenskih uporabnikov elektronske pošte do nezaželenih e-sporočil

8.1. Opredelitev namena in ciljev raziskave

Namen raziskave je dobiti vpogled v odnos, ki ga imajo slovenski potrošniki do nezaželenih e-sporočil. Glede na teoretično raziskavo okolja nezaželene e-pošte, ki je predstavljena v prvem delu diplomske naloge, je videti, da se sicer delajo raziskave glede deleža nezaželenih e-sporočil med celotno e-pošto, vendar pa ni nikjer opaziti raziskave, ki bi se usmerila na bolj kvalitativne lastnosti tega pojava. Prav to pa je bil namen moje raziskave in diplomske naloge.

Eno izmed najbolj osnovnih vprašanj, na katerega sem hotela dobiti odgovor je, kolikšen je sploh delež uporabnikov e-pošte, ki še niso prejeli nobenega nezaželenega e-sporočila. Glede na agresivnost, s katero pošiljatelji nezaželenih e-sporočil »napadajo« naše e-poštne nabiralnike, domnevam, da je delež uporabnikov e-pošte, ki se še niso srečali z nezaželenimi e-sporočili zelo majhen.

Nadalje me je zanimalo, ali večje število nezaželenih e-sporočil vpliva na to, ali se ljudje še »ubadajo« z njimi, torej ali si vzamejo čas, da jih preletijo, preberejo oz. se odzovejo ali jih takoj izbrišejo. Moja hipoteza je, da velja načelo obratne sorazmernosti – več nezaželenih e-sporočil prejmejo uporabniki, manj jih preberejo.

Zanimivo se mi je zdelo preučiti ali pošiljanje nezaželenih e-sporočil vpliva na ugled podjetja pri potrošniku in ali gre pri tem za negativen ali pozitiven vpliv. Glede na to, da so zaradi svojega obsega oglasna e-sporočila marsikdaj že avtomatično označena v posameznikovi percepciji kot spam, do katerega ima večina ljudi negativen odnos, domnevam, da to

posledično negativno vpliva na odnos uporabnika do podjetja, ki ta oglasna e-sporočila pošilja.

Kot opisano v prvem delu naloge, slovenska zakonodaja deloma že pokriva področje pošiljanja nezaželenih oglasnih e-sporočil, vendar me je zanimalo, ali se slovenski potrošniki tega sploh zavedajo in pa, če so se že kdaj obrnili na kak državni organ v zvezi s tem. Glede na slabo splošno seznanjenost Slovencev z zakonodajo menim, da je tudi poznavanje področij, ki pokrivajo nezaželeni e-sporočila, slabo ter, da se večina uporabnikov niti ne zaveda možnosti, da se lahko obrnejo tudi na zakonodajna telesa. Iz istega razloga tudi predpostavljam, da je le majhen delež ljudi, ki so se že obrnili na kak državni organ v zvezi s to problematiko.

Zanimalo me je tudi, ali obstaja razlika med odzivanjem na nezaželeni e-sporočila med mladimi in starejšimi potrošniki. Ker naj bi bili mladi ljudje bolj naklonjeni novotarijam in uporabi virtualnega sveta ter naj bi se v njem počutili »bolj domače«, domnevam, da so starejši uporabniki veliko bolj netolerantni do nezaželenih e-sporočil.

8.2. Metodologija

Do rezultatov oz. odgovorov na svoja vprašanja sem prišla s kvantitativno raziskavo. Uporabila sem anketo z neverjetnostnim oz. enostavnim slučajnim vzorčenjem.

Naslovnikom iz mojega elektronskega imenika sem poslala e-sporočilo s povezavo na strežnik, kjer je bila anketa, prav tako pa sem jih prosila, če lahko sporočilo posredujejo na čimveč naslovov. Anketa je bila na dostopna v začetku maja meseca, od 25.4. do 13.5.2006. Anketa je bila sprogramirana tako, da je vsaka oseba lahko izpolnila anketo le 1-krat, prav tako pa je anketiranec pri vsakem vprašanju lahko izbral le 1 odgovor. Tak način pridobivanja odgovorov sem uporabila, ker tako potuje tudi večina nezaželenih oglasnih e-sporočil.

Populacija v raziskavi so slovenski uporabniki e-pošte, vzorec pa je zajel 525 naključnih uporabnikov e-pošte.

Vprašalnik je bil sestavljen iz 46 vprašanj zaprtega tipa, pokrivala pa so več področij: razširjenost, količinsko opredelitev in vrsto nezaželene e-pošte, odnos posameznikov in sociodemografsko opredelitev anketirancev.

8.3. Struktura vzorca

Ker sem pri nekaterih svojih hipotezah primerjala odgovore med različnimi skupinami, sem na koncu vprašalnika dodala 5 socio-demografskih vprašanj.

8.3.1. Struktura vzorca glede na spol

Na vprašalnik je odgovorilo 332 moških (63,2%) in 180 žensk (34,3%). Glede na druge raziskave je tudi sicer večji delež moških kot ženskih uporabnikov interneta.

8.3.2. Struktura vzorca glede na starost

Daleč največji delež ima skupina anketirancev med 18 in 35 let. Glede na raziskavo Statističnega Urada RS to niti ni tako presenetljivo, saj naj bi bilo rednih uporabnikov interneta v starostni skupini od 16 do 34 let kar 81%. Glede na delež sta bili podobno zastopani še starostna skupina od 18 do 35 in od 36 do 60 let. Na vprašalnik sta odgovorili tudi 2 osebi, starejši od 60 let, kar predstavlja 0,4% vzorca.

Starostno strukturo sem primerjala s podatki Statističnega urada RS. Starostni okvirji se sicer razlikujejo, prav tako je opaziti odstopanja pri primerjavi podatkov za podobne skupine.

Tabela 4: Primerjava velikosti starostnih skupin

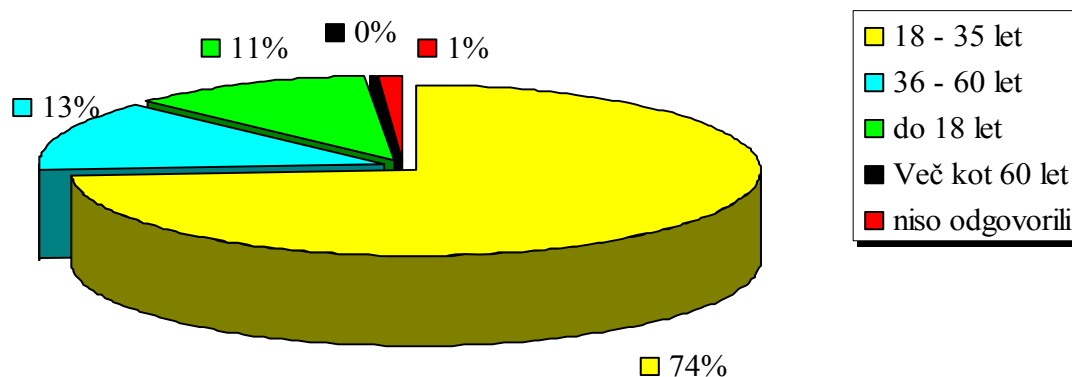
MOJA RAZISKAVA		
STAROST	% ODGOVOROV	KUM.
do 18 let	11,4%	11,4%
18 - 35 let	74,1%	85,5%
36 - 60 let	13,0%	98,5%
Več kot 60 let	0,4%	98,9%
Niso odgovorili	1,1%	100,0%

Vir: Lastna raziskava, 2006.

