Roskaposti

Sähköisen viestinnän kasvava uhka

Jarno Savinen

01.05.2004

Joensuun yliopisto
Tietojenkäsittelytiede
Pro gradu -tutkielma

Tiivistelmä

Roskapostista on muodostunut sähköpostin suurimpia uhkia. Valtavat roskapostimäärät rasittavat joustavaa, edullista ja luetettavaa sähköistä viestintävälinettä ja uhkaavat tehdä siitä käyttökelvottoman. Tutkielman tarkoitus on tutustuttaa lukija roskapostin ominaisuuksiin ja erilaisiin sisältöihin sekä selvittää erilaisia roskapostin torjuntamenetelmiä - teknisistä menetelmistä lakeihin ja hyviin käytäntöihin. Työssä käsitellään ongelmia, joita roskapostit aiheuttavat sähköpostin käyttäjille ja sähköpostipalveluiden ylläpitäjille. Tutkielmassa tarkastellaan roskapostittajien käyttämiä lähetystekniikoita sekä tapoja, joilla yritetään huijata roskapostintorjuntamenetelmiä. Tutkielmassa käydään lyhyesti läpi myös roskapostin historia ja sen suhde lakeihin Euroopassa ja Yhdysvalloissa.

Avainsanat: roskaposti

1. Johdanto

Roskapostista on muodostunut sähköpostin suurimpia uhkia. Roskaposti uhkaa tukkia sähköpostipalvelimet ja käyttäjien postilaatikot ei-toivotuilla mainoksilla, ketjukirjeillä sekä kaikkien tuntemilla, paljon rahaa tarjoavilla ”rikastu nopeasti ja vaivattomasti” -kirjeillä. Tällä hetkellä maailman kaikista sähköpostiviesteistä noin puolet on roskapostiksi luokiteltavaa materiaalia. (Brightmail 2004.)

Huolimatta siitä, että roskapostia lähetetään satoja miljoonia viestejä päivässä, ihmisten ja järjestöjen käsitykset roskapostista vaihtelevat. Tiukimmat määritelmät tuomitsevat roskapostiksi kaikki sellaiset viestit, joita emme ole pyytäneet tai hyväksyneet, kun toisten mielestä ainoastaan valheellinen ja haitallinen posti ansaitsee tulla nimetyksi roskapostiksi. Näiden kahden ääripään väliin mahtuu paljon erilaisia roskapostin määritelmiä. Seuraavassa tarkastelen muutaman roskapostia vastaan taistelevan tahon roskapostimääritelmiä.

MAPS (Mail Abuse Prevention System) (Mail-Abuse 2002) ja Spamhaus Project (Spamhaus 2004) määrittelevät roskapostin seuraavasti: Roskapostia on sähköpostiviesti, jonka sisältö ei ole riippuvainen henkilöstä, vaan on yhtä pätevä lähetettynä joukolle ihmisiä. Toisaalta myös viesti, jota vastaanottaja ei ole erikseen tai tarkoituksella pyytänyt, luetaan roskapostiksi, samoin viesti, jossa lähettäjä väittää antavansa vastaanottajalle suhteettoman suuren edun tai tarjouksen. CAUCE sen sijaan rajaa roskapostin klassisesti mainossähköpostiin, jota ei ole erikseen pyydetty (CAUCE 2003). Määritelmästä riippuen roskapostissa liikkuukin varsin erinäköistä postia: mainoksia ja huijauksia, virusten aiheuttamia posteja tai vaikkapa vitsejä tai hauskoja videopätkiä. Onko hauska ulkomaalaisviesti työkaverille vain vitsi ja päivän piriste vai loukkaava ja rasistinen työmoraalia laskeva roskaposti?

Roskapostin määrittelytapa vaihtelee henkilöstä toiseen, joten voisikin olla paikallaan nimittää kyseistä ilmiötä roskapostin *subjektiivisuudeksi*. Sama sähköpostiviesti voi olla toiselle hyvä tarjous tai haluttu ilmoitus, mutta toiselle pelkkää roskaa. Sanonta ”tiedän sen kun näen sen”, on kuin tehty roskapostille. Määritelmän suuresta vaihtelevuudesta huolimatta yleensä kaikki tuntevat termin roskaposti.

Roskapostivyöry aiheuttaa lukuisia ongelmia tukkien palvelimia ja kuluttaen kaistanleveyttä. Häiriöviesti voi huijata ihmisiä tai levittää viruksia tai muita inhottavia pikkuohjelmia. Roskaposti maksaa yrityksille huomattavia summia rahaa pelkästään menetettynä työaikana ja tehona. Roskaposti syö myös sähköpostin hyödyllisyyttä ja uskottavuutta. Mitä sähköpostin käyttäjät voivat oikein tehdä? Olemmeko me lopullisesti tuomittuja kahlaamaan roskapostimeressä ilman helpotusta, kunnes sähköpostijärjestelmä kaatuu omaan mahdottomuutensa roskalastin painon alla?

Roskapostia vastaan voidaan taistella monin eri tavoin sekä ohjelmallisesti että hyvien käytäntöjen avulla. Roskaposteja voidaan muun muassa suodattaa erittelemällä roskat kunnon postista. Näin tunnettujen roskaajien viestejä pyritään estämään, toisin sanoen vastaanotetaan viestejä vain ja ainoastaan sellaisilta ihmisiltä, jotka tunnemme ja joihin luotamme. Miten tämä inhottava roska sitten saapuu meille? Miten roskapostittajat saavat meidän osoitteemme ja miten he viestinsä lähettävät? Mitä temppuja roskaajat tekevät välttääkseen meidän hienot estotoimenpiteemme ja ohjelmistomme? Roskapostittajat ja roskapostin estäjät ovat haastaneet toisensa suoranaiseen roskapostisotaan. Tässä taistelussa molemmat puolet yrittävät kehittää parempia keinoja saavuttaakseen tavoitteensa. Roskapostin huima lisääntyminen ja sen aiheuttamat ongelmat ovat herättäneet myös lakien säätäjät. Roskapostilakeja valmistellaan valtameren molemmin puolin kovaa vauhtia. Lakien tehokkuudesta ja niiden roskapostimääritelmistä ollaan kuitenkin montaa mieltä.

Roskapostista on kirjoitettu vähän tieteellistä tekstiä eikä aiheesta löydy kirjallisuutta juuri ollenkaan. Roskapostia käsittelevät tieteelliset artikkelit keskittyvät johonkin tiettyyn roskapostin torjuntatekniikkaan tai esittelevät muutoksia jo olemassa oleviin tekniikoihin. Lähes kaikki roskapostista kirjoitettu ajankohtainen, mielenkiintoinen ja tähän kirjoitukseen sopiva tieto löytyy ainoastaan sähköisessä muodossa Internetistä. Nämä yritysten, järjestöjen ja tutkimuslaitosten tekemät tai teettämät tutkimukset ja raportit muodostavat tämän työn perustan. Monesti näissä raporteissa roskapostia käsitellään suppeasti eikä niissä pureuduta roskapostin määritelmän ongelmiin tai käsitellä roskapostin sisältöä. Silti ilman hyvää määritelmää ja ymmärrystä roskapostin sisällöstä sen tehokas torjuminen on vaikeaa, jopa mahdotonta.

2. Sähköposti

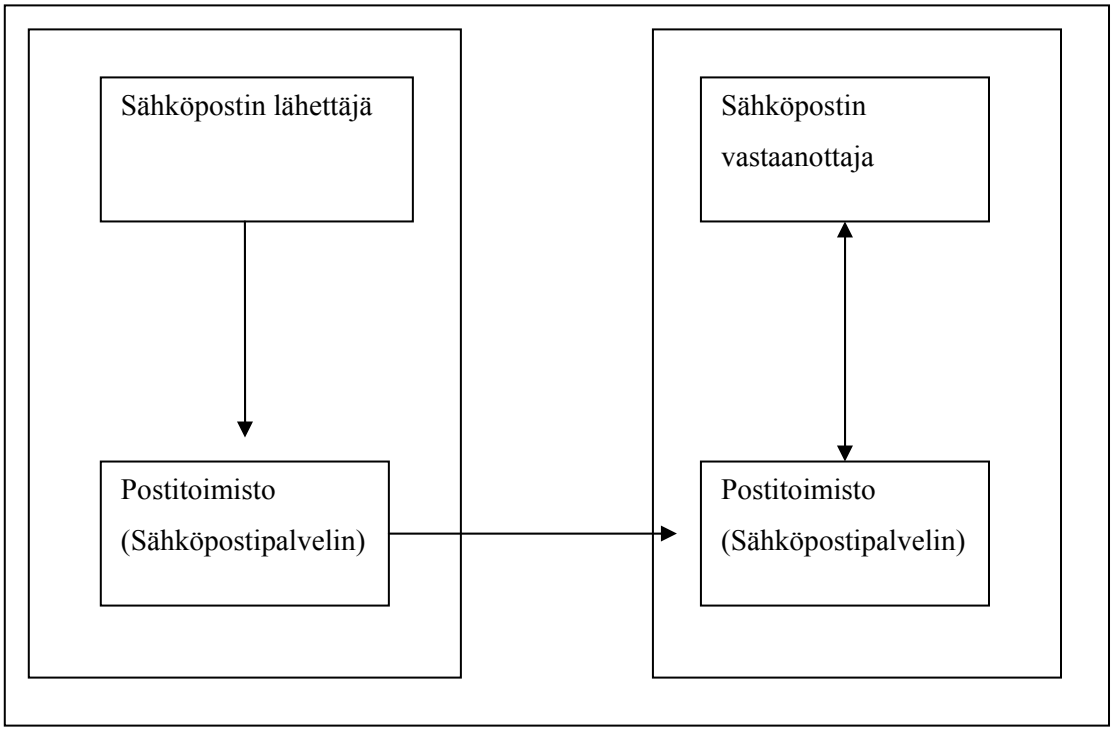
Sähköpostista on muodostunut aikamme tärkeimpiä keksintöjä. Se on halpa, nopea, helppo, monipuolinen sekä ajasta ja paikasta riippumaton viestintämuoto (Järvinen 2000), joka on muuttanut ihmisten käsitystä tiedon välityksestä. Sähköposti on välineenä yhtä vanha kuin Internet, mutta vasta viime vuosina se on noussut yhdeksi tärkeimmistä viestintävälineistämme. Sähköpostista puhutaan Internetin ”tappajasovellutuksena” eli Internetin eniten käytettynä osana (Fallows 2003; Pastore 2001). Sähköpostin nousu tähän asemaan johtuu tietokoneiden nopeutumisesta ja verkkoyhteyksien paranemisesta sekä tietokoneiden yleistymisestä yhteiskunnan eri alueilla. Paljon puhuttu digitaalinen televisio mahdollistaa ennen pitkää sähköpostin lukemisen ja kirjoittamisen suoraan television ruudulta. Parin seuraavan vuoden aikana langattomat ja taskussa kannettavat sähköpostilaitteet esimerkiksi matkapuhelimissa yleistyvät nopeasti ja sähköpostin käyttäjien määrä kasvaa entisestään. (Graham 2003a; 2003b; 2003c; Rice 2002.)

Koulut tarjoavat oppilailleen sähköpostiosoitteita ja kannustavat sähköpostin käyttöön alusta asti. Yliopistoissa ja korkeakouluissa sähköpostinkäyttö on ollut arkea jo monta vuotta. Myös yritysmaailma on ottanut sähköpostin tehokkaasti käyttöön (Fallows 2002; Pastore 2000). Sähköposti on korvannut normaalin postin ja telefaxit lähes kokonaan (Vault 2000). Vanhemmat ikäpolvet ovat myös alkaneet kiinnostua sähköpostista ja tietokonekurssit täyttyvät eläkeikäisistä ihmisistä (Nua 2003). Satelliittiyhteyksien aikana sähköposti on levinnyt hyvin laajoille alueille maapallolla aina Salomonsaarilta Nepalin vuoristoihin asti. Sähköpostia käytetään aktiivisesti jopa sellaisissa maailman kolkissa, joissa ei ole totuttu käyttämään puhelinta (Kupiainen 2002).

2.1. Sähköpostin toimintaperiaate

Seuraavaksi käyn lyhyesti läpi sähköpostin toimintaperiaatteet ja keskeistä sanastoa. Käsittelen myös sähköpostiin liittyviä Internetin perustoimintoja. Sähköposti on, niin kuin nimikin sanoo, sähköisten kirjeiden lähettämistä paikasta tai tietokoneesta toiseen. Sana ’sähköposti’ yhdistetään tavallisesti Internetiin, mutta sähköistä postia voidaan lähettää missä tahansa sähköisessä verkossa, jossa on tarvittavat osat ja ohjelmat. Osia ovat: *siirtotie*, *postitoimisto* eli *sähköpostipalvelin* ja *viestinvälitysagentti*. Neljäntenä osana voidaan pitää *käyttäjää* ja käyttäjän päätelaitetta sekä siinä pyörivää sähköpostiohjelmistoa (Järvinen 2000). Käyn myös läpi, miten postitoimistot ja välitysagentit keskustelevat keskenään sekä miten sähköpostin käyttäjät sopivat tähän järjestelmään. Kuvassa 1 on esitetty yksinkertaistettu malli sähköpostijärjestelmästä.

Kuva 1. Yksinkertaistettu sähköpostiviestin kulkureitti



2.1.1 Siirtotie

Siirtotie on se väline tai järjestelmä, jonka kautta sähköiset viestit kulkevat. Siirtotie yhdistää tietokoneet toisiinsa ja mahdollistaa viestien kulkemisen paikasta A paikkaan B. Suurin ja eniten käytetty siirtotie on Internet. Tästä syystä sähköpostia kutsutaan myös nimellä *Internetsähköposti*. Toisenlainen siirtotie voi olla esimerkiksi yritysten sisälle rakennettu sisäinen verkko, jossa kulkee vain ja ainoastaan yrityksen sisäinen viestiliikenne. (Järvinen 2000.)

2.1.2 SMTP

Internetissä viestien välittämiseen käytetään SMTP (Simple Mail Transfer Protocol) -nimistä protokollaa. Tämä protokolla antaa keinot sähköpostipalvelimien väliseen keskusteluun ja tiedon siirtoon tietokoneelta toiselle. STMP-yhteys on kaksisuuntainen ja alustariippumaton, ja se voidaan muodostaa suoraan palvelimelta palvelimelle tai käyttäen muita SMPT-palvelimia välityspalvelimina. SMTP-protokolla käyttää asymmetrista kysymys-vastaus -tyyppistä protokollaa, jossa lähetetyt viestit ovat ASCII-muotoisia eli helposti ihmisen ymmärrettävissä. Tästä syystä STMP-yhteyden voi luoda palvelimeen itse, ilman erillisiä SMTP-ohjelmia. Täytyy vain ottaa telnet-yhteys vastaanottajan koneen porttiin 25 ja kirjoittaa komennot suoraan komentoriville. (Karvinen, 1997; SMTP 2004.)