SURS					
STAROST	% UPORABNIKO V INTERNETA	ŠT. PREB.	ŠT. UPORABNIKOV INTERNETA	% MED VSEMI UPORABNIKI	KUM.
10 - 15 let	54%	102000	55080	5,9%	5,9%
16 - 34 let	81%	560000	453600	48,2%	54,1%
35 - 54 let	50%	750000	375000	39,8%	93,9%
55 - 74 let	14%	410000	57400	6,1%	100,0%

Vir: Prva statistična objava, 2005.

Slika 5: Starostna struktura anketirancev

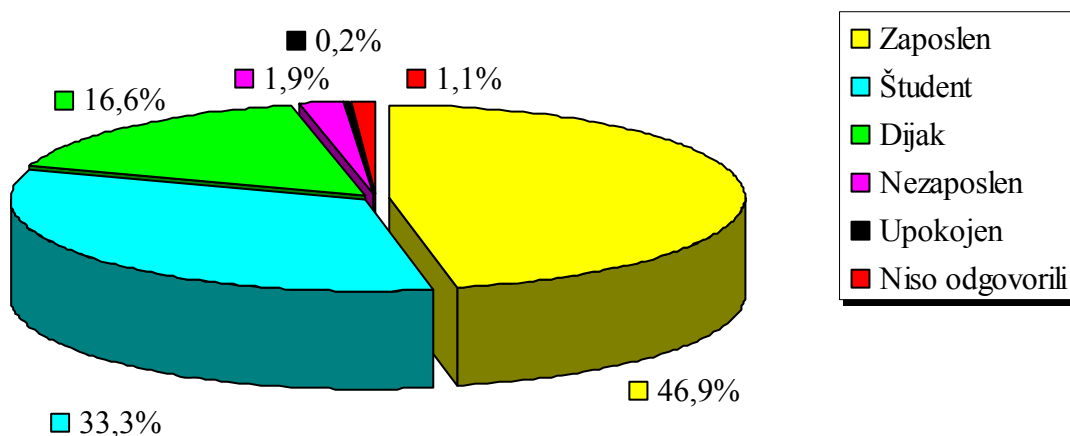


Vir: Lastna raziskava, 2006.

8.3.3. Struktura vzorca glede na status

Največji delež anketirancev je že zaposlenih, malo manj je študentov, skupaj pa predstavljata ti 2 skupini kar 80% vzorca.

Slika 6: Razdelitev vzorca glede na status

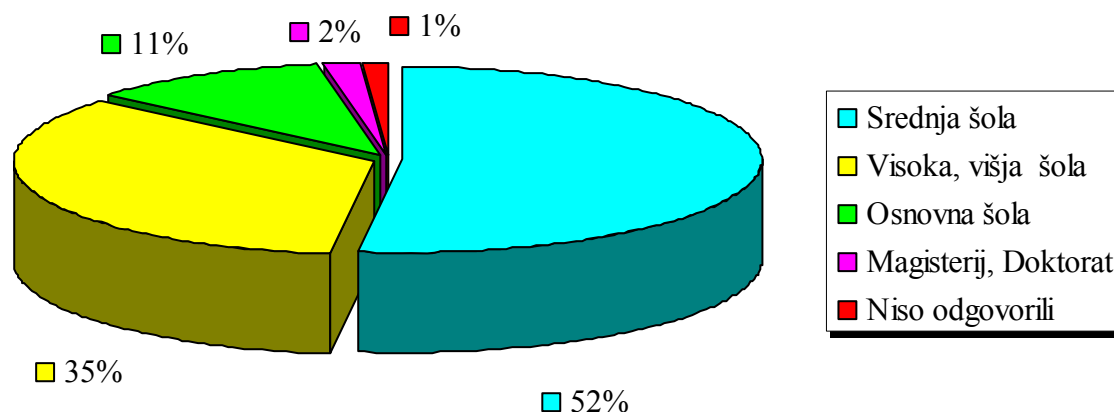


Vir: Lastna raziskava, 2006.

8.3.4. Struktura vzorca glede na izobrazbo

Največji delež anketirancev ima zaključeno srednjo šolo, kar je v povezavi z dejstvom, da je 33,3 % anketirancev študentov, ki šele končujejo višjo oz. visoko šolo, čisto razumljivo. Ravno tako dejstvo, da ima 11% anketirancev zaključeno le osnovno šolo, lahko povežemo s tem, da je 16,6% anketirancev dijakov, ki šele zaključujejo srednjo šolo.

Slika 7: Razdelitev anketirancev glede na izobrazbo



Vir: Lastna raziskava, 2006.

8.4. Nezaželena e-sporočila in slovenski uporabniki e-pošte

Moj osnovni cilj je bil preučiti odnos slovenskih uporabnikov e-pošte do nezaželenih e-sporočil. Preučevanja sem se lotila tako na količinski kot tudi vsebinski ravni.

8.4.1. Razširjenost nezaželenih e-sporočil

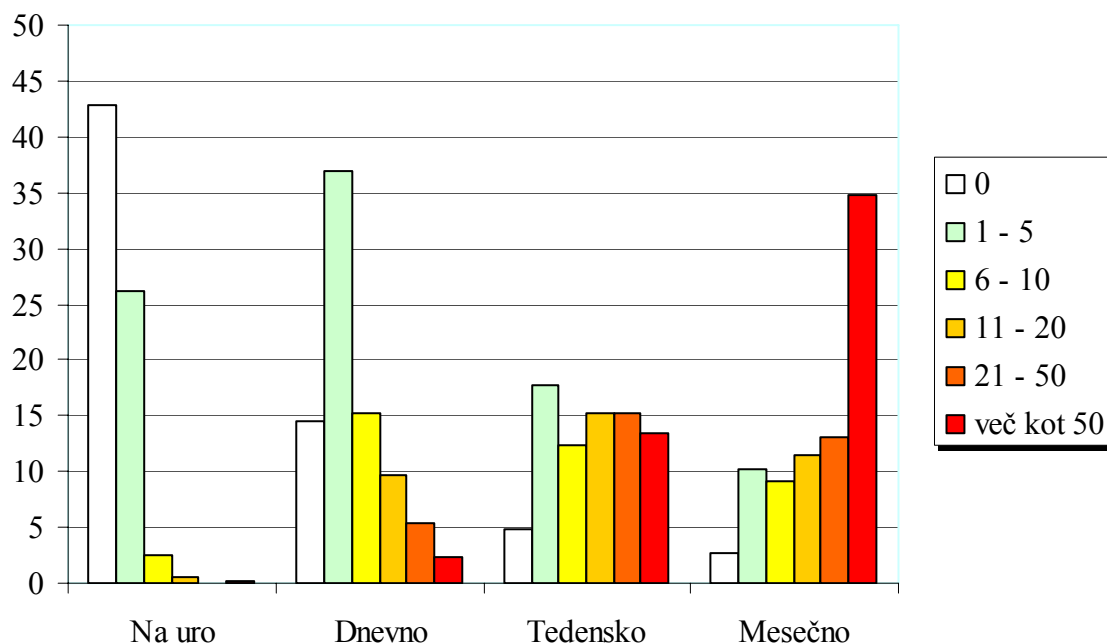
Na začetku raziskave me je zanimalo, koliko je sploh nezaželenih e-sporočil med slovenskimi uporabniki e-pošte. Vsaj 1 spam je v svoj e-poštni nabiralnik prejelo 516 anketirancev, kar zneso 98,3% vzorca. Raziskava torej potrjuje mojo hipotezo, da le majhen delež (1,7%) slovenskih uporabnikov elektronske pošte še ni prejelo nobenega nezaželenega e-sporočila.