2.1.3 Postitoimisto

Postitoimisto tai sähköpostipalvelin on tietokone, joka on yhdistetty viestien välitykseen käytettyyn siirtotiehen. Postitoimisto huolehtii viestien vastaanottamisesta ja varastoinnista. Saavuttuaan perille viesti talletetaan sen vastaanottajan postilaatikkoon. Postitoimistossa voi olla jopa miljoonien käyttäjien henkilökohtaiset postilaatikot. Jokaisessa postilaatikossa on oma yksilöllinen osoite, sähköpostiosoite. Osoite kertoo postitoimiston nimen ja sijainnin organisaatio-osassa, sekä henkilön postilaatikon nimen. Sähköpostiosoite on muotoa *henkilöosa@organisaatio-osa*. (Järvinen 2000.)

2.1.4 Postilaatikko

Postilaatikko on jokaisen käyttäjän oma nurkka sähköpostipalvelimella, jonne saapuneet viestit tallennetaan. Normaalissa tilanteessa käyttäjä ottaa yhteyden postipalvelimeen omalta

koneeltaan tai vaikka kännykältään ja pyytää saada viestit omasta postilaatikostaan. Tämä tapahtuu käyttämällä yhtä monista sähköpostiprotokollista.

Kaksi eniten käytettyä protokollaa ovat POP (Post Office Protocol) ja IMAP (Internet Mail Access Protocol). POP:in ja IMAP:in suurin ero on niiden tapa käsitellä sähköpostiviestejä. POP, joka tunnetaan sen uusimman version mukaan POP3:na, siirtää viestit sähköpostipalvelimelta käyttäjän koneelle tuhoten ne samalla palvelimelta. IMAP-protokolla kopioi postit käyttäjän koneelle, mutta jättää viestit myös palvelimelle. IMAP mahdollistaa myös useiden kansioiden käytön sähköpostipalvelimella. Näiden protokollien avulla sähköpostit siirtyvät palvelinpäästä eli sähköpostipalvelimelta käyttäjän omaan päätelaitteeseen. Sähköpostiviestit voidaan jättää talteen sähköpostipalvelimelle tai ne voidaan poistaa samalla kun siirto omalle koneelle tapahtuu. (Järvinen 2000.)

2.1.5 Viestinvälitysagentti

Viestinvälitysagentti (mail daemon) on ohjelma, joka saattaa sähköpostiviestin turvallisesti ja nopeasti siirtotietä hyväksikäyttäen haluttuun postitoimistoon. Välitysagenttiohjelma sijaitsee yleensä samalla koneella tai ainakin samassa järjestelmässä kuin postitoimisto. Tämä ei kuitenkaan ole välttämätöntä, ja viestejä voidaan lähettää mistä tahansa ja millä tahansa välitysagentilla, johon vain saadaan yhteys. Välitysagentti voi sijaita myös käyttäjän omalla koneella. Välitysagentit keskustelevat SMTP-protokollaa käyttäen sen postipalvelimen kanssa, jonne haluttu viesti lähetetään. (Järvinen 2000; Schwartz & Garfinkel 1999.)

2.1.6 DNS

Internetin sähköpostijärjestelmässä on olemassa DNS-palvelu (Domain Name Service), jonka tarkoitus on sitoa Internetin ip-osoitteet sähköpostipalvelimien nimiin. Tämä on eräänlainen puhelinluettelo, jossa puhelinnumeroiden ja nimien sijasta listataan ip-osoitteita sekä palvelinnimiä. (Saarni, 1998.)

2.1.7 MX

Läheisesti DNS-palveluun sitoutuvat MX-tietueet (*Mail eXchanger)*. MX-tietueet sijaitsevat sähköpostipalvelimella ja niiden tarkoitus on ohjata sinne tulevat sähköpostit jonnekin muualle. Tietueita voi olla useampia. Niitä käydään läpi tietyssä järjestyksessä, kunnes löytyy

palvelin, joka suostuu ottamaan siirretyn postin vastaan. Esimerkiksi palvelin A:ssa on kaksi MX-tietuetta, jotka ohjaavat postit palvelimille B ja C. Kun palvelin X lähettää sähköpostin palvelimelle A, ohjautuvat postit tilanteesta riippuen joko B tai C -palvelimelle. (Saarni 1998.)

2.2. Sähköpostiviestin rakenne

Sähköpostiviestissä on kaksi pääosaa: *otsikko* (header) ja varsinainen *viestin tekstiosa* (body). Otsikko-osassa sijaitsevat erilaiset otsikkotiedot, jotka kertovat mistä viesti on tulossa ja mihin se on menossa. Tämä osio on tarkoitettu pääasiassa sähköpostiohjelmien luettavaksi. Viestiosassa sijaitsee varsinainen sähköpostiviesti. Koska SMTP-postin kautta ei voida lähettää kuin ASCII-muotoista tekstiä, on sähköpostiviestiin usein lisätty myös MIME-osa. Tämä osio mahdollistaa esimerkiksi erikoismerkkien, kuten ä:n ja ö:n käytön, liitetiedostojen lähettämisen ja HTML-muotoiset sähköpostiviestit. (Schwartz & Garfinkel 1999.)

2.2.1 Tekstiosa ja Otsikko-osa

Tekstiosassa sijaitsee sähköpostiviestin varsinainen sisältö eli teksti. Otsikko-osa käsittää sähköpostin välittämiseen tarpeelliset tiedot. Otsikko-osan rakenne on yleensä aina samanlainen, ja siellä sijaitsevat seuraavat tiedot: from, reply-to, date, to, cc, bcc, message-id, subject, received ja X-kentät. Taulukossa 1 on esitetty tarkempi selite otsikko-osan kentille.

Taulukko 1. Otsikko-osan eri kentät

From	Kertoo viestin lähettäjän sähköpostiosoitteen.
Reply-to	Vaihtoehtoinen vastausosoite, jos viestin lähettäjä haluaa että viestiin vastataan eri osoitteeseen kuin siihen mistä se on lähetetty.
Date	Päivämäärä ja kellonaika, jolloin viesti on lähetty.
To	Osoite tai osoitteet, joihin sähköpostiviesti on lähetetty.
Cc	Toissijaiset sähköpostin lähetysosoitteet joihin lähetetään viestin kopiot (carbon copy).
Bcc	Toissijaiset sähköpostin lähetysosoitteet, joista viestin vastaanottaja näkee vain omansa. (blind carbon copy).
Message-id	Yksilöivä tunniste sähköpostiviestille.
Subject	Sähköpostiviestin otsikko tai aihe.
Recieved	Jokainen viestin matkallaan läpikäymä SMTP-palvelin lisää Received-otsikon, joka kertoo viestin vastaanottaman koneen sekä muuta SMTP-yhteyteen liittyvää tietoa.
X-kenttä	Määrittämättömiä kenttiä, joihin voidaan lisätä ylimääräistä tietoa esimerkiksi käytetystä sähköpostiohjelmasta.

2.2.2 MIME-osa

Alkujaan sähköpostin oli tarkoitus välittää vain ja ainoastaan 7-bittistä ASCII-tekstiä. Tämä mahdollisti ainoastaan englannin kielestä löytyvien kirjainten ja merkkien käytön. Sähköpostin leviäminen muihin maihin ja sen käytön yleistyminen toi tarpeen luoda keino, jonka avulla sähköpostissa voidaan lähettää myös muita erikoismerkkejä. MIME (Multipurpose Internet Mail Extensions) oli ratkaisu tähän merkkiongelmaan. MIME mahdollistaa myös muun kuin tekstityyppisen tiedoston lähettämisen sähköpostiviestin sisällä. Erilaisten tiedostojen liittäminen viestiin ja esimerkiksi HTML-postien lähettäminen on MIME:n avulla mahdollista. Tämä toimii yksinkertaistettuna siten, että MIME-osioon koodataan sähköpostiviesti tai sen osa, esimerkiksi liitetiedosto SMTP:n ymmärtämään muotoon. Jokaiselle sähköpostin MIME-osiolle on määritelty mediatyyppi, joka määrittää osion sisällön. Tavallisimpia MIME-mediatyyppejä ovat *text, image, audio, video, application, multipart, message* ja *model*.

Text-tyyppinen MIME-osio sisältää tekstiä. Tähän osioon eivät kuitenkaan kuulu tekstinkäsittelyohjelmien tiedostot. *Image*-osio sisältää erityyppisiä ja -formaattisia kuvia. *Audio*-osio koostuu äänestä, musiikista tai puheesta. *Video*-osio käsittää liikkuvaa kuvaa. *Application*-osa sisältää binääridataa, joka ei liity mihinkään muuhun mediatyyppiin. Tässä osassa siirretään esimerkiksi ohjelmia tai tekstinkäsittelyohjelmien tekstitiedostoja. *Message*-osa sisältää Internet-viestejä kuten sähköposteja tai esimerkiksi uutisryhmäartikkeleita. *Model*-osiossa on erilaista mallinnusdataa. *Multipart*-osio sisältää useita eri mediatyyppisiä MIME-osioita. Jokaisella mediatyypillä on vielä erillinen alaosa, joka tarkentaa sitä edelleen. Esimerkiksi mediatyyppi text/plain kertoo kyseisen MIME-osan sisältävän pelkkää muotoilutiedotonta tekstiä, kun taas image/gif paljastaa osion sisältävän gif-tyyppisen kuvan. (Borenstein 1993.)

3. Roskaposti

Mitä roskaposti oikeasti on, miten roskan tunnistaa kunnollisesta sähköpostista? Suurin osa sähköpostin käyttäjistä tietää kyllä vastauksen, mutta kunnollisen määritelmän antaminen voi osoittautua vaikeaksi tehtäväksi. Roskapostin mahdollisimman tarkka ja selkeä määrittäminen on kuitenkin ensimmäinen ja tärkeä askel tämän ilmiön ymmärtämisessä ja sen torjumisessa. Ensin käyn läpi roskapostin yleisimpiä nimityksiä sekä niiden eroja ja tarkoituksia. Määritän myös termin roskattomalle sähköpostille. Sitten tarkastelen roskapostin eri määreitä ja katson, mitä roskapostiviestit sisältävät. Lopuksi pureudun roskapostin aiheuttamiin haittoihin.

3.1. Roskapostin nimiä

3.1.1 Spam

Roskapostilla on monia nimiä ja lyhenteitä. Englannin kielessä yleisin termi on *spam*. Internet in alkuaikoina 1990-luvun vaihteessa, toistuvia ja häiritseviä uutisryhmäpostituksia alettiin kutsua sanalla spam, joka alunperin merkitsi purkitettua lihavalmistetta. Myöhemmin sana levisi tarkoittamaan sähköpostissa tapahtuvaa toistuvaa, saman tai samankaltaisen viestin lähettämistä. Itse asiassa Monty Python –koomikkoryhmän sketsi lienee syy tähän yllättävään merkityksen muutokseen lihavalmisteesta roskapostiksi: sketsissä sanaa spam toistetaan jatkuvasti kasvavalla vauhdilla, kunnes kyseinen sana on ainoa asia, mitä sketsissä kuulee. Spam-sana ikään kuin syö kaiken hyödyllisen tiedon pois sketsissä käytävästä keskustelusta. Saman asian ärsyttävyyteen saakka toistaminen ja hyödyllisen tiedon peittäminen kuvaakin hyvin roskapostin kahta tunnusmerkkiä: toistuvuutta ja häiritsevyyttä (Schwartz & Garfinkel 1999).

3.1.2 UBE ja UCE

Vaikka spam lienee yleisin ja eniten käytetty termi sähköpostin käyttäjien sekä lehdistön keskuudessa, niin asiantuntijoiden ja roskapostin tutkijoiden piirissä on noussut esiin useita lyhenteitä, joilla pyritään määrittelemään spammia aiempaa tarkemmin. Ensimmäinen

lyhenne on UBE (unsolicited bulk email tai unsolicited broadcast email) eli *ei-toivottu massasähköposti*. Toinen paljon käytetty lyhenne on UCE (unsolicited commercial email) eli *ei-toivottu kaupallinen sähköposti*. (Jacobsson 2003.)

3.1.3 Junk Mail

Sanoja *junk mail* tai *junk e-mail* käytetään paljon. Junk mail tarkoittaa tavallisessa ”etanapostissa” kulkevaa mainospostia. Kontekstista riippuen sanalla viitataan tavalliseen mainospostiin tai roskapostiin yleensä, ja se käsittää myös sähköisen roskapostin. Junk e-mail -termillä viitataan puolestaan ainoastaan sähköiseen roskapostiin. Nämä termit voidaan silti yhdistää helposti lyhenteeseen UCE, jolla viitataan eritoten mainosroskapostiin.

3.1.4 Roskaposti

Suomen kielessä *roskaposti* on eniten käytetty termi, joskin sen rinnalla käytetään englannista lainattuja sanoja spämmi tai spammi, etenkin puhekielessä. Silloin tällöin nämä termit esiintyvät myös kirjoitetussa kielessä. Samoin ilmaisuja ’roskasähköposti’ ja ’sähköinen roskaposti’ näkee käytettävän medioissa ja kirjallisuudessa.

3.1.5 Ei-roskaposti

Varsinaista kunnollista sähköpostia, niin sanottua ei-roskapostia, kutsutaan englanninkielisissä artikkeleissa käsitteellä *ham*. Termiä käytetään yleensä keskusteluissa tai teksteissä, kun halutaan korostaa nimenomaan eroa spammin ja ei-roskapostin välillä. Eritoten erilaisten estomenetelmien yhteydessä on tärkeää erottaa nämä kaksi sähköpostilaatua toisistaan. Termeille spam ja roskaposti on yhteistä niiden yleisluonteisuus. Kumpikaan termi ei sinällään sisällä mitään roskapostin määritelmää. Tästä syystä olen päätynyt termiin roskaposti. Ei-roskapostista (ham) käytän työssäni termiä ’kunnollinen posti’ tai ’kunnollinen sähköposti.’

3.2. Roskapostin ominaisuuksia

Roskapostin monet erilaiset nimet ja erilaiset määritelmät kuvaavat hyvin roskapostin subjektiivista luonnetta. Subjektiivisuudella tarkoitan tässä tilanteessa henkilökohtaista arviota tai mielipidettä. Eri ihmiset tai tahot voivat määritellä roskapostin hyvin monella eri tavalla ja silti käyttää samoja termejä. Joillekin roskaposti merkitsee vain porno- tai viruspostia; toisille kaikki sellainen posti, jota ei ole pyydetty tai hyväksytty, on roskaa. Määritelmien kirjavuudesta johtuen toisen roskaksi kokema materiaali voi olla toiselle jopa toivottua postia. Ihmisten mielipiteet ja määritelmät vaihtelevat myös ympäristön mukaan. Hauska vitsi voi muuttua loukkaavaksi siirryttäessä kotipostista työpostiin. Esimerkiksi sähköpostitse leviävään Viagra-mainokseen suhtautuminen voi kokonaan muuttua iän karttuessa – roskaposti toimiikin hyödyllisenä ja kiinnostavana mainoksena. Seuraavaksi esittelen erilaisia roskapostin määreitä.

3.2.1 Ei-haluttavuus

Lähes jokaisen roskapostimääritelmän tärkein kohta on viestin ei-haluttavuus. Roskapostiksi luetaan viesti, jota vastaanottaja ei halua ja joka on lähetetty ilman lupaa. Samoin roskapostiksi lasketaan sellaiset viestit, joita ei ole erikseen pyydetty. Tämä ei tietenkään tarkoita sitä, että laskut tai muut ikävät ilmoitukset, joita sähköpostin omistaja voi saada, olisivat roskapostia. Toisaalta esimerkiksi työkaverin lähettämät videopätkät tai hauskat kuvat voivat olla pahakin riesa, jos posti haetaan modeemin tai muun hitaan ja kalliin yhteyden yli sähköpostipalvelimelta. Hyvää tarkoittava posti muuttuu näin nopeasti hyvinkin ei-halutuksi. Tähän ristiriitaan antaa valoa seuraava roskapostin määre eli yhteys.

3.2.2 Yhteys

Toinen tärkeä roskapostin piirre on lähettäjän ja vastaanottajan välinen aikaisempi yhteys – tai oikeastaan sen puuttuminen. Vaikka sähköpostia lähetetään ilman toisen suoraa lupaa tai pyyntöä, sähköpostin katsotaan olevan kunnollista, kun viestin lähettäjällä ja vastaanottajalla on jonkinlainen ennalta muodostettu yhteys tai suhde. Esimerkiksi sähköpostiviestit opettajalta, kaverilta tai vaikka työnantajalta sisältävät selvän suhteen viestin lähettäjän ja sen vastaanottajan välillä. Vaan mikä on viestintäsuhteen laatu esimerkiksi silloin, jos olet ostanut uuden monitorin verkkokaupasta ja sen jälkeen alat saada mainospostia muista kyseisen

kaupan tuotteista? Tässä tapauksessa ennalta määrätty suhde on kauppias-asiakas -suhde. Monien – varsinkin sähköpostimainostajien – mielestä pelkkä asiakassuhde riittää oikeuttamaan mainospostin lähettämisen asiakkaalle. Joskus pelkkä kiinnostuksen osoittaminen verkkokauppaa tai muuta instanssia kohtaan – kuten sähköpostilla lähetetty kysymys jostain tuotteesta – voidaan mieltää sähköpostisuhteen synnyttäväksi tapahtumaksi. Voiko tällainen suhde syntyä myös pelkästä käynnistä nettikaupan verkkosivuilla tai osallistumisesta kaupan järjestämään kilpailuun? Tästä ollaan varsin erimielisiä roskapostia vastustavien ja mainospostia lähettävien leireissä. Vastustajien mielestä ilman suoraa lupaa lähetetty posti on aina luvatonta eli roskapostia. Juuri suhteen syntymisen ongelmaan liittyy kiinteästi roskapostirintamalla käytävä opt-in- ja opt-out -taistelu.

3.2.3 Opt-out, Opt-in ja Double opt-in

On muodostunut kolme käytäntöä sähköpostimarkkinoijien ja asiakkaiden väliseen ristiriitaan siitä, mikä on haluttua tai hyväksyttyä postia ja milloin kunnollisen mainospostin lähettämiseen tarvittava suhde on muodostunut. Näitä käytäntöjä kutsutaan termeillä *Opt-out, Opt-in* ja *Double opt-in*.

Opt-out on näistä kolmesta käytännöistä löysin ja yleensä sähköpostimarkkinoijien kannattama. Siinä oletetaan, että mainostajan ja mainoksen vastaanottajan, toisin sanoen lähettäjän ja vastaanottajan välinen suhde on aina voimassa. Tämä tarkoittaa, että mainostajat voivat lähettää postia kenelle tahansa, vapaasti ja rajattomasti. Viesteissä on kuitenkin oltava mahdollisuus estää niiden tulo, eli vastaanottaja voi poistaa itsensä mainoslistalta. (Gauthronet 2001.)

Tähän malliin liittyy runsaasti ongelmia: jos käyttäjä yrittää poistaa itseään listoilta, siitä seuraa tavallisesti vain lisää roskapostia. Tämä tilanne ja Opt-out -perusidea eivät voisi olla enempää ristiriidassa keskenään. Toinen ongelma koskee viestityyppiä: voiko autokauppias lähettää sinulle mainoksia Volvosta sen jälkeen kun kielsit Mersun mainoksien lähettämisen, vai pitääkö autokauppiaan lopettaa mainospostin lähettäminen asiakkaalle kokonaan yhden peruuttamisviestin jälkeen? (Gauthronet 2001.)

Opt-in tarkoittaa mallia, jossa sähköpostin lähettäjällä ei ole suhdetta viestin saajaan, vaan suhde on luotava ennen viestien lähettämistä. Tämä tarkoittaa käytännössä sitä pientä rastilaatikkoa nettikilpailun vastauslaatikon yläpuolella, jossa sivulla vierailijalta pyydetään lupaa informaation lähettämiseen. Tämä rastituksen jälkeen sivun käyttäjä on hyväksynyt asiakassuhteen ja hänelle voidaan lähettää jatkossa mainoksia. Samoin kun Opt-out:issa vastaanottajalla on täysi oikeus lopettaa viestien tulo milloin vain. Opt-in:istä on myös vahvempi muoto eli double opt-in. Tässä mallissa, jota kaikki roskapostin vastustajat yleisesti vaativat sähköpostimarkkinoijilta, hyväksytyn suhteen jälkeen lähetetään asiakkaalle vielä yksi sähköpostiviesti, jossa pyydetään uudestaan lupaa lähettää mainospostia tähän sähköpostiosoitteeseen. Tämä malli estää myös kiusanteon, esimerkiksi muiden ihmisten lisäämisen mainoslistoille. (Gauthronet 2001.)

3.2.4 Massapostitus

Massapostitus (bulk mail) on keskeinen roskapostin ominaisuus. Paljon käytetyssä roskapostia tarkoittavassa UBE-lyhenteessä painotetaan juuri roskapostin massapostitusluonnetta. Massapostitus tarkoittaa postitusta, jossa lähetetään kerralla monta samaa tai samankaltaista viestiä eri vastaanottajille. Mutta kuinka monta viestiä päivässä pitää lähettää, että kyseessä on massapostitus? Onko kymmenen viestiä riittävästi vai täytyykö massapostin sisältää vähintään sata viestiä päivässä? Toisaalta jopa tuhat samansisältöistä viestiä voidaan helposti lähettää yhdessä postituslistassa eikä kyseessä ole roskapostitus, vaan esimerkiksi tärkeä ilmoitus työpaikan tai yliopiston henkilöstölle. Tarkkaa massapostin määritelmää onkin viestimäärän perusteella mahdoton antaa, mutta yleensä noin kaksikymmentä viestiä vuorokaudessa oikeuttaa massapostin määritelmään (Puolamäki 2002).

Massapostituksen määritelmän yhteydessä nousee esiin toinen tärkeä termi, *samankaltaisuus*. Samankaltaisuus tarkoittaa massapostituksessa viestin samaa asiasisältöä. Viestien ei tarvitse olla identtisiä, riittää, että niiden sisältämä asiasisältö on tarpeeksi samankaltainen. Esimerkiksi, jos viestistä vaihtaa vastaanottajan nimen ja otsikon, ei se muuta viestin merkityksellistä sisältöä mihinkään. Samankaltaisuuden tarkka määritteleminen onkin vaikea tai mahdoton tehtävä. Eräänlainen ”minusta tuntuu” -tuntuma vaivaa muutenkin monia roskapostiin liitettäviä seikkoja. Tämä vahvistaa aikaisemmin mainittua kysymystä

roskapostiongelman subjektiivisuudesta tai yksilösidonnaisuudesta. Subjektiivisuudesta seuraa lisäongelmia sähköpostin torjunnalle.

3.2.5 Osoitteiden alkuperä

Roskapostin tunnusmerkkinä voivat toimia myös ne erinäiset keinot, joilla viestin lähettäjät ovat saaneet haltuunsa vastaanottajien osoitteet. Osoite voidaan hankkia joko luvallisesti tai luvattomasti. Luvallisessa tapauksessa sähköpostiosoitteen omistaja tietää luovuttavansa osoitteensa taholle, joka aikoo lähettää hänelle postia. Luvattomassa tilanteessa osoitteet pyydetään ilman ilmoitusta mahdollisesta mainospostista. Luvatonta osoitteiden hankkimista on myös osoitteiden kerääminen ihmisten, laitosten tai yritysten kotisivuilta. Luvatonta keräämistä tapahtuu lisäksi keskustelualueilla, uutisryhmissä, jopa chateissa. Näissä tapauksissa osoitteet viedään osoitteenomistajilta ilman minkäänlaista ilmoitusta tai lupaa. Voidaan tietysti väitellä siitä, antaako henkilö tai yritys luvan lähettää sähköpostia julkaistessaan osoitteensa esimerkiksi kotisivuillaan.

Luvallisesti sekä luvattomasti kerätyillä sähköpostiosoitteilla käydään myös vilkasta kauppaa. Kuka tahansa voi ostaa halutessaan Internetistä valtavan määrän sähköpostiosoitteita muutamalla dollarilla. Huomionarvoista on myös se, että luvallisestikin kerätyt osoitteet muuttuvat luvattomiksi heti, kun ne myydään kolmansille osapuolille ilman osoitteen omistajan lupaa. Tällaisessa tilanteessa sähköpostiosoitteen omistajan valta säädellä vastaanottamaansa postia haihtuu tuulena ilmaan.

3.2.6 Kaupallisuus

Kaupallisuus on ehkä eniten käytetty ja paljon kiistoja aiheuttanut roskapostin ominaisuus. Joidenkin tahojen mukaan sähköpostiviestin pitää myydä, mainostaa tai tuoda julki jotain tuotetta tai palvelua ennen kuin se voidaan määritellä roskapostiksi. Kaupallisuuden korostamista tukee se tosiasia, että väljimmänkin mainoksen määritelmän mukaan suurin osa ihmisten saamista ei-toivotuista viesteistä on mainoksia. Kaupallisten viestien suuren joukon perusteella monet rajaavat roskapostin vain sellaisiin viesteihin, jotka sisältävät mainoksia. Termit ’UCE’ ja ’mainosroskaposti’ painottavat kaupallisuuden huomioimista roskapostia määriteltäessä.

Silti kaikki sähköpostiin saapuva mainosposti ei ole roskapostia. Internetissä on huomattava määrä kunnollisia sähköpostimarkkinoijia, jotka noudattavat lakia ja hyviä tapoja. Lienee kuitenkin mahdotonta luoda sellaisia säännöksiä, että mainostaja pystyisi lähettämään mainospostia, jota kukaan ei leimaisi roskapostiksi.

3.2.7 Haitallisuus

Seuraava roskapostin piirre on haitallisuus. Roskapostiksi voidaan luetella viestit, jotka lähetetään tarkoituksena vahingoittaa tai kiusata vastaanottajaa. Esimerkiksi sellaiset viestit, jotka sisältävät viruksia, matoja tai muita vaarallisia ohjelmia tulkitaan roskapostiksi. Kiusaamisella tarkoitetaan viestejä, joissa ”neuvotaan” käyttäjää poistamaan koneesta joitain tärkeitä käyttöjärjestelmän tarvitsevia tiedostoja tekaistun viruksen tai muun uhan takia.

3.2.8 Valheellisuus

Haitallisuudesta voidaan helposti siirtyä toiseen roskapostin inhottavaan ominaisuuteen eli valheellisuuteen. Valheellisuutta näyttää olevan kahta eri päätyyppiä. Ensinnäkin viestin lähetystietojen muuttaminen tai väärentäminen on yhden tyypin valheellisuutta (CDT 2003). Toisaalta erilaiset huijauskirjeet, kuten pyramidihuijaukset tai rahankeräyskirjeet ovat esimerkkejä roskapostissa esiintyvästä valheellisuudesta. Samaan valheellisuuden vyyhtiin kuuluvat myös olemattomat tai selvästi toimimattomat tuotteet, joita roskapostissa usein kaupitellaan ja mainostetaan. (FTC 2003.) Esimerkiksi käyvät kaikkien tuntemat jalkojen tai muiden ruumiinjäsenten pituuskasvua lisäävät pillerit sekä muut hämmästyttäviä tuloksia tuottavat luonnonvalmisteet. Ehkä tunnetuin huijauskirjetyyppi on niin sanottu nigerialainen kirje, joka on laajalle levinnyt ja paljon keskustelua herättänyt huijausroskaposti.

Nigerialaisiksi huijauskirjeiksi kutsutaan tietynlaisia sähköpostikirjeitä. Niissä pankkiiri, syrjäytetty presidentti tai joku muu rikas taho etsii kumppania, jonka avulla voitaisiin siirtää uskomattoman suuria summia rahaa ulos maasta. Kyseinen maa on usein Nigeria, niin kuin huijauksen nimikin antaa ymmärtää, tai joku muu Afrikan tai Aasian valtio. Todellisuudessa huijarit ovat yleensä Yhdysvalloista tai Euroopasta. Palkinnoksi avusta luvataan prosentit siirretystä summasta, joka on useita miljoonia dollareita. Ainoa asia mitä uhrin pitää tehdä, on antaa pankkitilinsä numero, henkilötiedot ja muutaman sata tai tuhat dollaria kuluihin. Tietenkään mitään rahoja ei ole olemassa, ja lähetetyt rahat häviävät kuin tuhka tuuleen.

Tämän ensimmäisen rahojen siirron jälkeen alkaa varsinainen huijausoperaatio, jossa uhrilta yritetään huijata lisää rahaa loputtomien verukkeiden avulla. Lopuksi henkilö yritetään saada matkustamaan huijareiden luokse, mitä voi seurata jopa kidnappaus. Erilaisia versioita tästä huijauskirjeestä liikkuu yleisesti, mutta kaikki ovat varmasti täyttä valhetta. Tämä huijaus tunnetaan myös nimellä 419. Numero viittaa Nigerian perustuslain lakipykälään, joka kieltää näiden kirjeiden lähettämisen. (Edelson 2003.)

3.2.9 Loukkaavuus

Roskapostin loukkaavuus on noussut viime aikoina puheenaiheeksi varsinkin Yhdysvalloissa ja Englannissa. Eritoten pornoa sisältävät viestit aiheuttavat paljon paheksuntaa ja mielipahaa. Roskapostille luonteenomainen sokeus aiheuttaa sen, että kuka tahansa vauvasta vaariin voi saada hyvinkin graafista ja kieleltään karkeaa postia. Sähköposti mielletään helposti yksityiseksi ja hyvin henkilökohtaiseksi viestintävälineeksi – mitä se ei kuitenkaan ole – ja tästä syystä viesteistä loukkaannutaan tai jopa pelästytään helposti. Eritoten ja syystäkin ollaan huolissaan lasten ja nuorten saamista loukkaavista ja anatomisesti tarkoista roskaposteista. Törkeiden kuvien lisäksi erilaiset elinten ja jäsenten kasvatuslääkkeet tai ”rikastu nopeasti”- huijaukset voivat hämmentää ja aiheuttaa mielipahaa nuorten roskapostiuhrien keskuudessa. Yhdysvalloissa ollaan huolissaan myös yritysten työntekijöiden saamista törkeistä roskaposteista. Yritykset pelkäävät oikeusjuttuja, joita loukkaavia posteja saavat henkilöt voivat yritystä vastaan nostaa. (Trudeau, 2003a; Wired 2003.)