Glede na ugotovitev, da kar 71,2% anketirancev uporablja anti-spam zaščito, lahko z veliko verjetnostjo predvidevamo, da so uporabniki e-pošte res že naveličani tovrstnih sporočil, ki najpogosteje vsebujejo oglasno vsebino.

Med uporabniki, ki so že kdaj prejeli spam je kar 77,5% anketirancev prejelo več kot 50 letih, le 9,3% prejemnikov pa je v svojem nabiralniku našlo manj kot 10 nezaželenih e-sporočil. Nekateri »težki« uporabniki e-pošte in s tem veliki prejemniki nezaželenih e-sporočil so se obregnili ob količinsko razdelitev, češ da prejmejo na stotine, nekateri celo tisoče nezaželenih e-sporočil, zato se jim je količina 50 zdela smešno nizka.

Zanimalo me je tudi, povprečno koliko prejmejo uporabniki nezaželenih e-sporočil v določenem časovnem obdobju, pri čemer sem časovno lestvico ločila na uro, dan, teden in mesec. Pričakovano se število prejetih nezaželenih e-sporočil spreminja premo sorazmerno z dolžino proučevanega obdobja.

Slika 8: Število prejetih nezaželenih e-sporočil v odvisnosti od časa



Vir: Lastna raziskava, 2006.

Mesečno ne prejme nobenega nezaželenega e-sporočila le 2,7% anketirancev, medtem ko je uporabnikov, ki dnevno ne prejmejo nobenega nezaželenega e-sporočila 14,6%. Zanimivo je dejstvo, da je le 1 (0,2%) anketiranec v povprečju prejel več kot 50 nezaželenih e-sporočil na uro, medtem ko je mesečno prejelo v povprečju več kot 50 nezaželenih e-sporočil kar 182 (34,7%) anketirancev.

8.4.2. Vsebina in izvor prejetih nezaželenih e-sporočil

Tako kot niso vsi načini tržnega komuniciranja primerni za vse izdelke, je tudi uporaba oglasnih e-sporočil namenjena le nekaterim vrstam izdelkov oz. storitev. Zanimalo me je, kateri so izdelki, ki se največkrat pojavijo kot oglaševan izdelek ali storitev. Slabih 60% anketirancev je izjavilo, da prejme precej ali ogromno nezaželenih e-sporočil s področja spolnosti, še nekaj odstotkov več anketirancev pa prejme precej ali ogromno nezaželenih oglasnih e-sporočil v povezavi z denarjem. Delež anketirancev, ki še nikoli niso prejeli nezaželenega oglasnega e-sporočila z izbranega področja je tudi najnižji pri teh dveh skupinah.

Slika 9: Koliko oglasnih e-sporočil, ki pokrivajo naslednja področja ste že prejeli

Vir: Lastna raziskava, 2006.

Ker me je zanimal izvor prejetih nezaželenih e-sporočil, sem postavila vprašanje tudi s tega področja. Očitno se slovenska podjetja še niso tako močno usmerila na izkoriščanje tega načina tržnega komuniciranja, saj je le 0,4% anketirancev odgovorilo, da so prejela nezaželeni e-sporočila le slovenskega izvora. Prevladujejo tuja nezaželena e-sporočila, kar je potrdilo kar 89,7% anketirancev, ki so izjavili da so ta sporočila večinoma (46,5%) ali čisto vsa (43,2%) tujega izvora.

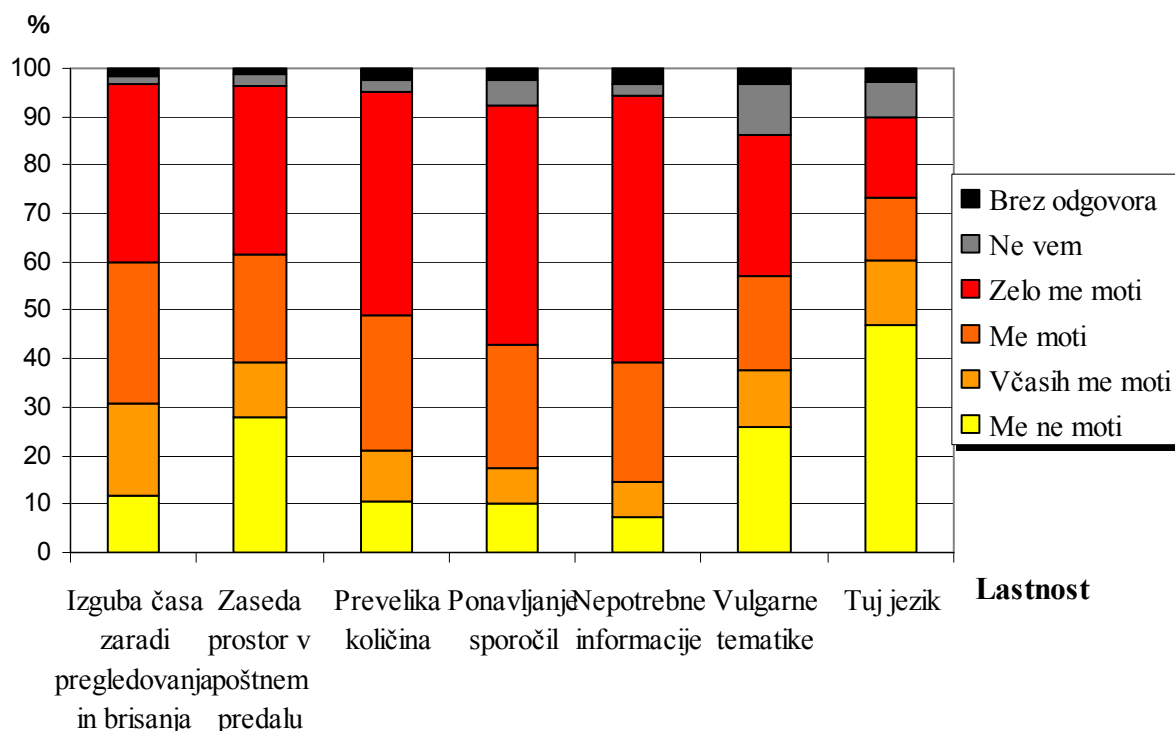
Vedno nova nezaželena e-sporočila prejema le 2,1% anketirancev, 2,3% pa jih prejema vedno ista. Glede na to, da prejemniki v večini primerov dobivajo tako nova kot že prejeta nezaželena e-sporočila lahko sklepamo, da pošiljatelji le-teh ubirajo več različnih poti za pošiljanje ali pa ponavljajo »izdajo« elektronskega oglasa.