3.2.10 Sokeus

Roskaposti on myös usein ”sokeaa”. Roskapostittajat eivät ole kiinnostuneet siitä, kuka viestin saa, tai onko viesti aiheellinen tai edes kiinnostava tälle henkilölle. Sähköpostimainonta voisi olla hyvinkin suunnattua ja tarkennettua, silti roskapostittajat lähettävät viestejä periaatteella ”kaikille kaikkea”. (Lindberg 1999.)

3.3. Roskapostin sisältö

Roskapostilla on monta nimeä ja vielä enemmän määritelmiä, kyseessä onkin monimuotoinen ilmiö ja ongelma. Kaiken tämän ytimessä on roskapostiviesti. Mitä roskapostittajat haluavat meille myydä, kertoa tai ilmoittaa? Seuraavaksi käyn läpi roskapostiviestien eri tyyppejä ja sisältöjä.

3.3.1 Roskapostin tyypit

Roskapostin määritelmiin nojautuen roskapostiviestit voidaan jakaa seuraavasti. Ensimmäisen ja suurimman ryhmän muodostavat puhtaat mainospostit. Nämä sähköpostiviestit yrittävät myydä meille jotain oikeaa, todellista tuotetta. Toinen ryhmä koostuu huijausviesteistä, joilla yritetään huijata ihmisiltä tili- tai luottokorttitietoja, osoitetietoja tai käteistä rahaa. Kolmatta ryhmää kutsun ilkivaltaviesteiksi. Näiden viestien ainoa tarkoitus on hankaloittaa ja haitata ihmisten elämää. Neljännen ryhmän muodostavat ketjukirjeet. Ne voidaan luetella omaksi ryhmäkseen, vaikka niissä välillä esiintyy elementtejä huijauskirjeistä ja ilkivaltakirjeistä.

Viidentenä ryhmänä voidaan pitää erilaisia propaganda- ja tiedotuskirjeitä. Kuudes ryhmä on tuttujen, työtovereiden ja omaisten lähettämä viihderoskaposti. Seitsemäntenä ryhmänä voidaan pitää pientä mutta sitäkin kummallisempaa ”outojen” roskapostiviestien joukkoa. Outoihin roskaposteihin kuuluvat esimerkiksi viestit, joissa halutaan ostaa Star Trek – fantasiamaailmaan liittyviä tavaroita, kuten aikamatkustustarvikkeita. Kuka näitä viestejä lähettää ja miksi? Usein niiden epäillään olevan roskapostittajien testiviestejä, joilla testataan roskapostisuodattimia ja muita puolustusmenetelmiä. Kahdeksanteen ryhmään lasken virusten levittämistä varten tehdyt roskapostit. Sen sijaan yhdeksänteen ryhmään kuuluu virusten leviämisessä syntyvä roskaposti.

3.3.2 Mainosroskaposti

Mainosposti on suurin roskapostin ryhmä sekä viestimäärällisesti että siinä liikkuvan rahan kannalta. Mainosviestit tarjoavat kuluttajille mitä mielenkiintoisimpia tavaroita, palveluita ja ideoita. Roskapostin kautta myytävät tuotteet ovat yleensä hyvin halpoja, hämäräperäisiä ja jopa laittomia tai muuten arkaluonteisia. Tuotteet ovat yleisesti ottaen sellaisia, joita ei pysty, saa tai kannata mainostaa muualla. Mainospostiin kuuluvat myös tuotteet, joiden mainostetut

vaikutukset ovat todellisuudessa hyvin heikkoja tai olemattomia. Tällaisia tuotteita ovat esimerkiksi lääkevalmisteet, jotka lupaavat kasvattaa sukupuolielimien kokoa. Nämä selvästi ei-toimivat tuotteet voitaisiin sijoittaa aivan hyvin myös huijauskategoriaan, mutta niin kauan kun vastaavia tuotteita tarjotaan valtakunnallisilla televisiokanavilla esitettävissä mainosohjelmissa, nämä tuotemainokset voidaan lukea mainospostiksi. (Wood 2003.)

Mainospostin yleisyyden syy on ilmeinen, sillä tässä roskapostin muodossa liikkuu eniten rahaa. Esimerkiksi eräs salakuunteluohjelmistoja 40 dollarin kappalehintaan myynyt yrittäjä ansaitsi 700 000 dollaria vuodessa ”puhtaana käteen” (Westley 2003). Roskapostissa näkyvät myös sesonkiajat: lomakuukausina, kuten joulun alla roskapostin määrät nousevat selvästi (Roberts 2002). Federal Trade Commision (FTC 2003) jakaa mainosviestit seuraavaan kahdeksaan ryhmään: talous, aikuisviihde, terveys, Internet ja tietokoneet, vapaa-aika ja matkailu, koulutus, tuotteet ja muut mainosviestit. Mainosroskapostin lajien suurusluokat esitetään Taulukossa 2:

Taulukko 2. Mainosroskapostin eri lajit ja prosentit (FTC 2003)

Mainosroskapostin tyypit	%
Talous	17
Yritystoiminta	20
Aikuisviihde	18
Terveys	*10*
Internet ja tietokoneet	*7*
Vapaa-aika ja matkailu	2
Koulutus	1
Tuotteet	16
Muut	9

Talous

Tähän ryhmään kuuluvat erilaiset omaa taloudellista tilannetta parantavat tuotteet ja neuvot. Roskapostissa liikkuu paljon tarjouksia halvoista lainoista sekä ohjeita luottokorttien

helppoon hankintaan. Lisäksi roskapostista löytyy ohjeita muun muassa veloista eroon pääsemiseen sekä erilaisia sijoitusneuvoja ja niin sanottuja pyramidihuijausjärjestelmiä. Tähän kategoriaan kuuluvat myös erilaiset maksulliset ohjeet, kuten neuvot normaalin kirjepostin ilmaiseen lähettämiseen. Roskapostin luonteen mukaisesti kaikkien näiden neuvojen tehokkuus tai laillisuus on aina kyseenalainen.

Yritystoiminta

Tähän ryhmään kuuluvat kaikki yritystoimintaan liittyvät mainokset ja maksulliset ohjeet. Niistä löytyy muun muassa ohjeita oman tuottavan yrityksen pystyttämiseksi. Ohjeet kertovat, kuinka tulee toimia jos haluaa ryhtyä myymään autoja tai perustaa vaikkapa kauppaketjun. Kirjailijoiksi haluaville löytyy palveluja, jotka lupaavat lähettää kirjoituksia kustantajille. Toiset palvelut taas lupaavat asiakkaalleen varman työpaikan hyvällä palkalla ilman minkäänlaista kokemusta tai koulutusta. Kaiken tämän informaation saa pientä maksua vastaan. Tähän kategoriaan luetaan myös erilaiset ”työskentele kotona” -palvelut sekä ”tienaa rahaa surffaamalla Internetissä” -järjestelmät.

Aikuisviihde

Eniten yleistä keskustelua aiheuttava roskapostimainonnan muoto on aikuisviihde eli pornografia. Nämä viestit mainostavat erilaisia treffipalveluita tai ihmissuhdeneuvoja sisältäviä sivuja – tai keskittyvät aikuisviihdesivujen esittelemiseen. Aikuisviihdeviesteihin liittyy usein kuvia ja viestit ovat kieleltään hyvin karkeita.

Terveys

Erilaisten terveyttä ja ihmisen hyvinvointia lisäävien tuotteiden roskapostimainonta on erittäin suosittua. Tästä käyvät esimerkeiksi vitamiini- ja hivenainemainokset sekä erilaiset ihmeyrttimainokset, jotka lupaavat nopeaa laihtumista tai pituuskasvun kiihtymistä. Näiden selvästi toimimattomien tuotteiden lisäksi roskaposteissa myydään erilaisia lääkkeitä, kuten Viagraa ja antihistamiineja tai jopa rauhoittavia ja psyykelääkkeitä – tietenkin ilman reseptiä.

Internet ja tietokoneet

Tähän kategoriaan kuuluvat tuotteet ja palvelut, jotka liittyvät tietokoneisiin tai Internetiin. Esimerkeiksi sopivat kotisivujen julkaisu- ja ylläpitopalvelut, *web hosting*, roskapostin

torjuntapalvelut sekä sähköpostimainontapalvelut. Roskapostista on tullut niin laaja ongelma ympäri maailmaa, että myös itse roskapostittajat ovat alkaneet myydä roskapostin torjuntaohjelmistoja.

Piraattiversioiden myynti muka alkuperäisinä tuotteina on myös hyvin yleistä. Ohjelmat joko ladataan roskapostittajan tietokoneelta tai ne lähetetään huonosti kopioidun CD:n kanssa ilman ohjeita. On lisäksi mahdollista, että maksettuasi ohjelman et saakaan yhtään mitään postia. Sen sijaan roskapostittajan koneelta ladattavien ohjelmien mukana asiakas voi saada viruksen tai vaikkapa niin sanotun troijalaisen. Troijalainen asentaa koneellesi salakuunteluohjelmia, jotka keräävät sähköpostiosoitteesi sekä salasanasi. Sitten ohjelma lähettää tiedot takaisin roskapostittajalle. Ohjelma voi jopa tehdä tietokoneesta roskapostitusaseman, joka alkaa öisin käyttäjän tietämättä lähettää roskaposteja ympäri maailmaa. (Goldman 2003.)

Vapaa-aika ja matkailu

Halpoja matkoja, lomakohteita tai lomaosakkeita tarjotaan myös roskapostin muodossa. Samoin on-line -kasinoiden mainokset kuuluvat tähän kategoriaan. Tarjotut matkat, hotellihuoneet tai lomaosakkeet ovat uskomattoman halpoja, mutta lähes aina kyse on jonkinlaisesta huijauksesta.

Koulutus

Erilaiset diplomit ja todistukset kuuluvat roskapostin perustarjontaan. Miltä kuulostaisi lupaus maisterin papereista ilman turhaa koulunkäyntiä, tai tarjous valmiista gradusta yhdellä napin painalluksella. Myös niin sanotut ”vain dollari per sana” -tyyppiset mainokset kuuluvat tähän ryhmään.

Tuotteet ja palvelut

Tähän ryhmään lasketaan mukaan kaikki muut mahdolliset tuotteet ja palvelut, jotka eivät sovi muihin edellä mainittuihin kategorioihin, mutta joiden mainoksia roskaposteissa silti esiintyy. Tämän kategorian mainoksissa myydään esimerkiksi merkkituotteita uskomattoman halvalla tai tarjotaan asiakkaille laitteita, jotka tekevät mitä ihmeellisimpiä asioita. Lisäksi

tämän luokan roskaposteissa myydään aivan tavallisia tavaroita kuten leluja. Joulun alla eräs laajasti levinnyt roskapostimainos myi radio-ohjattavia autoja.

3.3.3 Huijausroskaposti

Huijaussähköpostit tarjoavat ilmaista rahaa ja keinoja helppoon rikastumiseen. Tämän tyypin roskapostit eivät suoraan myy mitään tuotetta, vaan tarjoavat ystävällisiä mahdollisuuksia tai keinoja tienata hieman ylimääräistä. Huijauspostit voivat myös houkutella ihmisiä lataamaan koneeseensa erilaisia apuohjelmia, jotka ovat oikeasti mainos- tai vakoiluohjelmia. Toisinaan tällaiset huijauspostit toimivat myös kehotuksina vierailla yrityksen kotisivuilla, jossa sitten haitallisia ohjelmia pystytään lataamaan käyttäjän tietokoneelle. Tähän roskapostityyppiin kuuluvat esimerkiksi paljon keskustelua synnyttäneet ”nigerialaiset kirjeet”, jotka tunnetaan myös 491-huijausposteina. Numerokoodi tule lakipykälästä, joka kieltää kyseiset huijauspostit. (Edelson 2003.)

3.3.4 Ilkivaltaroskaposti

Ilkivaltaviestejä ovat esimerkiksi tapaukset, joissa ihmisiä käsketään poistamaan tärkeitäkin käyttöjärjestelmän komponentteja virusuhan varjolla. Toisinaan esiinnytään vaikkapa käyttöjärjestelmiä tekevänä firmana ja tarjotaan vinkkejä käyttöjärjestelmän korjaamiseen. Todellisuudessa vinkit voivat aiheuttaa vakaviakin tuhoja tietokoneen käyttöjärjestelmässä. Postien perimmäinen tarkoitus jää arvailujen varaan. Kyse saattaa olla ilkivallasta ja sitä voisi verrata virustehtailuun.

Toinen ilkivallan muoto on ”joe jobiksi” kutsuttu sähköpostihyökkäys. Siinä roskapostittajat suorittavat roskapostihyökkäyksen, jonka lähettäjäksi naamioidaan eli väärennetään hyökkäyksen uhrin sähköpostiosoite tai sähköpostipalvelin. Roskapostit voidaan myös lähettää kyseisen henkilön huonosti turvatusta sähköpostipalvelimesta tai sähköpostimadon saastuttamasta kotikoneesta. Tämän jälkeen hyökkääjät vain odottavat, kunnes onneton uhri saa ryöpyn valituskirjeitä ja hänet listataan useisiin mustiin listoihin. Tämä tapahtuu yleensä hyvin nopeasti. Uhrin sähköpostipalvelu saatetaan jopa irtisanoa ennen kuin uhri ehtii tajuta, mitä on tapahtunut.

3.3.5 Propagandaroskaposti

Propagandan tai omien ajatusten levittäminen sähköpostin kautta on halpaa ja helppoa. Erilaisten asioiden lobbaus tai erikoistenkin ajatusten levittäminen laajaan tietoisuuteen on yllättävän yleistä roskapostimaailmassa. Ilkivaltapostien ja propagandapostien välimaastossa sijaitsevat erilaiset mustamaalausroskapostit. Näiden tarkoitus on yrittää tuhota ihmisen, organisaation tai järjestön maine. Tämä tapahtuu levittämällä kohteelle haitallista, usein valheellista tietoa.

3.3.6 Ketjukirjeet

Alun perin normaalista postissa alkaneet ketjukirjeet ovat nykyään siirtyneet sähköpostiaikaan. Ketjukirje on viesti, jonka tarkoitus on levitä mahdollisimman laajalle. Samalla kirje voi levittää jotain sanomaa, kerätä nimiä adressiin tai toimia vain huvittavana päivänpiristyksenä. Ketjukirjeet eroavat muista roskapostityypeistä siten, että ne pyytävät tai pahimmassa tauksessa uhkaavat viestin saajaa, jos hän ei suostu lähettämään viestiä eteenpäin mahdollisimman suurelle joukolle ihmisiä. Harmittomimmillaan ketjukirjeet ovat hauskoja viihdepaketteja; pahimmillaan ne sisältävät pyramidihuijauksien tapaisia rahankeruupyyntöjä. Tämän kaltaiset viestit lupaavat huimia summia pienellä alkupääomalla, mutta rahaa saa todellisuudessa vain kirjeen aloittanut henkilö, kuten pyramidihuijauksissa on tapana. (FTC 2002; 2003.)

3.3.7 Viihderoskaposti

Viihderoskaposti on mielenkiintoinen roskapostin muoto. Viihderoskapostilla tarkoitetaan vitsejä, videopätkiä, viihdyttäviä näytönsäästäjiä tai hupiohjelmia, joita opiskelijat tai työntekijät lähettävät toisilleen työpäivän piristykseksi. Mikä tekee tästä harmittoman oloisesta hupiviestien lähettämisestä roskapostittamista? Tällainen viestittely voidaan lukea viihderoskapostiksi viestien vaatiman kaistanleveyden johdosta sekä viihdeviestien lähettämisessä ja nauttimisessa hukkaan kuluvan työajan perusteella. Monien työnantajien tai miksei oppilaitostenkin kannalta tällaiset viestit täyttävät monta roskapostin tunnusmerkkiä ja siksi ne tuomitaan monilla työpaikoilla roskapostiksi (Trudeau 2003a.)

3.3.8 Virusroskaposti

Virusroskapostiksi luetaan viestit, jotka syntyvät kun sähköpostimadot ja virukset leviävät sähköpostiviestien avulla. Tämän kaltainen virusten aiheuttama liikenne on pahimmillaan äärimmäisen vaarallista ja saattaa aiheuttaa isojenkin sähköpostipalvelimien ylikuormittumisen, mistä seuraa palveluiden hidastumista ja jopa palvelun täydellinen luhistuminen. Virusroskapostiksi luetaan myös mainosroskapostit tai vastaavat, joiden mukana seuraa ilkeä yllätys kuten virus tai troijalainen (BBC 2003a; 2003b).

Viruksilla tarkoitetaan sähköpostin välityksellä itsestään Internetissä leviäviä pieniä ohjelmia. Yleensä näiden ohjelmien tavoitteena on levitä mahdollisimman laajalle ja samalla toimia tekijänsä nimen tai salanimen mainostajana, sillä virusten tekeminen on laitonta suurimmassa osassa maapalloa. Viruksen toinen vaarallisempi ja ilkeämpi tehtävä on aiheuttaa yleistä tuhoa saastuttamallaan koneella. Tällaiset virukset pyyhkivät saastuttamiltaan koneilta tiedostoja ja muita tietoja mahdollisimman tehokkaan laajenemisen lisäksi. Pyyhkimisen ohella virukset voivat lähettää tärkeitä tietoja saastuneelta koneelta viruksen tekijälle. Näitä tietoja voidaan käyttää hyväksi myöhemmissä hyökkäyksissä tai murtautumisyrityksissä. Uudemman ajan virukset kaappaavat saastuttamansa koneet. Näitä viruksia kutsutaan myös troijalaisiksi tunnetun Troijan puuhevosen mukaan. Nimen alkuperän tavoin virukset kantavat mukanaan ohjelman tai ohjelmia, jotka ne asentavat saastuttamalleen tietokoneelle. Näitä kaapattuja koneita voidaan käyttää hyökkäyksiin muita tietokoneita vastaan tai esimerkiksi roskapostin levittämiseen. (BBC 2003b; Lo 2003.)

3.4. Roskapostin ongelmia

Roskapostin inhottavuudesta ja häiritsevyydestä tuskin kuulee poikkeavia lausuntoja. Mutta roskapostin ongelmat ulottuvat myös syvemmälle ja levittäytyvät laajemmalle kuin satunnainen sähköpostinkäyttäjä arvaakaan. Seuraavaksi pureudutaan roskapostin ongelmiin ja kustannuksiin. Mitä roskaposti aiheuttaa meille käyttäjille, sähköpostipalvelimien ylläpitäjille, yhteiskunnalle tai itse sähköpostijärjestelmälle?

3.4.1 Hämmennys

Roskapostin saaminen vaikuttaa ihmisten kuvaan sähköpostin luotettavuudesta ja käytettävyydestä, varsinkin jos määrät ovat suuret. Vähän sähköpostia käyttävät sekä vähän asiasta tietävät henkilöt voivat huolestua oudoista ja usein törkeistä viesteistä, jotka saapuvat heille tuntemattomilta ihmisiltä tai tahoilta. Roskapostittajat muuttavat usein roskapostiviestien otsikon tai jopa lähettäjän tiedot sellaiseen muotoon, että viesti näyttää tulevan kollegalta tai muulta samassa työpaikassa toimivalta taholta, esimerkiksi mikrotuelta. Yleensä peruskäyttäjät eivät tiedä, mistä ja miksi heidän postikansioonsa ilmestyy roskapostia. Vielä suurempaa sekaannusta tai tuhoa aiheutetaan, jos saapuva viesti on luonteeltaan haitallinen. (Fallows 2003.)

3.4.2 Roskapostihalvaus

Sähköpostilaatikon täyttyminen roskapostista aiheuttaa käyttäjälle myös muita ongelmia. Tärkeiden viestin häviäminen roskan sekaan on hyvin yleistä. Näin voi tärkeitä viestejä jäädä huomaamatta – tai vielä pahempaa: ne voidaan tuhota vahingossa. Suurien roskamäärien poistamisen yhteydessä tuhoutuu helposti vahingossa myös kunnollisia ja tärkeitä sähköpostiviestejä. Tämä ”spam spasm” eli roskapostihalvauksena tunnettu ilmiö on kaikille paljon roskapostia saaneille tuttu ongelma. Yhdenkin tärkeän viestin menettäminen roskapostin takia on liikaa.

3.4.3 Roskapostin kustannusrakenne

Roskapostittajat vertaavat helposti omaa levittämäänsä roskaa normaaliin, perinteisessä postissa jaettavaan mainospostiin. Yhtäläisyyksistä huolimatta suurin ja ratkaisevin ero on roskapostimainonnan kustannusrakenteessa. Etanapostissa saapuvassa mainospostissa viestien lähettäjä maksaa kulut. Roskapostissa suurimmat kulut siirtyvät vastaanottajalle. Roskapostin lähettäminen on ilmaista tai lähes ilmaista. Tämä on yksi syy siihen, miksi roskapostissa liikkuvat viestimäärät ovat niin järjettömän suuria. Toinen syy roskapostin suureen lähetysmäärään on alhainen reagointikynnys sähköisiin mainoksiin. Reagointikynnyksellä tarkoitetaan sitä, kuinka nopeasti viestin saanut henkilö reagoi viestiin lähettäjän haluamalla tavalla – esimerkiksi käy tietyillä sivuilla tai ostaa tuotteen. Alhainen reagointikynnys korvataan lähettämällä suunnattoman suuria postimääriä, jolloin vain parin promillen reagointimäärä tuottaa satoja tai tuhansia reagointeja. Roskapostin kustannusrakenne on myös

sellainen, että mitä enemmän viestejä lähetetään, sen halvempaa se on lähettäjälle, mutta sen kalliimpaa vastaanottajalle. Normaalissa postissa vastaanottajan kustannukset eivät kasva, vaan pikemminkin hieman vähenevät viestimäärien kasvaessa. Lähettäjän kustannukset yksittäistä mainosta kohti tippuvat myös lähetysmäärän kasvaessa, mutta vain tiettyyn pisteeseen, ja ovat sen jälkeen lähes vakio. (Ahlm 2003.)

3.4.4 Kaistanleveyden kulutus

Roskapostin suuret lähetysmäärät aiheuttavat suurimmat kustannukset ja ongelmat palveluiden tarjoajille. Kenties suurin roskapostin runsaasta määrästä johtuva haitta on kaistanleveyden kulutus. Yhden roskapostin koko on noin viisi kilotavua. Yhdessä roskapostilähetyksessä voidaan lähettää miljoonia sähköposteja, jolloin päästään helposti usean gigatavun kokoisiin lähetyksiin. Tämä hidastaa ja jopa vaarantaa sähköpostin tai muunkin tietoliikenteen kulkemista. Turha posti pakottaa palveluntarjoajia sijoittamaan enemmän rahaa palvelinlaitteisiin, etenkin prosessitehon ja levytilan takaamiseksi. Tämä puolestaan johtaa korotettuihin käyttömaksuihin, eli itse asiassa loppukäyttäjä kustantaa roskapostituksen. (Wood 2003.)

3.4.5 Asiakastyytyväisyys ja sähköpostin uskottavuus

Toinen suuri ongelma on asiakastyytyväisyys. Palvelujen tarjoajat menettävät paljon asiakkaita roskapostin takia. Roskaposti on ongelma kaikille isoille sähköpostintarjoajille. Yksittäinen tapaus voi saada ihmiset menettämään uskonsa yritykseen ja vaihtamaan palvelusta toiseen. Myös asiakkaiden auttaminen on kallista. Erilaisten help-desk -palveluiden ruuhkautuminen roskapostien takia on yleistä, ja tämä tietysti lisää asiakkaiden tyytymättömyyttä. (Ahlm 2003.)

3.4.6 Kasvanut työn, työvoiman ja ohjelmistojen tarve

Roskapostia vastaan taisteleminen aiheuttaa myös kustannuksia henkilöstölle ja ohjelmistoille. Työntekijät joutuvat selvittämään sähköpostikansiotaan päivittäin, toisin sanoen etsimään kunnollisia viestejä roskapostin joukosta ja tuhoamaan roskaposteja. Tutkimuksen (Nucleus 2003) mukaan jokaisen työntekijän tuottavuus laskee vuosittain 1,8 % roskapostin takia ja yrityksen mittakaavassa suodattimet laskevat tuottavuutta 26%. Suodattimien ostaminen ja huoltaminen sekä estolistojen ylläpitäminen maksavat yrityksille

vuosittain paljon rahaa ja aikaa (Wood 2003). On laskettu, että jokaista 690 työntekijää kohden tarvitaan yksi täysipäiväinen IT-henkilö hoitamaan roskapostiasioita (Nucleus 2003).

3.4.7 Torjunnan ongelmia

Roskapostin torjuminen aiheuttaa myös ongelmia. *Estolistaus* (Blacklisting) eli tiettyjen sähköpostiosoitteiden tai palvelimien boikotoiminen on eniten käytettyjä tapoja vähentää roskapostia. Estolistalla ylläpidetään luetteloa roskapostia lähettävistä osoitteista ja näistä tulevat postit torjutaan täysin. Tämä tarkoittaa myös sitä, että kaikki näistä osoitteista tulleet kunnolliset, niin sanotut ei-roskapostit torjutaan samalla kertaa. Estolistauksen kanssa pitää olla erittäin tarkkana, sillä huolimattomasti käytettynä ne voivat estää huomattavaa määrää kunnollisia sähköpostiviestejä pääsemästä perille. Tämä uhka horjuttaa pahasti koko sähköpostin luotettavuutta. Ongelman tekee vakavaksi myös se, että käyttäjällä eli lopullisen viestin vastaanottajalla ei ole mitään sananvaltaa siihen, mitä estetään ja minkä takia. Roskapostin määritelmänhän tekee lopullisesti itse käyttäjä, joka sanoo mitä haluaa ja mitä ei halua vastaanottaa.

Myös postien suodattaminen aiheuttaa ongelmia. Liian tarkaksi viritetyt suodattimet syövät kunnollisia posteja ja nämä kadonneet postit voivat aiheuttaa huonoimmassa tapauksessa pahojakin ongelmia. Mitä parempia suodattimet ovat ja mitä vähemmän virheitä sattuu, sitä tuhoisampia ne ovat myös vahinkotilanteissa. (Ferris 2003.) Ongelmia voi syntyä myös silloin, kun suodatus tapahtuu palvelimentarjoajan päässä. Näin yksityisen käyttäjän sananvalta voi jäädä tässä torjuntamuodossa hyvin vähäiseksi. Käyttäjien on alistuttava palveluntarjoajien määritelmiin hyvästä ja kunnollisesta postista. Esimerkiksi tiettyjen poliittisten tai uskonnollisten viestien luokitteleminen roskapostiksi voi saada helposti valvonnan tai sensuurin muotoja.

Jatkuvasti yleistyvä suodattaminen on luonut myös uudenlaisia ja ennalta arvaamattomia ongelmia. Huolimatta siitä, että vain pieni osa kaikesta sähköpostiliikenteestä kulkee suodattimien läpi, on syntynyt joukko vaarallisia ”roskapostisanoja”. Näiden sanojen kuten ”viagra” tai ”sex” liiallinen käyttäminen saattaa tahattomasti leimata hyvää tarkoittavan, tärkeänkin viestin vaikuttamaan roskapostilta. Suodatuksen yleistyessä alkaa olla riskialtista käyttää sellaisia sanoja kuten ”subscribe”, jota käytetään paljon roskapostissa ja

postituslistoissa. Tällöin liian innokkaan suodatuksen ansiosta esimerkiksi uutislehdet eivät pääse perille.

3.4.8 Säädyttömät viestit

Varsinkin Yhdysvalloissa ollaan huolissaan roskapostin sisällön säädyttömyydestä tai moraalittomuudesta. Tällä tarkoitetaan aikuisviihdepalvelujen usein graafisia viestejä, jotka sisältävät hyvin rohkeaa kieltä. Yritykset ovat huolissaan työsähköpostiin ilmestyvistä seksiviesteistä, koska ne saattavat loukata työntekijöitä. Huoli on aiheellinen ainakin Yhdysvalloissa, jossa jopa oikeustoimet voivat uhata yhtiötä, joka ei pysty suojelemaan työntekijöitään loukkaavilta viesteiltä. (Wood 2003.)

Mielestäni suurempi ongelma kuin säädyttömät viestit on lapsille tuleva pornoroskaposti sekä muu lapsille sopimaton aineisto. Nykyään lapset alkavat käyttää sähköpostia yhä nuorempina, koulun ensimmäisistä luokista alkaen. Kouluissa kannustetaan lapsia käyttämään sähköpostia ja monet koulut antavat oppilailleen omat sähköpostiosoitteet. Roskapostittajat eivät katso kenelle viestejään lähettävät, ja siksi myös lapset saavat osansa pornoviesteistä.

3.4.9 Yksityisyys ja tietoturvaongelmat

Roskaposti aiheuttaa myös ongelmia yksityisyyden ja tietosuojan suhteen. Roskapostittajat keräävät suunnattoman suuria miljoonien osoitteiden osoitelistoja. Ongelma on se, että näitä tietoja kerätään, käytetään ja säilytetään ilman asianosaisen lupaa tai edes tietoa. Listoista saattaa lisäksi käydä ilmi, milloin ja mistä osoitteet on kerätty. Monien maiden lakien, kuten Suomenkin lainsäädännön mukaan tällainen listojen keräys on luvanvaraista.
(NOIE 2002; Puolamäki 2002.)