8.4.3. Odnos potrošnikov do nezaželene elektronske pošte

Nezaželena e-sporočila motijo 87,4% anketirancev, pri čemer se število spreminja v odvisnosti od števila prejetih nezaželenih e-sporočil. Med anketiranci, ki so prejeli manj ali 10 nezaželenih e-sporočil, jih je 79,17% izjavilo, da jih le-ta motijo. Pri anketirancih, ki so prejeli že več kot 50 nezaželenih e-sporočil pa je ta delež predstavljal kar 90,23%. Večje število nezaželenih e-sporočil, ki jih potrošnik sprejme, torej negativno vpliva na dožemanje teh oglasov.

Nadalje me je zanimalo, kaj pri prejemanju nezaželenih e-sporočil najbolj moti prejemnike. Informativna narava elektronskega sporočila je tista lastnost, ki je najbolj na udaru. Nepotrebne in ponavljajoče se informacije ter prevelika količina le-teh so dejavniki, ki imajo največji vpliv pri negativnem dožemanju nezaželenih e-sporočil. Zanimivo je dejstvo, da skoraj polovice vprašanih (47%) ne moti, če je nezaželeno e-sporočilo napisano v tujem jeziku, prav tako pa ima ta lastnost med primerjanimi tudi najmanjši delež odgovorov »zelo me moti« (17%).

Slika 10: Odnos potrošnikov do posameznih lastnosti nezaželenih e-sporočil



Vir: Lastna raziskava, 2006.

Zanimalo me je tudi, ali imajo določeni dejavniki vpliv na to, ali potrošnik prebere e-sporočilo ali ne. Večina izmed naštetih dejavnikov (pravilno napisan naslov, določene teme, uporaba barv, lepo oblikovan tekst) ne vpliva na to, ali je e-sporočilo prebrano. Pri 32,6% anketirancev zanimiv naslov povzroči, da vedno ali vsaj včasih preberejo dobljeno nezaželeno e-sporočilo, medtem ko ta delež pri e-sporočilih, ki vsebujejo privlačne slike, znaša 25,1%.

Pod možnost »drugo« pri dejavnikih, ki vplivajo na to, ali prejemnik prebere prejeto nezaželeno e-sporočilo so anketiranci med drugimi omenili tudi teme iz področja zdravega življenja, športa, računalništva, internetnih igranic in avtomobilizma. Nekaj anketirancev pa prebere nezaželena e-sporočila zgolj za zabavo ali celo, da vidijo na kakšen način spamerji potrošnika »vlečejo za nos«.

Za spamerje je verjetno zelo nespodbudno dejstvo, da kar 65% anketirancev ne prebere nobenega prejetega nezaželenega e-sporočila, slaba 1/3 pa jih prebere le nekaj. Izmed 525 anketirancev sta le 2 osebi odgovorili, da prebereta vsa prejeta nezaželena e-sporočila. Med osebami, ki so izjavile, da jih nezaželena e-sporočila motijo je kar 97% anketirancev izjavilo, da ne prebere nobenega (66,7%) ali le malo (30,3%) le-teh. Na drugi strani pa je 15,9% anketirancev, ki jih nezaželena e-sporočila ne motijo, izjavilo, da preberejo vsaj polovico (5,3%), večino (8,8%) ali celo vsa (1,8%) prejeta nezaželena e-sporočila.

Kar 70,3% anketirancev zbriše prejeta nezaželena e-sporočila, brez da bi jih prej prebrali, 27,2% anketirancev pa le preleti ta sporočila in jih nato zbriše. 90,5 % anketirancev, ki jih nezaželena e-sporočila motijo, takoj izbriše le-ta, brez da bi jih prej prebrali. Natančno prebere (0,8%) ali se morda celo odzove z nakupom (0,4%) torej le majhen del prejemnikov nezaželenih e-sporočil.

Z nakupom so se na nezaželena oglasna e-sporočila že odzvali 3 anketiranci, kar znaša 0,6%.

8.4.4. Seznajenost z zakonodajo

Presenetljivo je dejstvo, da je dobra polovica (50,9%) anketirancev seznajena z dejstvom, da morajo imeti podjetja oz. pošiljatelji prejemnikovo dovoljenje za pošiljanje oglasnih e-sporočil. 11 anketirancev (2,1%) pa je celo že prijavilo podjetje oz. pošiljatelja zaradi nedovoljenega pošiljanja nezaželenih oglasnih e-sporočil. Moja hipoteza o slabem poznavanju slovenske zakonodaje, ki pokriva to področje, je torej napačna, prav tako pa je presenetljiv tudi delež ljudi, ki so se že poslužili uradnih organov pri boju proti nezaželeni e-pošti.

8.4.5. Vpliv pošiljanja nezaželenih e-sporočil na ugled podjetja

Podjetje, ki pošilja nezaželena e-sporočila izgubi ugled v očeh slabih 60% anketirancev, medtem ko dobra 1/3 ne spremeni mnenja o podjetju. 4 anketiranci (0,8%) so odgovorili, da jih tako podjetje pozitivno pritegne, eden izmed naštetih razlogov pa je tudi ta, da se tako podjetje očitno zelo trudi za povečanje svoje prodaje. Hipotezo o negativnem vplivu pošiljanja nezaželenih e-sporočil na ugled podjetja lahko torej potrdim.

8.4.6. Razlika v odzivu med starostnimi skupinami

Izmed 4-ih anketirancev, ki prejeta nezaželena e-sporočila natančno preberejo in šele nato zbrišejo, so kar 3 osebe iz starostne skupine od 18 do 35 let, kar predstavlja 0,8% anketirancev iz te starostne skupine. Skoraj 73% anketirancev iz te starostne skupine takoj izbriše nezaželena e-sporočila, brez da bi jih prej prebrali, medtem ko enako ravna 60,3% anketirancev iz starostne skupine 36 do 60 let ter oba anketiranca, ki sta stara več kot 60 let. Natančno prebere ali preleti ter šele nato izbriše nezaželena e-sporočila slabih 40% anketirancev v starostni skupini med 36 in 60 let, medtem ko je takih le dobrih 26% anketirancev iz starostne skupine 18 do 35 let. Na podlagi vzorčnih podatkov sem s chi-square testom ugotovila, da so razlike med spremenljivkama značilne ($P=0,000$), zato lahko trdim, da starost vpliva na sprejemanje in odzivanje na nezaželena e-sporočila.

Razlika je tudi v količini nežeženih e-sporočil, ki jih osebe iz določene starostne skupine preberejo. Kar dobrih 96% anketirancev iz starostne skupine od 18 do 35 let prebere malo (29,8%) oz. nobeno (66,6%) nezaželeno e-sporočilo, medtem ko je delež enakih oseb v starostni skupini med 36 in 60 let 92,7 (36,8% in 55,9%).

Razlika med sprejemanjem in odzivanjem na nezaželeno oglasna e-sporočila glede na starost anketiranca torej obstaja, vendar je obratna, kot sem predvidevala. »Mlajše« osebe preberejo manj nezaželenih e-sporočil, poleg tega pa jih tudi hitreje zbrišejo oz. so bolj brezkompromisne pri ravnanju z njimi.

8.4.7. Povzetek raziskave

Če povzamem vse ugotovitve iz raziskave, lahko rečem, da so nezaželeno e-sporočila, kamor velikokrat sodijo tudi oglasna e-sporočila, precej slabo sprejeta pri slovenskih uporabnikih e-pošte.