3.4.10 Lähetystietojen valheellisuus ja väärentäminen

Kuten Roskapostin ominaisuuksia -luvussa todettiin, yhtenä roskapostin piirteenä pidetään valheellisuutta, joka on myös yksi suurimmista roskapostin haitoista (NOIE 2002). Valheellisuutta ilmenee roskapostissa monella eri tavalla, joista viestien lähetystietojen väärentäminen on eräs esimerkki.

Roskapostin lähettäjien kannalta lähetystietojen väärentäminen on tärkeää, sillä se estää mahdollisten perille menemättömien viestien takaisin tulemisen. Roskaajien postituslistoissa on paljon virheellisiä, vanhoja tai muuten toimimattomia osoitteita, jotka saavat postipalvelimen lähettämään ilmoituksen takaisin viestin lähettäjälle. Tämä voi tarkoittaa suurimpien roskapostittajien kohdalla jopa miljoonia viestejä. Tällainen viestimäärän vastaanottaminen vaatisi isoja postipalvelimia, joissa on paljon tehoa ja vielä enemmän muistia sekä kovalevytilaa.

Sen sijaan silloin, kun viestien alkuperä on väärennetty, nämä viestit siirtyvät jonkun muun onnettoman sähköpostipalvelimelle eivätkä ne enää häiritse roskapostittajia itseään. Tästä seuraa se, että roskapostiviestien lähettäminen voidaan suorittaa kevyemmällä kalustolla. Samalla säästetään rahaa ja rahastahan roskapostituksessa on lopulta kuitenkin kyse. Suurimmat haitat tällaisesta toiminnasta syntyvät sille poloiselle palvelimelle, jonka nimeä roskapostittajat ovat käyttäneet. Tähän osoitteeseen tulevat sekä valitukset että ne viestit, jotka eivät löytäneet annettua osoitetta.

Toinen syy lähetystietojen väärentämiselle on se, että näin roskapostittajat pysyvät anonyymeinä. Samalla säästytään vihaisten roskapostinsaajien kyselyiltä ja valituksilta sekä – monissa maissa – poliisin vierailulta. Roskapostittamista kriminalisoidaan parhaillaan eri maissa. Tähän aiheeseen palaan myöhemmin tekstissä. Kolmas syy lähetystietojen väärentämiseen on toisen yrityksen luottamuksen hyväksikäyttö. Vastaanottaja lukee helpommin viestin, joka näyttää tulevan arvostetulta yritykseltä tai taholta.

Nimettömyyttä pidetään yllä myös viesteissä itsessään. Useimmissa roskaposteissa yhteystietoina on vain pelkkä sähköpostiosoite, Internetsivu tai puhelinnumero. Puhelinnumerossa vastaa yleensä automaattinen puhelinvastaaja, joka ottaa tilaukset vastaan. Viestissä ja sivuilla esiintyvät sähköpostiosoitteet ovat yleensä peräisin jostain ilmaisia sähköpostiosoitteita tarjoavasta yrityksestä ja ne lakkautetaan nopeasti postin lähetyksen jälkeen. Internetsivut ovat myös joko väärillä nimillä tai nimettömästi hankittuja eikä niissä ole sen parempia yhteystietoja kuin varsinaisessa roskapostiviestissäkään.

3.4.11 Kostotoimenpiteet

Niin sanotut kostotoimenpiteet (vigilante actions) ovat eräitä roskapostin lähettämisestä syntyviä haittoja. Näitä hyökkäyksiä voidaan pitää myös roskapostin torjuntakeinoina. Ihmisten turhautuminen purkautuu usein kiusantekona tai muunlaisena haitantekona roskapostittajia kohtaan. Ongelmaksi nousee yleensä se, että tämä kiusanteko tai jopa sabotointi ei aina rajoitu pelkästään roskapostittajiin, vaan kärsiä saavat myös sivulliset tai muuten syyttömät. Myöskään yleinen laittomuuksien tai arveluttavien keinojen käyttäminen ei ole hyväksyttävää edes roskapostittajia kohtaan. Turhautuneiden sähköpostinkäyttäjien ei kannata laskeutua samalle tasolle roskapostittajien kanssa.

Kostotoimenpiteisiin voidaan lukea myös estolistojen väärinkäyttö. Estolistoille laitetaan osoitteita, jotka eivät ole suoraan roskapostiosoitteita, mutta jotka ovat jonkin mutkan kautta yhteydessä roskapostin lähettäjiin. Tiedossa on myös tapauksia, joissa riitelevät osapuolet ovat lähettäneet toistensa sähköpostiosoitteen erilaisille mustille listoille pelkästään kostomielessä. Tällainen toiminta on edesvastuutonta, ja se aiheuttaa suurimmat haitat sähköpostin loppukäyttäjille. (Verisign 2003.)

3.4.12 Virukset ja roskaposti

Virukset liittyvät keskeisesti roskapostiongelmaan. Roskapostiviestit voivat sisältää viruksia tai muita vahingollisia ohjelmia. Nämä ohjelmat muuttavat saastuneen tietokoneen roskapostikoneeksi. Virus tutkii sähköpostiohjelman osoitelistat sekä lähettää viestin ohessa kopion itsestään kaikkiin listassa oleviin osoitteisiin. Näin virus leviää nopeasti ja samalla tuottaa huomattavat määrät roskapostia.

Itseään sähköpostin välityksellä levittävistä viruksista on olemassa myös kehittyneempiä muotoja, joita roskapostittajat ahkerasti käyttävät. Tällaiset virukset leviävät aivan kuten normaalit virukset mutta muuttavat saastuneen koneen roskapostittajille avoimeksi roskapostinlähetyspisteeksi.

3.4.13 Haittaohjelmat

Roskapostien välityksellä levitetään myös *soitto-ohjelmia* (dialer program). Roskapostissa saattaa olla linkkejä sivuille, jotka sisältävät ilmaista pornografiaa tai esimerkiksi mp3-

tiedostoja. Käyttäjän tarvitsee vain asentaa sivulta ladattava soitto-ohjelma. Maksuttomuus on näistä puheluista kaukana, sillä ohjelmat soittavat modeemilla johonkin, usein kaukaiseen maksulliseen numeroon. Käyttäjä katselee kauniita kuvia luullen olevansa yhteydessä edelleen omaan Internet-yhteyden ylläpitäjäänsä. Todellisuudessa puhelu ohjautuu toisaalle ja hinta voi olla jopa kymmeniä euroja minuutilta. Ohjelmat voivat myös käynnistää modeemiyhteyden automaattisesti esimerkiksi yöllä. Kiinteiden yhteyksien käyttäjillä nämä ohjelmat ottavat yhteyden palvelimeen, joka imee tiedostoja ja tietoja käyttäjän koneelta. (Sauver 2003.)

Roskapostittajat voivat yrittää saada käyttäjän lataamaa tietokonetta tutkivia *vakoiluohjelmia* (spy ware). Ohjelmat on usein naamioitu apuohjelmiksi tai hupiohjelmiksi kuten näytönsäästäjiksi tai pikku peleiksi. Vakoiluohjelma voi tulla myös toisen ohjelman kylkiäisenä tai vaikka viruksen tai madon mukana. Nämä ohjelmat ovat kotisivuilla, joihin roskapostissa olevat linkin viittaavat tai ne voivat jopa tulla liitetiedostoina sähköpostin mukana. Nämä ikävät pikku koodinpätkät tutkivat koneen läpikotaisin etsien esimerkiksi salasanoja tai roskapostittajien haluamia sähköpostiosoitteita. Kerätyt tiedot lähetetään vaivihkaa takaisin ohjelman lähettäjälle samalla kun esimerkiksi luet sähköpostisi tai surffaat netissä.

HTML-koodatut roskapostiviestit voivat sisältävät myös aktiivisia, pieniä, yhden kuvapisteen kokoisia kuvalinkkejä nimeltään ”web bug” tai ”Web beacon”. Nämä linkit aktivoituvat, kun viesti luetaan ja ne ilmoittavat linkin päässä olevalle sivulle, että viesti on luettu. Näin roskapostittajat pystyvät pitämään kirjaa kuinka paljon viestejä avataan tai kuinka paljon tietyn tyyppisiä viestejä pääsee läpi suodatinohjelmista. Näin nähdään myös onko kyseisessä sähköpostiosoitteessa elämää. Tätä tekniikkaa käyttävät myös kunnolliset sähköpostimainostajat selvittääkseen viestien avaus- tai lukemismääriä. (Aladdin 2003; Graham & Cumming 2003.)

3.5. Roskapostin historia

Roskapostin esinäytöksenä voidaan pitää vuonna 1975 sähköpostijärjestelmästä löydettyä virhettä. Keskuskone eli sähköpostipalvelin ei voinut kieltäytyä sille lähetetystä sähköpostiviestistä millään tavalla. Tämän huomion tehnyt Jon Postel kirjoitti tapauksesta raportin. Siinä hän mainitsi, että olisi hyödyllistä, jos keskuskone (sähköpostipalvelin) pystyisi estämään sille lähetetyt postit koneelta, jonka se uskoo olevan toimimaton tai jopa häiritsevä. Kukaan ei tehnyt asialle mitään kahdeksaantoista vuoteen.

Roskapostin esihistoriassa, 1980-luvulla ja 1990-luvun alkupuolella ketjukirjeet tai huonosti suunnitellut automaattiset vastausautomaatit aiheuttivat eniten ongelmia ja paheksuntaa sähköpostimaailmassa. Nämä ongelmat olivat enimmäkseen harmitonta ja johtuivat lähinnä huonosta suunnittelusta tai ajattelemattomuudesta.

Oikeat ongelmat alkoivat vuonna 1994, kun kaksi Arizonalaista asianajajaa, Laurence Canter ja Martha Siegel lähettivät yli kuuteentuhanteen uutisryhmään viestin, jossa mainostettiin lainopillisia neuvoja Green Card -arpajaisista kiinnostuneille siirtolaisille. Tämä massaviestitys aiheutti paljon puhetta ja paheksuntaa kahdesta syystä. Ensinnäkin se oli laajin yhden ja saman viestin massapostitus uutisryhmien historiassa, ja toiseksi, vaikka Green Card arpajaiset olivat ilmaiset, niin viestissä mainostetut palvelut eivät sitä olleet. Kymmenet tuhannet Usenetin käyttäjät valittivat tästä parivaljakon Internet-palveluntarjoajalle. Tämä viestien paljous tukki ja lopulta kaatoi palvelimen. Tästä kaikesta hälinästä vihastunut palveluntarjoaja irtisanoi asianajajien liittymän. Sittemmin nämä kirjoittivat kokemuksistaan kirjan nimeltä ”Miten rikastua tiedon valtatiellä” eli *How to Make a Fortune on the Information Superhighway* (Canter & Siegel 1994).

Seuraavana vuonna 1995 päätti ”Miten rikastua tiedon valtatiellä” -kirjan lukenut Jeff Slaton kokeilla, pystyykö sähköpostimainonnalla todella ansaitsemaan rahaa. Hän alkoi Canterin ja Siegelin ohjeiden mukaan kerätä ihmisten sähköpostiosoitteita ja Usenet-ryhmien nimiä. Slaton kysyi palveluntarjoajaltaan lupaa massapostittaa mainoksia omalta sähköpostitunnukseltaan. Kun tämä ei sopinut palveluntarjoajalle, Slayton irtisanoi sopimuksensa ja kun tunnuksen sulkeutumiseen oli enää kaksi päivää aikaa, hän massapostitti

mainoksensa maailmalle. Koko operaatio maksoi Slaytonille 18 dollaria ja hän myi mainostamaansa tuotetta tuhansia kappaleita ympäri maailmaa. Myöhemmin roskapostikuninkaaksi itseään nimittänyt Slayton keksi monia nykyäänkin roskapostittajien käytössä olevia tekniikoita kuten väärennetyt lähetysosoitteet. Hän käytti myös erillistä ohjelmaa massapostituksen lähettämiseen ja vähentääkseen valituksia hän väitti ylläpitävänsä listaa sähköpostiosoitteista, jotka eivät haluaisi vastaanottaa hänen mainoksiaan.

Vuonna 1996 nousi roskapostiareenalle uusi nimi Sanford Wallace, joka syrjäytti roskapostikuningas Slaytonin Cyber Promotions -yrityksensä avulla. Wallace nosti roskapostittamisen vielä tehokkaammaksi liiketoiminnaksi kuin Slayton. Wallace käytti erittäin nopeaa T1-linjaa, kun Slayton oli käyttänyt modeemiyhteyttä. Wallace otti käyttöönsä oman verkkotunnuksen nimeltään ”cyberpromo.com” ja sanoi haluavansa laillistaa massasähköpostimainonnan. Hän otti maalikseen suuren amerikkalaisen yhteydentarjoajan nimeltään America Online (AOL) ja sen miljoonat käyttäjät. Wallace oli kerännyt miljoonien sähköpostiosoitteiden listat ja alkoi pommittaa niitä viiden ja kuuden viestin päivävauhdilla. Nämä mainokset sisälsivät esimerkiksi nykyäänkin tuttuja laihdutusneuvoja tai ”helppoa rahaa” -ilmoituksia. Tämä aiheutti suurta ärtymystä AOL-asiakkaiden keskuudessa ja yritys joutui perustamaan roskapostisuodattimen, jolla Wallacen postitukset voitaisiin estää. Wallace ei tästä luovuttanut vaan päätti kiertää suodattimet toisin keinoin. Hän sanoi tehneensä sopimuksen 50 Internet-yrityksen kanssa heidän T1-yhteydensä vuokraamisesta. Nyt Wallace pystyi vaihtamaan lähetysosoitettaan tarpeen mukaan ja ohittamaan näin AOL-suodattimet jatkossakin.

Seuraavien vuosien aikana Wallace taisteli useita oikeustaisteluita. Tästä huolimatta hänen yrityksensä pysyi voitollisena. Vuonna 1997 Wallace ilmoitti, että Cyber Promotionilla on yli 11 000 asiakasta. Hyvin jatkunut roskapostittajan ura katkesi kuin seinään, kun hänen Internet-yhteyden toimittajansa AGIS irtisanoi T1-linjan. Yritys oli tiennyt jo vuosia Wallacen harrastaneen massapostitusta. Itse asiassa AGIS oli toiminut muidenkin roskapostittajien palveluntarjoajana, ja vasta kun yritys itse joutui roskapostitusta vastustavien tahojen hyökkäyksen kohteeksi, se päätti lopettaa yhteystyön kaikkien roskapostittajien kanssa. Wallacen taru roskapostikuninkaana oli ohi. Tämä ei kuitenkaan vähentänyt roskapostin määrää ihmisten postilaatikoissa, sillä tässä vaiheessa roskapostittamisesta oli

tullut kaikkien oikeus ja sadat elleivät tuhannet yritykset olivat valinneet sen toimenkuvakseen. (Schwartz & Garfinkel 1999.)