Pozitiven vpliv na dožemanje oglasnih e-sporočil pri prejemnikih e-pošte bi lahko imeli visoka stopnja personalizacije in natančna segmentacija potrošnikov. Z zelo podrobno segmentacijo bi poskrbeli, da bi prejemniki e-pošte prejeli manjše število oglasnih e-sporočil in še to le tista, ki bi se v precejšnji meri pokrivala z njihovimi interesnimi področji.

Vsak posameznik ima rad občutek, da lahko soodloča, zato bi morali na začetku pošiljanja oglasnih e-sporočil dati potrošniku možnost, da sami soustvarijo e-sporočila, ki bi jih želeli prejemati – tako vsebinsko (akcije, nasveti, novosti, dnevne spremembe, ipd.) kot tudi količinsko (1-krat tedensko, 1-krat mesečno, ipd.). Prav tako pa bi morali tudi kasneje potrošnika vpletati v ta sporočila – bodisi preko kratkih vprašanj (vprašanje ali dva) glede izbranih področij, odgovori katerih bi bili uporabljeni v naslednjih e-sporočilih, da bi imel potrošnik občutek, da je bil »slišan« ali pa bi kot v zahvalo za svoj odgovor prejel kak vzorec ali darilce. Če bi prejemniku e-sporočil lahko pokazali in dokazali, da imajo naša oglasna e-sporočila večjo dodano vrednost ter se razlikujejo od ostalih oglasnih e-sporočil, bi bil tudi potrošnikov odziv drugačen. Če bi vedel, da ga v vsakem našem e-sporočilu čaka nekaj novega, bi bila verjetnost, da bo sporočilo prebral veliko večja. Vendar je potrebno svojo drugačnost oz. svojo vrednost dokazovati že od prvega stika naprej.

9. Sklep

Široko razširjena nezaželena e-sporočila, največkrat z oglasno vsebino, oz. spam so na splošno zelo slabo sprejeta s strani uporabnikov e-pošte. Vkolikor bodo tržniki hoteli tudi v prihodnje uporabljati to orodje pri svojih trženjskih aktivnostih, bodo morali veliko delati na tem, da bodo oglasna e-sporočila zopet postala zanimiva in privlačna za uporabnike e-pošte. Tudi nizek odziv, ki je sicer potreben, da označimo trženje preko e-pošte za uspešno, bo oz. je vedno težje dosegljiv.

Oglasna e-sporočila imajo velik potencial za doseg dobrih trženjskih rezultatov, vendar so bila žal v preteklih letih uporabljena preveč nenačrtovano oz. »vsepovprek« in so zato izgubila na svoji vrednosti. Žal je ravno zato dandanes prava vrednost marsikaterega oglasnega e-sporočila prezrta. Izziv in pot v uspeh e-trženja je torej pokazati oz. dokazati uporabnikom e-pošte, da oglasno e-sporočilo ni le spam, temveč se v njem skriva veliko več.

LITERATURA

1. Alsapach Ted: E-pošta na internetu. Izola : DESK, d.o.o., 1996. 107 str.
2. Baczewski Philip: E-mail virus protection handbook. Rockland : Syngress Publishing, 2000. 476 str.
3. Bavec Cene: Urejenost podjetja – strukture in procesi, Dopolnilno študijsko gradivo za izredne študente. Koper : Visoka šola za management v Kopru, 2002. 48 str.
4. Coupey Eloise: Marketing and the internet. New Jersey : Prentice Hall, inc. 2001. 362 str.
5. Duncan Tom. Principles of Advertising & IMC. Second edition. New York : McGraww-Hill Companies, Inc., 2005. 774 str.
6. Flynn Nancy, Flynn Tom: Writing effective E-mail. London : Kogan Page limited, 2000. 82 str.
7. Huneycutt Jerry: Internet v uporabi. Izola : Desk, 1997. 338 str.
8. Jerman – Blažič Borka: Internet. Ljubljana : Novi forum, 1996. 87 str.
9. Kotler Philip: Marketing management. New Jersey : Prentice Hall, 2003. 706 str.
10. Kotler Philip: Principles of marketing. 7th edition. New Jersey : Prentice Hall, 1996. 712 str.
11. Kotler Philip: Principles of marketing. 11th edition. New Jersey : Prentice Hall, 2006. 651 str.
12. Kovačič Matej: Zasebnost na internetu. Ljubljana : Mirovni inštitut, 2003. 216 str.
13. Levinson Jay Conrad, Charles Rubin: Gverilski marketing na internetu. Popoln priročnik za služenje denarja v omrežju. Maribor : Rotis, 1996. 281 str.
14. Rowley James: Remodeling marketing communication in an Internet environment, Internet research. Journal of website promotion, Hawort, 3(2006), 11, str. 203-212.
15. Smith Paul, Chaffey Dave: Emarketing eXcellence: The heart of eBusiness. Burlington : Elsevier Butterworth-Heinemann, 2005. 372 str.
16. Smith Rob, Mark Thompson, Mark Speaker: The complete Idiot's guide to e-Commerce. Indianapolis : A division of Macmillan Computer Publishing, 2000. 364 str.
17. Starman Danijel: Tržno komuniciranje: izbrana poglavja. Ljubljana : Ekonomska fakulteta, 1996. 87 str.
18. Šturm, Lovro: Komentar ustave Republike Slovenije. Ljubljana : Fakulteta za podiplomske državne in evropske študije, 2002. 1247 str.
19. Wells William, Moriarty Sandra, Burnet John: 7th Edition Advertising principles and practice. New Jersey : Prentice Hall, inc, 2006. 592 str.

VIRI

1. American Marketing association. [URL: <http://www.marketingpower.com/>], 18.11.2005.
2. Androustopoulos, Evangelos. F. Magirou, Dimtrios Vassilakis: A game Theoretic Model of Spam E-Mailing. 8 str. [URL: <http://www.ceas.cc/papers-2005/113.pdf>], 11.01.2006.
3. Barry Leiba, Nathaniel Borenstein: A Multifaced approach to Spam reduction. 8 str. [URL: <http://www.research.ibm.com/spam/papers/multifaceted-approach.pdf>], Julij 2006.
4. BBC news [URL: <http://news.bbc.co.uk/2/hi/technology/5284618.stm>], 11.9.2006.
5. Capek Peter, Leiba Barry, Wegman Mark: Charity begins at...your Mail program. 8 str. [URL: <http://www.research.ibm.com/spam/papers/charity-seals.pdf>], 11.1.2006.
6. Central Iprom [URL: www.centraliprom.com], 25.8.2006.
7. Data protection working party 2004. [URL: <http://www.bfd.bund.de/Presse/pm20041115b.pdf>], 18.11.2005.
8. Dopolnilno študijsko gradivo za izredne študente »Urejenost podjetja – strukture in procesi«. [URL: <http://klemenr.si/ol.net/vsm/datoteke/urejeno-strukture/dodatno.pdf#search=%22virtualno%20podjetje%20definicija%22>], 22.8.2006.
9. Eurostat – Safer internet. 56 str. [URL: http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/eurobarometer_2005_25_ms.pdf], 22.8.2006.
10. Eurostat – use of internet among enterprises and households. str. 8 [URL: <http://www.ris.org/uploadi/editor/1144668164KS-NP-06-012-EN.pdf>], 22.8.2006.
11. Kazenski zakonik Republike Slovenije. (Uradni list RS št. 40/04 2004)
12. Jupiter Research. [URL: <http://www.jupiterresearch.com/bin/item.pl/research:service/1103/>], 11.9.2006.
13. MessageLab 2005 Annual Security report. [URL: http://www.messagelabs.com/publishedcontent/publish/threat_watch_dotcom_en/intelligence_report/2005_annual_security_report/DA_123230.chp.html], 6.9.2006.
14. MessageLabs Intelligence Report April 2007. 10 str. [URL: http://www.messagelabs.com/portal/server.pt/gateway/PTARGS_0_0_437_417_417_43/http%3B01200176CTC1%3B8080/publishedcontent/publish/threat_watch_dotcom_en/intelligence_reports/april_2007/message_labs_intelligence_report__april_2007_5.pdf], 15.4.2007.
15. Moj profit. [URL: www.profit-on.net/index.php?id=8&lang=sl&article_id=159], 11.9.2006.
16. Moustakos Evangelos, C. Ranganathan, Penny Doquenoy: Combating spam through legislation: A comparative analysis of US and European approaches. 8 str. [URL: <http://www.research.ibm.com/spam/papers/multifaceted-approach.pdf>], 11.1.2006.
17. Nasvet. [URL: <http://www.nasvet.com/>], 25.2.2007.
18. Nezaželena e-pošta (spam Delo IT). [URL: http://www.delo.si/index.php?fl=0&sv_path=43,50&id=416a02f95c4b2eadb52e1f0109adb95c04&source=Delo], 29.4.2005.