4. Roskapostin torjunta

Tässä luvussa esittelen erilaisia tapoja estää, vähentää tai edes hiukan rajoittaa roskapostin syöksyä postilaatikkoihimme. Torjuntamenetelmiä on paljon ja ne eroavat toisistaan selvästi. On olemassa teknisiä ja ohjelmallisia ratkaisuja, joihin kuuluvat erilaiset suodattimet, mustat ja valkoiset listat, erilaiset postimaksujärjestelmät ja postin lähettäjän tunnistus tai varmistus -ohjelmistot. Toinen torjuntakeinojen pääryhmä ovat hyvät tavat ja käytännöt. Tähän ryhmään kuuluvat kaikki toimet, joiden avulla jokainen käyttäjä voi vähentää roskapostin määrää ja vähentää roskapostin haittaavuutta jokapäiväisessä elämässä.

4.1. Torjuntakohta

Torjuntaohjelmistot voivat sijaita sähköpostiketjun kolmessa eri kohdassa. Käyttäjän omalla koneella eli käyttäjäpuolella toimivat ohjelmat käsittelevät ja tutkivat sähköpostit ennen kuin ne ilmestyvät sähköpostiohjelmaan. Sähköpostipalvelujen tarjoajan päässä eli palvelin-puolella toimivat ohjelmat tutkivat sähköpostit ennen kuin ne talletetaan käyttäjän sähköpostilaatikkoon palvelinkoneella. Torjuntaohjelmat voivat toimia myös kolmannen osapuolen palvelinkoneilla, jonne otetaan yhteyttä joko käyttäjän toimesta eli asiakaspäästä tai sitten postipalvelun ylläpitäjän toimesta eli palvelinpäästä. Nämä kolmansien osapuolten palvelut ovat yleensä varmennus- ja tunnistusohjelmia, mustia listoja tai sormenjälkisuotimia.

Torjuntaohjelman sijainti vaikuttaa paljonkin ohjelman käyttöön ja siihen liittyviin mahdollisiin ongelmiin. Roskapostin määrittelee viime kädessä käyttäjä itse. Tämän periaatteen mukaan palvelintasolla olevat suotimet ovat vähintään arveluttavia, ainakin jos ne poistavat postin suoraan. Tällöin roskapostin määritteleminen siirtyy pois käyttäjältä ja jonkun toisen käsiin. Tämä tilanne voi johtaa kärjistyneessä tilanteessa sensuuriin tai ”isoveli valvoo” -tilanteeseen: joku toinen kun sinä itse päätät, mikä on kunnollista, ei-roskapostia ja samalla sellaista postia, joka sinulle näytetään. Samat ongelmat sisältyvät myös kolmansien osapuolten tarjoamiin järjestelmiin.

4.2. Yhteistyö ja yhteisöllisyys

Kolmansien osapuolten ohjelmistoissa voidaan käyttää niin sanottuja yhteisöllisiä menetelmiä. Tällä tarkoitetaan tilannetta, jossa yhteisö yhdessä päättää, mikä on roskaa ja mikä ei. Tämä tilanne tulee esille esimerkiksi mustissa listoissa tai joissain suodatinmenetelmissä. Yhteisön sisältä kerätään tietoa siitä, millaista roskapostia sen käyttäjillä liikkuu ja sen mukaan suoritetaan luokittelu roskan ja ei-roskan välillä. Tämä on toisaalta paljon parempi ja turvallisempi tapa kuin yhden ihmisen tai tahon päätös siitä, mitä roska on. Näin saadaan paljon suurempi otos maailmalla liikkuvasta roskapostista ja roskan tunnistaminen helpottuu. Huonona puolena yhteisöllisessä roskapostin torjunnassa on se, että yksilöiden erilaisia tarpeita tai mielipiteitä roskapostin luonteesta ei huomioida. Roskapostin lopullisen määritelmän tekee normaalisti viestin vastaanottaja, mutta tässä mallissa päätöksen tekee yhteisö. Tämä tarkoittaa pahimmassa tapauksessa sitä, että jokin mainos tai posti jää tulematta, vaikka haluaisitkin, koska yhteisö on päättänyt sen olevan roskaa. Monien mielestä tämä on pieni hinta siitä parantuneesta suodatustehosta, mitä yhteisölliset suodattimet tai mustat listat tuovat. (Cunningham et al. 2003; Hird 2002.)

4.3. Suodattimet

Sähköpostisuodattimet (filters) ovat ohjelmia, jotka luokittelevat sähköposteja roskaposteiksi ja kunnolliseksi, halutuksi postiksi. Suodatinohjelmat käyttävät monia erilaisia tekniikoita, joilla muodostetaan päätös roskasta. Tekniikat voidaan jakaa kolmeen eri ryhmään: sääntöpohjaisiin, tilastollisiin ja tunniste- tai sormenjälkitekniikoihin. Lisäksi voidaan tuoda esiin aktiiviset hyökkäävät suodattimet, jotka suodatuksen ohella aiheuttavat roskapostin lähettäjälle muita hankaluuksia.

4.3.1 Sääntöpohjaiset suodattimet

Sääntöpohjaiset suodattimet ovat tänä päivänä eniten käytettyjä roskapostinestosuotimia. Sääntöpohjaisten järjestelmien sydän on joukko sääntöjä, joiden pohjalta tunnistetaan, onko kyseessä roskaposti vai ei. Yksinkertaisin muoto tästä on systeemi, jossa sähköpostiviesti,

otsikko ja varsinaisen viestin kaikki sanat käydään läpi ja etsitään sopivia roskapostisanoja. Sitten kun tällainen sopiva roskapostisana löydetään, viesti tuomitaan suoraan roskapostiksi. Käyttäjä voi lisätä sanoja sen mukaan, millaisia sanoja hänen roskaposteissaan yleensä käytetään, vaikkapa *porn*, *sex* tai *viagra*. Tässä hyvin yksinkertaisen ja helposti toteutettavan suodattimen selvänä huonona puolena on se, että se saa kyllä haaviinsa huomattavan määrän roskaposteja, mutta sen kyky erottaa omat vihollisesta on hyvin huono. Pelkkä sanan viagra mainitseminen sähköpostissa saa sen muuttamaan muuten asiallisen jutun kaverilta roskapostiksi. Suodattimen aiheuttama haitta on helposti varsinaista roskapostia suurempi, jos näin yksinkertaista ohjelmaa käytetään siten että kaikki roskapostiviestit tuhotaan suoraan. Haitta on edelleen huomattava, vaikka roskapostien poistamisen sijaan viestit ohjattaisiin roskapostikansioon: käyttäjä joutuisi selaamaan roskakansiotaan päivittäin siinä hyvin todennäköisessä pelossa, että suodatin olisi tehnyt virheen.

Paranneltu versio edellisestä on malli, jossa avainsanoille annetaan painoarvoja sen ”roskaisuuden” mukaan. Esimerkiksi sana viagra olisi kymmenen pisteen arvoinen ja sana penis taas lisäisi 50 pistettä loppusummaan. Näin käydään viestin kaikki sanat läpi ja lasketaan sähköpostiviestin lopullinen roskapostiarvo. Tämän jälkeen tarkastetaan, ylittääkö näiden sanojen yhteenlaskettu summa tietyn ennalta määrätyn rajan. Rajan ylittyessä viesti luokitellaan roskaksi. Tällainen pisteenlaskumenetelmä ei ole yhtä kankea ja mustavalkoinen kuin sen ”kerrasta poikki” -pikkuveljensä. Kaikesta huolimatta kaverin lähettämä artikkeli voi hyvinkin sisältää tarpeeksi monta kiellettyä sanaa; taas roskapostikansio täyttyy, vaikka viesti olisi kaukana roskasta. Vaikka tällä menetelmällä saadaan roskaposteja hyvin kiinni, niin kunnollisten postien määrä roskakorissa on yleensä aivan liian suuri.

Tekniikkaa on paranneltu edelleen, jolloin viestin sisällön tutkimukseen otetaan mukaan myös ”hyvät” sanat. Huonojen roskasanojen lisäksi tässä menetelmässä annetaan positiivisia pisteitä sellaisille sanoille, joita roskaposteissa ei yleensä ilmene, kuten perhe tai vaikkapa lapsi. Nyt pitkä kirje äidiltä sisältää tarpeeksi ”hyviä” sanoja, jotta muutamat huonot roskasanat eivät enää tuomitse kirjettä roskaksi. Samanlaisia ”avainsanoja” voidaan metsästää myös otsikosta tai jopa sähköpostiviestin lähettäjän osoitteista. Näin voidaan suodattaa posteja, joilla on muita helposti tunnistettavia piirteitä kuten esimerkiksi lähettäjän tai yrityksen nimi.

Sääntöpohjaisten suodattimien teho on noin 90-95 % (Graham 2003b). Vääriä hälytyksiä eli roskapostiksi tuomittuja kunnollisia posteja ei synny enää juuri ollenkaan, joskin kaikki riippuu siitä, millaisia sääntöjä suotimessa käytetään. Nyrkkisääntönä voidaan todeta: mitä tiukemmat ja kattavammat säännöt sitä enemmän roskapostia saadaan kiinni, mutta samalla sivullisten uhrien määrä lisääntyy eli roskaksi tuomitaan yhä useampi kunnollinen posti.

Sääntöpohjaisten suotimien suurin heikkous on niiden staattisuus. Roskaposti on jatkuvasti muotoaan muuttava ja kehittyvä vastustaja. Tällöin muuttumattomat jäykät säännöt voivat muuttua tehottomiksi hyvinkin nopeasti. Tämän voi toki kiertää päivittämällä niitä sitä mukaa, kun uusia roskapostimuotoja ilmenee. Se taas vaatii paljon aikaa ja osaamista, jota peruskäyttäjällä tuskin on. (Hird 2002; Trudeau 2003.)

4.3.2 Tilastolliset suodattimet

Tilastolliset suodattimet ovat uusin ja tällä hetkellä tehokkain tapa suodattaa roskaposteja. Tilastolliset menetelmät perustuvat roskaposteissa ja ei-roskaposteissa esiintyvien sanojen tai kirjainyhdistelmien tilastolliseen esiintymiseen. Kuinka monessa roskapostissa käytetään sanaa ”viagra” suhteessa siihen, kuinka monessa kunnollisessa sähköpostiviestissä sana ilmenee. Tai päinvastoin: kuinka monessa kunnollisessa roskapostissa sana ”perhe” ilmenee verrattuna roskaposteihin. Tämä vertailu tehdään jokaiselle sähköpostiviestin sanalle tai merkkijonolle ja tulokseksi suodatin antaa todennäköisyyden sille, kumpaan joukkoon viesti kuuluu.

Tilastollisen suodattimen suurin vahvuus kehittyneimpiinkin sääntöpohjaisiin suodattimiin verrattuna on sen kyky oppia tunnistamaan roskapostia. Tilastollinen laskutoimitus perustuu suodattimen läpikäymiin ja tutkimiin viesteihin eikä ennalta annettuihin sanoihin, kuten sääntöpohjaisissa suotimissa. Suodatinta opetetaan aluksi mahdollisimman suurella joukolla ennalta määriteltyjä, tunnettuja ja varmistettuja roskaposteja. Tämän jälkeen sille syötetään suuri ja mahdollisimman monipuolinen joukko kunnollisia posteja. Tämän jälkeen suodatin oppii, millaisia posteja käyttäjä saa ja kuinka ne sijoittuvat roskaposti – kunnollinen posti -akselilla. Tämän alustavan opetuksen jälkeen filtteri oppii jokaisesta läpikäymästään viestistä lisätietoa siitä, millainen juuri tämän käyttäjän roskaposti tai kunnollinen posti on. Jos

suodatin tekee virheen ja päästää roskapostin ilmestymään postilaatikkoosi tai peräti laittaa kunnollisen postin roskalaatikkoon, voidaan suodinta ojentaa ja kertoa, että kyseinen posti ei ollut roskaa vaan kunnollinen posti, tai toisinpäin. Seuraavalla kerralla suodin ei enää tee samaa virhettä.

Tämän suotimen oppimiskyky auttaa myös sääntö- tai sormenjälkisuotimia haittaavaan ongelmaan eli roskapostin muuttuvuuteen. Roskaposti muuttuu koko ajan. Viestien sisällöt muuttuvat ja niiden esitystavat vaihtuvat, koska roskapostittajat pyrkivät tekemään roskaposteistaan suotimille näkymättömiä. Tämä muutos voi ajaa muut suotimet vääriin tuloksiin, mutta tilastolliset suotimet oppivat itsestään miten roskaposti muuttuu ja pysyvät jatkuvasti tilanteen tasalla.

Tilastolliset suotimet selviytyvät myös monista roskapostittajien kehittämistä, yleensä sääntöpohjaisille tai sormenjälkisuotimille tarkoitetuista tempuista. Kaikki sellaiset, lisäykset joita ei normaaleissa posteissa ilmene, ovat häiritsemisen sijaan parempia roskapostin tunnusmerkkejä. Esimerkiksi satunaisten kirjainyhdistelmien lisääminen tai väärinkirjoittaminen – ellei sinulla ole todella pahasti lukihäiriöisiä ystäviä – lisäävät roskapostin ja normaalin kunnollisen postin välille syntyvää eroa. Toki normaalin tekstin kuten kirjan kappaleen lisääminen viestiin voi siirtää viestin kunnollisten viestien joukkoon. Tämän kaltainen toiminta ei ole vielä yleistä, mutta yleistyessään se voi tuoda mukanaan uuden ongelman. Roskapostien täytesanoina paljon käytetyt sanat alkavat saada suotimen sisällä roskapostimerkityksiä. Tähän antavat viitteitä kertomukset, kuinka esimerkiksi sanaa ”subscribe” ei voida enää käyttää turvallisesti sähköpostitse jaettavissa lehdissä tai posteissa (Fontana 2002). Tämä sana yhdessä muiden vähän kyseenalaisten sanojen kanssa saattaa tuomita kunnollisen viestin roskaksi. Sama ongelma esiintyy myös sääntöpohjaisissa suotimissa, joskin tilastollisissa se pysyy piilossa suotimen sisällä, kun sääntöpohjaisissa se on kaikkien luettavissa listoilta. Tilastollinenkaan menetelmä ei ole lopullinen keino roskapostin estämiseksi.

Muita tilastollisten suotimien heikkouksia ovat niiden suhteellisen kovat laitevaatimukset. Tilastolliset laskutoimitukset vaativat paljon laskutehoa jokaista sähköpostitiliä kohden. Ne vaativat jonkin verran kovalevytilaa tiedoille, joiden avulla päätökset viestien

roskapostisuudesta tehdään. Kotikoneilla tämä ei tuota minkäänlaisia ongelmia, mutta näiden kahden vaatimuksen takia se ei sovellu palveluntarjoajien isojen palvelimien suodattimeksi. Sähköpostipalveluiden tarjoajilla voi olla miljoonia sähköpostitilejä, joten kaikkien niiden postien läpikäyminen tilastollisilla suodattimilla olisi liian hidasta ja vaatisi aivan liian paljon kovalevytilaa käyttäjää kohden. (Graham 2003b; Trudeau 2003.)