19. PCMG – Pospeševalni center za malo gospodarstvo. [URL: <http://www.pcmg.si/upload/other/SPP1-1trzenje.doc>], 25.8.2006.
20. Pošta Slovenije [URL: www.posta.si], 25.2.2007.
21. Privacy and Human rights 2004. [URL: [http://www.privacyinternational.org/index.shtml?cmd\[342\]\[\]=c-1-ivacy+and+Human+Rights&als\[theme\]=Privacy%20and%20Human%20Rights%202004&conds\[1\]\[category.....\]=Privacy%20and%20Human%20Rights](http://www.privacyinternational.org/index.shtml?cmd[342][]=c-1-ivacy+and+Human+Rights&als[theme]=Privacy%20and%20Human%20Rights%202004&conds[1][category.....]=Privacy%20and%20Human%20Rights)], 18.11.2005.
22. Prva statistična objava, št. 228. Ljubljana: Statistični urad Republike Slovenije, Oktober 2005, 2. str.
23. RIS 2002 – podjetja, internet in informacijske tehnologije. Ljubljana: CMI, april 2003, 107 str.
24. Setinšek Irena: Oglaševalsko leto 2006 v znamenju telekomunikacij, trgovcev in spletnega oglaševanja. MM marketing magazine, Januar 2007. 2 str.
25. Skrt Radoš: Desetletje spletnega oglaševanja. [URL: <http://www.nasvet.com/desetletje-spletnega-oglasovanja/>], oktober 2005.
26. Skrt Radoš: Vpliv interneta na trženjski splet podjetja (3. del: trženjsko komuniciranje). [URL: <http://www.nasvet.com/trzenjski-splet-3/>], januar 2001.
27. Slo-tech. [URL: <http://www.slo-tech.com/clanki/03040/03040.shtml>], 25.8.2006.
28. Spammers manipulate stock markets. [URL: <http://news.bbc.co.uk/2/hi/technology/5284618.stm>], 25.8.2006.
29. Spammers use subliminal messages in latest pump-and-dump scams. [URL: <http://www.sophos.com/pressoffice/news/articles/2006/09/subliminalspam.html>], 6.9.2006.
30. Tržno komuniciranje. [URL: <http://baza.svarog.org/ekonomija/trznokomuniciranje.php>], 25.2.7.
31. Ustava Republike Slovenije (Uradni list RS, št. 68/2006)
32. Zakon o elektronskih komunikacijah (Uradni list RS, št. 43/04)
33. Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 25/04)
34. Zakon o slovenski obveščevalno-varnostni agenciji (Uradni list RS, št. 61/2006)
35. Zakon o varstvu osebnih podatkov (Uradni list RS, št. 86/2004)
36. Zakon o varstvu potrošnikov (Uradni list RS, št. 98/2004)
37. Wikipedia. [URL: <http://sl.wikipedia.org>], september 2006.

Priloge

Priloga 1: Povzetek najpomembnejših členov Zakona o varstvu osebnih podatkov (ZVOP-1), v veljavi od 1.1.2005

**I. DEL
SPLOŠNE DOLOČBE**

...

5. člen

1. Osebni podatek - je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen.

2. Posameznik - je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se jo lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa.

3. Obdelava osebnih podatkov - pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana (sredstva obdelave).

4. Avtomatizirana obdelava - je obdelava osebnih podatkov s sredstvi informacijske tehnologije.

5. Zbirka osebnih podatkov - je vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi; strukturiran niz podatkov je niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika.

6. Upravljevec osebnih podatkov - je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki sama ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov oziroma oseba, določena z zakonom, ki določa tudi namene in sredstva obdelave.

...

14. Osebna privolitev posameznika - je prostovoljna izjava volje posameznika, da se lahko njegovi osebni podatki obdelujejo za določen namen, in je dana na podlagi informacij, ki mu jih mora zagotoviti upravljevec po tem zakonu; osebna privolitev posameznika je lahko pisna, ustna ali druga ustrezna privolitev posameznika.

15. Pisna privolitev posameznika - je podpisana privolitev posameznika, ki ima obliko listine, določila v pogodbi, določila v naročilu, priloge k vlogi ali drugo obliko v skladu z zakonom; podpis je tudi na podlagi zakona s podpisom izenačena oblika, podana s telekomunikacijskim sredstvom, ter na podlagi zakona s podpisom izenačena oblika, ki jo poda posameznik, ki ne zna ali ne more pisati.

16. Ustna ali druga ustrezna privolitev posameznika - je ustno ali s telekomunikacijskim ali drugim ustreznim sredstvom ali na drug ustrezen način dana privolitev, iz katere je mogoče nedvomno sklepati na posameznikovo privolitev.

...

23. Zasebni sektor - so pravne in fizične osebe, ki opravljajo dejavnost po zakonu, ki ureja gospodarske družbe ali gospodarske javne službe ali obrt, in osebe zasebnega prava; zasebni sektor so javni gospodarski zavodi, javna podjetja in gospodarske družbe, ne glede na delež oziroma vpliv države, samoupravne lokalne skupnosti ali samoupravne narodne skupnosti.

...

II. DEL - OBDELAVA OSEBNIH PODATKOV

1. poglavje - Pravne podlage in nameni

8. člen

(1) Osebni podatki se lahko obdelujejo le, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika.

(2) Namen obdelave osebnih podatkov mora biti določen v zakonu, v primeru obdelave na podlagi osebne privolitve posameznika pa mora biti posameznik predhodno pisno ali na drug ustrezen način seznanjen z namenom obdelave osebnih podatkov.

...

10. člen

(1) Osebni podatki v zasebnem sektorju se lahko obdelujejo, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika.

...

3. poglavje - Zavarovanje osebnih podatkov

24. člen

(1) Zavarovanje osebnih podatkov obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščen uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščen obdelava teh podatkov tako, da se:

...

3. preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih;

...

III. DEL - PRAVICE POSAMEZNIKA

Pravica do dopolnitve, popravka, blokiranja, izbrisa in ugovora

32. člen

(1) Upravljavalec osebnih podatkov mora na zahtevo posameznika, na katerega se nanašajo osebni podatki, dopolniti, popraviti, blokirati ali izbrisati osebne podatke, za katere posameznik dokaže, da so nepopolni, netočni ali neažurni ali da so bili zbrani ali obdelani v nasprotju z zakonom.

(3) Posameznik, katerega osebni podatki se obdelujejo v skladu s četrtem odstavkom 9. člena

ali tretjim odstavkom 10. člena tega zakona, ima kadarkoli z ugovorom pravico zahtevati prenehanje njihove obdelave. Upravljavec ugovoru ugotovi, če posameznik dokaže, da niso izpolnjeni pogoji za obdelavo po četrtem odstavku 9. člena oziroma po tretjem odstavku 10. člena tega zakona. V tem primeru se njegovih osebnih podatkov ne sme več obdelovati.

...

VI. DEL - PODROČNE UREDITVE

1. poglavje - Neposredno trženje

Pravice in dolžnosti upravljavca

72. člen

(1) Upravljavec osebnih podatkov lahko uporablja osebne podatke posameznikov, ki jih je zbral iz javno dostopnih virov ali v okviru zakonitega opravljanja dejavnosti, tudi za namene ponujanja blaga, storitev, zaposlitev ali začasnega opravljanja del z uporabo poštnih storitev, telefonskih klicev, elektronske pošte ali drugih telekomunikacijskih sredstev (v nadaljnjem besedilu: neposredno trženje) v skladu z določbami tega poglavja, če drug zakon ne določa drugače.

(2) Za namene neposrednega trženja lahko upravljavec osebnih podatkov uporablja le naslednje osebne podatke, ki jih je zbral v skladu s prejšnjim odstavkom: osebno ime, naslov stalnega ali začasnega prebivališča, telefonsko številko, naslov elektronske pošte ter številko telefaksa. Na podlagi osebne privolitve posameznika lahko upravljavec osebnih podatkov obdeluje tudi druge osebne podatke, občutljive osebne podatke pa le, če ima za to osebno privolitev posameznika, ki je izrecna in praviloma pisna.

(3) Upravljavec osebnih podatkov mora neposredno trženje izvajati tako, da posameznika ob izvajanju neposrednega trženja obvesti o njegovih pravicah iz 73. člena tega zakona.

(4) Če namerava upravljavec osebnih podatkov posredovati osebne podatke iz drugega odstavka tega člena drugim uporabnikom osebnih podatkov za namene neposrednega trženja ali pogodbenim obdelovalcem, je dolžan o tem obvestiti posameznika in pred posredovanjem osebnih podatkov pridobiti njegovo pisno privolitev. Obvestilo posamezniku o nameravanem posredovanju osebnih podatkov mora vsebovati informacijo, katere podatke namerava posredovati, komu in za kakšen namen. Stroške obvestila krije upravljavec osebnih podatkov.

Pravica posameznika

73. člen

(1) Posameznik lahko kadarkoli pisno ali na drug dogovorjen način zahteva, da upravljavec osebnih podatkov trajno ali začasno preneha uporabljati njegove osebne podatke za namen neposrednega trženja. Upravljavec osebnih podatkov je dolžan v 15 dneh ustrezno preprečiti uporabo osebnih podatkov za namen neposrednega trženja ter o tem v nadaljnjih petih dneh pisno ali na drug dogovorjen način obvestiti posameznika, ki je to zahteval.

(2) Stroške vseh dejanj upravljavca osebnih podatkov v zvezi z zahtevo iz prejšnjega odstavka krije upravljavec.

...

VII. DEL - KAZENSKÉ DOLOČBE

Splošne kršitve določb tega zakona

91. člen

(1) Z globo od 1.000.000 do 3.000.000 tolarjev se kaznuje za prekršek pravna oseba ali samostojni podjetnik posameznik:

1. če obdeluje osebne podatke, ne da bi imel za to podlago v zakonu ali v osebni privolitvi posameznika (8. člen)

...

14. če ravna v nasprotju z 32. členom ali če ravna v nasprotju z drugim ali petim odstavkom 33. člena;

(2) Z globo od 200.000 do 500.000 tolarjev se kaznuje za prekršek iz prejšnjega odstavka tudi odgovorna oseba pravne osebe ali samostojnega podjetnika posameznika.

(3) Z globo od 200.000 do 500.000 tolarjev se kaznuje za prekršek odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti, ki stori dejanje iz prvega odstavka tega člena.

(4) Z globo od 50.000 do 200.000 tolarjev se kaznuje za prekršek posameznik, ki stori dejanje iz prvega odstavka tega člena.

...

Kršitev določb o zavarovanju osebnih podatkov

93. člen

(1) Z globo od 1.000.000 do 3.000.000 tolarjev se kaznuje za prekršek pravna oseba ali samostojni podjetnik posameznik, če v skladu s tem zakonom obdeluje osebne podatke in ne zagotovi zavarovanja osebnih podatkov (24. in 25. člen).

(2) Z globo od 200.000 do 300.000 tolarjev se kaznuje za prekršek iz prejšnjega odstavka tudi odgovorna oseba pravne osebe ali samostojnega podjetnika posameznika.

(3) Z globo od 200.000 do 300.000 tolarjev se kaznuje za prekršek odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti, ki stori dejanje iz prvega odstavka tega člena.

(4) Z globo od 50.000 do 200.000 tolarjev se kaznuje za prekršek posameznik, ki stori dejanje iz prvega odstavka tega člena.

...

Kršitev določb o neposrednem trženju

94. člen

(1) Z globo od 500.000 do 1.000.000 tolarjev se kaznuje za prekršek pravna oseba ali samostojni podjetnik posameznik, če v skladu s tem zakonom obdeluje osebne podatke za namene neposrednega trženja in ne ravna v skladu z 72. ali 73. členom.

(2) Z globo od 100.000 do 300.000 tolarjev se kaznuje za prekršek iz prejšnjega odstavka tudi odgovorna oseba pravne osebe ali samostojnega podjetnika posameznika.

(3) Z globo od 50.000 do 200.000 tolarjev se kaznuje za prekršek posameznik, ki stori dejanje iz prvega odstavka tega člena.

Številka: 210-01/89-3/25

Ljubljana, dne 15. julija 2004

EPA 1228-III

**KAZENSKI ZAKONIK
URADNO PREČIŠČENO BESEDILO
(KZ-UPB1)**

...

Zloraba osebnih podatkov

154. člen

(1) Kdor v nasprotju z zakonom uporabi osebne podatke, ki se smejo voditi samo na podlagi zakona ali na podlagi osebne privolitve posameznika, na katerega se osebni podatki nanašajo, se kaznuje z denarno kaznijo ali z zaporom do enega leta.

(2) Enako se kaznuje, kdor vdre v računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobil kakšen osebni podatek.

(3) Če stori dejanje iz prvega ali drugega odstavka tega člena uradna oseba z zlorabo uradnega položaja ali uradnih pravic, se kaznuje z zaporom do dveh let.

...

Neupravičen vstop v informacijski sistem

225. člen

(1) Kdor neupravičeno vstopi v informacijski sistem ali kdor neupravičeno prestreže podatek ob nejavnem prenosu v ali iz informacijskega sistema, se kaznuje z denarno kaznijo.

(2) Kdor podatke v informacijskem sistemu neupravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem neupravičeno vnese kakšen podatek, ovira prenos podatkov ali delovanje informacijskega sistema, se kaznuje za zaporom do dveh let.

(3) Poskus dejanja iz prejšnjega odstavka je kazniv.

(4) Če je z dejanjem iz drugega odstavka tega člena povzročena velika škoda, se storilec kaznuje z zaporom od treh mesecev do petih let.

Številka: 713-01/89-3/61

Ljubljana, dne 17. junija 2004

EPA 1348-III

Priloga 3: Anketa

1. Ali ste že prejeli kakšen spam oz. nezaželeno e-sporočilo?

DA o NE

1.1 Ali uporabljate anti-spam zaščito?

DA o NE

2. Koliko nezaželenih e-sporočil ste že prejeli

- ☐ 1 – 10
☐ 11– 50
☐ Več kot 50

3. Povprečno koliko nezaželenih e-sporočil prejmete v določenem obdobju:

	0	1-5	6-10	11-20	21-50	Več kot 50
Na uro	☐	☐	☐	☐	☐	☐
Dnevno	☐	☐	☐	☐	☐	☐
Tedensko	☐	☐	☐	☐	☐	☐
Mesečno	☐	☐	☐	☐	☐	☐

4. Koliko sporočil (spamov), ki pokrivajo naslednja področja ste že prejeli:

	Nobenegaj	Malo	Precej	Ogromno
Spolnost	☐	☐	☐	☐
Denar	☐	☐	☐	☐
Turizem	☐	☐	☐	☐
Zdravstvo (hujšanje, lepotne operacije)	☐	☐	☐	☐
Kozmetični pripomočki	☐	☐	☐	☐
Drugo	☐	☐	☐	

5. Ali vas motijo ta nezaželena e-sporočila (spami)?

DA o NE o

6. Označite, kako močno vas motijo naslednje lastnosti teh sporočil (spamov)

	Me ne moti	Malo me moti	Me moti	Precej me moti	Zelo me moti
Izguba časa zaradi pregledovanja, brisanja	☐	☐	☐	☐	☐
Zaseda prostor v mojem poštnem predalu	☐	☐	☐	☐	☐
Prevelika količina	☐	☐	☐	☐	☐
Ponavljanje sporočil	☐	☐	☐	☐	☐
Nepotrebne informacije	☐	☐	☐	☐	☐
Vulgarne tematike	☐	☐	☐	☐	☐
Sporočila v tujih jezikih	☐	☐	☐	☐	☐

7. Kakšna so prejeta nezaželena e-sporočila?

- ☐ Vedno ista
- ☐ Večkrat ista
- ☐ Nova in ista
- ☐ Skoraj vedno nova
- ☐ Vedno nova

8. Kolikšen delež nezaželenih e-sporočil je slovenski?

- ☐ Ta sporočila so samo tuja
- ☐ Večinoma so tuja
- ☐ Približno enak delež je tujih in slovenskih
- ☐ Večinoma so slovenska
- ☐ Samo slovenska

9. Koliko nezaželenih e-sporočil dejansko preberete?

- ☐ Vsa
- ☐ Večino
- ☐ Približno polovico
- ☐ Malo
- ☐ Nobenega

10. Kateri od naslednjih dejavnikov vplivajo na to, ali preberete nezaželeno e-sporočilo:

	Da	Včasih	Ne
Zanimiv naslov	0	0	0
Pravilno napisan naslov (cele besede, brez npr., X, %, }, ¥...)	0	0	0
Tema:			
Spolnost	0	0	0
Denar	0	0	0
Turizem	0	0	0
Zdravstvo	0	0	0
Kozmetika	0	0	0
Drugo	0	0	0
Oblika			
Uporaba barv	0	0	0
Privlačne slike	0	0	0
Lepo napisan tekst	0	0	0

11. Ali ste na kakšno nezaželeno e-sporočilo že odgovorili?

DA 0 NE 0

12. Ali ste že kdaj naročili proizvod/storitev, ki je bila oglaševana v takem sporočilu?

DA 0 NE 0

13. Kaj naredite z prejetimi nezaželenimi e-sporočili?

- ☐ Takoj zbrišem, brez da bi prebral/a
- ☐ Preletim, nato zbrišem
- ☐ Natančno preberem in nato zbrišem
- ☐ Preberem in se nanj odzovem z nakupom

14. Ali veste, da je v Sloveniji zakonsko določeno, da morajo podjetja imeti vaše dovoljenje preden vam pošljejo oglasno e-sporočilo?

DA ☐ NE ☐

15. Ali ste že kdaj prijavili kakšnega pošiljatelja ali podjetje, ker vam je pošiljalo nezaželena oglasna e-sporočila?

DA ☐ NE ☐

16. Kako vpliva na vaše mnenje o določenem podjetju dejstvo, da vam le-to pošilja nezaželena oglasna e-sporočila?

- ☐ Podjetje me pozitivno pritegne
- ☐ Moje mnenje o pošiljatelju se ne spremeni
- ☐ Podjetje izgubi ugled v mojih očeh
- ☐ Drugo: _____

17. Vaš spol

moški ☐ ženski ☐

18. Starost

- ☐ Do 18 let
- ☐ 18 – 35 let
- ☐ 35-60 let
- ☐ Več kot 60

19. Status

- ☐ Dijak
- ☐ Študent
- ☐ Zaposlen
- ☐ Nezaposlen
- ☐ Upokojen

20. Izobrazba

- ☐ Osnovna šola
- ☐ Srednja šola
- ☐ Univerzitetna/višješolska diploma
- ☐ Magisterij, doktorat

Slovarček uporabljenih izrazov

- **Business-to-business (B2B)** – transakcija izdelkov ali storitev med dvema pravnima oz. poslovnima osebama
- **Business-to-customer (B2C)** – transakcija izdelkov ali storitev končnim kupcem
- **TCP/IP protokol** – množica protokolov, ki izvaja protokolski sklad, preko katerega teče internet
- **ARPANET** – napredno raziskovalno projektno agensko omrežje
- **WWW** – svetovni splet
- **HTML** – Hyper Text Markup Language – označevalni jezik za izdelavo spletnih strani
- **EU15** – 15 držav Evropske unije pred 1.majem 2004 (Avstrija, Belgija, Danska, Finska, Francija, Nemčija, Grčija, Irska, Italija, Luksemburg, Nizozemska, Portugalska, Španija, Švedska, Velika Britanija)
- **EU25** – 25 držav Evropske unije med 1.5.2004 in 1.1.2007 (Avstrija, Belgija, Danska, Finska, Francija, Nemčija, Grčija, Irska, Italija, Luksemburg, Nizozemska, Portugalska, Španija, Švedska, Velika Britanija, Slovenija, Madžarska, Češka, Slovaška, Poljska, Litva, Latvija, Estonija, Malta in Ciper (samo grški del))
- **USE-NET** – uporabniško omrežje; svetovna elektronska oglasna deska