4.3.3 Sormenjälkisuodattimet

Sormenjälkisuodattimien toimintaperiaate on luoda jokaisesta tavatusta roskapostista sormenjälki eli yksilöllinen tunniste. Tällä tunnisteella pystyttäisiin tunnistamaan kaikki täsmälleen samanlaiset roskapostit helposti ja nopeasti. Tätä menetelmää käytetään virustorjunnassa ja se on todettu hyvin tehokkaaksi sekä nopeaksi tavaksi löytää viruksia. Roskapostin suhteen sormenjälkitunnistus ei ole kuitenkaan kovin tehokas menetelmä. Jokainen uusi roskaposti pitää huomata ja tunnistaa ennen kuin sitä voidaan estää. Vaikka roskaposteja lähetetään suurissa erissä, erilaisia roskaposteja on lukuisia ja uusia roskaposteja sekä vanhojen variaatioita syntyy jatkuvasti lisää. Uuden tyyppisten roskapostien keräämistä on pyritty tehostamaan perustamalla niin sanottuja *roskapostiansoja* eli sähköpostiosoitteita, joiden tarkoitus on vain kerätä liikkeellä olevia roskaposteja. Lisäksi roskapostittajat ovat pyrkineet estämään sormenjälkien käytön lisäämällä satunnaisia merkkijonoja roskaposteihin, jolloin vanhat sormenjäljet eivät enää tunnista niitä. (Graham 2003b; Trudeau 2003.)

4.3.4 Rankaisusuodattimet

Idea suodattimista, jotka suodattamisen lisäksi aloittavat jonkin tasoisen vastahyökkäyksen roskapostittajia kohtaan, on suhteellisen uusi. Tällaisissa *rankaisusuodattimissa* pyritään kasvattamaan roskapostittajien kuluja ja muuttamaan roskapostin kulurakennetta. Etenkin mainosroskaposteja lähetetään järjettömän suuria määriä, koska niiden vastausprosentti on todella pieni. On esitetty arvioita, että roskapostin vastausprosentti voi olla niinkin alhainen kuin 1/100 000 ja postittaminen on vielä kannattavaa (Westley 2003). Suuret postimäärät nostavat saatujen vastausten määrät kannattaville tasoille, eli roskapostittajan silmin suuret lähetysmäärät takaavat tarpeeksi suuren reagointiprosentin viestiä kohden. Rangaistussuodattimissa nämä roskapostin suuret lähetysmäärät käännetään roskaajia vastaan esimerkiksi lähettämällä vastaviesti jokaista saatua roskapostia kohden.

Toinen ehdotettu malli on se, että suodatinohjelma käy automaattisesti läpi jokaisen roskapostissa mainitun linkin useita kymmeniä tai satoja kertoja. Jos tarpeeksi monta suodatinta tekisi samoin ja kävisi samoilla sivuilla yhtä aikaa, niin mainostajien sivujen toiminta häiriintyisi ja ne voisivat jopa kaatua kasvavan liikenteen seurauksena. Molemmat hyökkäykset suoritettaisiin ainoastaan tunnettuja ja listattuja roskapostittajia ja heidän sivustoja kohtaan. Tällöin perustettaisiin listoja sellaisista sivuista, jotka ”ansaitsevat” tulla hyökätyksi, samaan tapaan kuin nyt ylläpidetään mustia listoja roskapostittajista, joilta ei enää kannata vastaanottaa postia.

Nämä rangaistussuodattimet ovat vielä idean asteella. Roskapostimäärien noustessa ja ihmisten turhautuneisuuden lisääntyessä voivat tämän tyyppiset suodattimet toteutua piankin. (Graham 2003a; 2003b.) Rangaistusuotimiin liittyy paljon ongelmia. Mielestäni tällainen ”tulella tulta vastaan” -ajatusmalli ei ole kovin järkevä eikä kestävä ratkaisu roskapostin hillitsemiseksi. Ongelmia syntyy esimerkiksi lisääntyneestä liikenteessä: jos jokaista roskapostia vastaan tulisi vielä yksi ”hyökkäysviesti”, niin liikenteen kasvu olisi huomattava. Verkkoliikenteen kasvua pidetään yhtenä roskapostin suurista haitoista, jolloin lisäliikenteen luominen tuskin lienee toimiva ratkaisu. Toisen ongelman aiheuttavat listat, joilla pyritään estämään hyökkäyssuotimen väärinkäyttö. Mustien listojen tai muiden estolistojen käytössä on esiintynyt ongelmia (ks. Fontana 2002). Mikä estää samanlaisten sivullisten uhrien syntymistä myös hyökkäyssuotimien listojen kanssa?

4.4. Listat

On olemassa kahden tyyppisiä roskapostilistoja, *mustia* ja *valkoisia*. Listat ovat toiminnaltaan toistensa vastakohtia. Mustat listat estävät tai poissulkevat siinä listatut nimet tai osoitteet; valkoiset listat hyväksyvät ainoastaan listalla olevat osoitteet.

4.4.1 Mustat listat

Mustat listat ovat sulku- tai estolistoja. Jos sähköpostin lähtöosoite, ip-osoite tai sähköpostiosoite löytyy näiltä sulkulistoilla, sen perillemeno estetään ja viesti tuhotaan. Mustalle listalle joutuvat roskapostittajat, roskapostittajien yhteistyökumppanit, avoimet

sähköpostipalvelimet tai reitittimet (relay) riippuen sulkulistan politiikasta tai tarkoituksesta. Mustat listat ovat joko sähköpostipalvelimen ylläpitäjän itsensä keräämiä tai sitten muilta ostettuja tai saatuja kolmansien osapuolten listoja. (Hird 2002.) Itse kerättyjen sisäisten listojen etu on siinä, että niitä voidaan kontrolloida paremmin ja hoitaa tehokkaammin kuin kolmansien osapuolten listoja (Aladdin 2003).

Kolmansien osapuolten listat jaan kahteen ryhmään, nopeisiin ja hitaisiin listoihin. Nopeat listat päivittyvät reaaliajassa tai lähes reaaliajassa. Näihin listoihin lisätään ja niiltä poistetaan osoitteita hyvin nopeassa tahdissa. Tällaiset listat yrittävät pysyä nopeasti paikkaansa vaihtavien roskapostittajien vauhdissa toimimalla itsekin nopeasti. Käytännössä osoitteita laitetaan listaan ilman tarkastusta tai lyhyen selvityksen jälkeen, listanpitäjälle tulleiden ilmoitusten mukaan. Lisääminen on usein automaattista, jolloin ihminen ei tarkista listalle meneviä osoitteita. Tämä lisää virheiden määrää ja virheellisten osoitteiden joutuminen estolistoille on helppoa. Estolistoilta pois pääseminen ei ole enää yhtä nopea ja vaivaton prosessi. Esimerkkinä Spamhaus Block List SBL (Spamhause 2004) tai SpamCop (SpamCop 2003).

Hitaat mustat listat toimivat harkitummin ja käyttävät enemmän aikaa listan lisäyksiin. Jokainen ehdokas tutkitaan tarkkaan ennen kuin nimi lisätään listalle. Kyseisen ip-osoitteen omistajaan otetaan etukäteen yhteyttä, jolloin tämä voi todistaa syyttömyytensä ennen listalle joutumista. Näin väärien tuomioiden määrä pienenee ja listan ”puhtaus” pysyy parempana. Esimerkki hitaasta estolistasta on MAPS RBL (Mail-Abuse 2002). Listojen tehokkuus roskapostin estäjinä perustuu siihen ajatukseen, että suurin osa roskapostista tulee samasta paikasta. Listoissa listataan esimerkiksi ip-osoitteita, joista tiedetään tulleen tai tulevan paljon roskapostia. Mustissa listoissa voidaan listata myös avoimia sähköpostin välittäjiä tai tunnettuja roskapostittajien tukijoita tai yhteistyökumppaneita.

Mustien listojen suurin heikkous on niiden ehdottomuus ja sokeus. Kaikki tietystä osoitteesta tulevat postit ovat roskaa. Myös kaikki tästä osoitteesta lähtevät kunnolliset postit häviävät bittiavaruuteen. Kunnollisten viestien estäminen on nousemassa isoksi ongelmaksi yhä kovenevassa roskapostisodassa. Monia yksityisiä henkilöitä, yrityksiä sekä muita onnettomia

ja syyttömiä tahoja on lisätty toistuvasti estolistoille. Tunnettuja esimerkkejä tästä ovat NetAction (ks. Olsen 2002) ja Whirlycott.net (ks. Bray 2003).

4.4.2 Valkoiset listat

Valkoiset listat ovat nimensä mukaisesti mustien listojen vastakohtia. Mustat listat estävät listalla olevista osoitteista tulevat postit päästäen muut läpi, mutta valkoinen lista päästää läpi vain listalla olevista osoitteista tulevat postit ja tuhoavat muuta. Valkoisia listoja ei käytetä yleensä samalla tavalla yhteisinä listoina vaan enemmän henkilökohtaisina roskapostintorjunnan menetelminä. Suuret sähköpostin tarjoajat ovat viime aikoina alkaneet tarjota valkolistapalveluja myös ilmaisten sähköpostiosoitteiden käyttäjille. Erona perinteiseen valkoinen lista –periaatteeseen on, että normaalisti tuhottavaksi menevät, tuntemattomista osoitteista tulevat sähköpostit siirtyvätkin muiden roskapostin estomenetelmien, yleensä suodattimien hampaisiin. Siellä määritetään, onko kyseinen viesti roskaa vai ei. (Aladdin 2003; Hird 2002.)

4.5. Postimaksujärjestelmät

Postimaksujärjestelmien ajatus on luoda eräänlainen sähköinen postimerkkijärjestelmä sähköpostiin. Sähköinen merkki voisi maksaa joko rahaa tai mahdollisesti laskentatehoa ja koneaikaa, jotka tietokonemaailmassa ovat yhtä kuin raha. Rahalla ostettavat merkit voisivat olla hyvinkin samankaltaisia kuin normaalit etanapostin postimerkit. Käytännössä tämä tarkoittaa, että maksat joitain senttejä tai sentin murto-osia jokaisesta lähetetystä postista. Toinen vaihtoehto olisi käyttää rahaa jonkinlaisena panttina. Käytännössä tämä tarkoittaa sitä, että maksat jokaisesta lähetetystä postituksesta tietyn summan rahaa. Pantti palautetaan takaisin viestin lähettäjälle, mikäli viestin vastaanottaja ei ilmoita tietyn ajan kuluessa viestin olevan roskapostia. Näin sähköposti pysyy maksuttomana tavalliselle käyttäjälle, mutta muuttuu liian kalliiksi roskapostittajalle.

Tämä torjuntamenetelmä perustuu siihen aikaisemminkin mainittuun seikkaan, että roskapostittaminen on erittäin halpaa ainakin normaaliin postiin verrattuna. Torjuntamenetelmän perusidea olisi, että jokaisella lähetetyllä sähköpostilla olisi jokin maksu.

Maksu voisi olla hyvin pieni, normaalille käyttäjälle olematon summa rahaa. Tämä mitätön summa alkaa kasaantua nopeasti, kun puhutaan miljoonista tai sadoista miljoonista lähetetyistä sähköposteista, joita roskapostittajat lähettävät. Näin pystytään siirtämään sähköpostin kulurakennetta pois vastaanottajalta kohti lähettäjää.

Ajan eli laskentatehon käyttäminen maksuvälineenä perustuu vaikeisiin ja aikaa vieviin laskutoimituksiin. Näiden laskujen tuloksista muodostetaan jonkinlainen leima tai ”postimerkki”, jonka avulla sähköpostiviesti tunnistetaan ei-roskapostiksi. Tekniikan ideana on se, että normaali sähköpostinkäyttäjä pystyisi laskemaan laskutoimitukset nopeasti, sekunnin murto-osissa. Sen sijaan miljoonia posteja lähettävä roskapostittaja joutuisi odottamaan tunteja tai päiviä laskutoimitusten valmistumista. (Kraut 1999.)

Näissä postimerkkimenetelmissä on kuitenkin ongelmia alkaen rahankäytöstä Internetissä. Tällä hetkellä ei ole yhtään menetelmää, jolla voitaisiin kerätä ihmisiltä pieniä summia rahaa ilman suuria käsittelykustannuksia. Ongelmia aiheuttavat myös roskapostittajilta kerätyt postimaksut. Kuka kerää rahat ja kuka päättää, kenelle kerätyt varat annetaan? Menevätkö ne roskapostia saaneille henkilöille, roskapostia saaneiden henkilöiden palvelimille vai aivan muualle? Toinen suuri ongelma on se, että tämänkaltainen systeemi vaatisi koko nykyisen sähköpostijärjestelmän vaihtamista toiseen. Ei ole olemassa nykyisen järjestelmän päälle liimattavaa rajapintaa, joka mahdollistaisi tämän kaltaiset toiminnot.

4.6. Lähettäjän tunnistus ja varmennus

Sähköpostin kasvottomuutta ja nimettömyyttä on pidetty yhtenä sähköpostin suurimmista eduista. Tämä seikka on lopulta mahdollistanut myös sähköpostin suurimman haitan ja vitsauksen, roskapostin. Ratkaisuna tähän on esitetty monia erilaisia sähköpostin lähettäjän tunnistuksen tai varmennuksen menetelmiä. Tapoja on kahta päätyyppiä. Erillisen ohjelman tai palvelun avulla käyttäjät voivat varmistaa lähettäjän olevan ihminen eikä roskapostiautomaatti ja varmistua tämän aikeiden kunnollisuudesta. Toinen tyyppi on radikaalimpi ja perusteellisempi: SMTP-protokollaan tehdään muutos tai lisäys. Sen avulla jokainen sähköpostin lähettäjä voitaisiin tunnistaa eli jäljittää siihen ip-osoitteeseen, josta

viesti on lähetetty. Tämä lähettäjän varmennus tekisi mahdottomaksi lähettää postia nimettömänä ja salassa, jolloin roskapostittajat saataisiin jäljitettyä. (Graham 2003b.)

4.6.1 Lähettäjän varmennus

Sähköpostin lähettäjien varmennuspalveluja on olemassa monia ja niiden toimintaperiaatteet ovat samat: tarkoitus on tehdä mahdottomaksi tai ainakin vaikeammaksi lähettää nimetöntä tai suuria määriä postia. Sähköpostiviestin tullessa käyttäjän sähköpostiohjelmaan tai sähköpostipalvelimelle ohjelma lähettää kysymyksen viestin lähettäjälle. Siinä pyydetään varmistamaan, että viesti oli todella lähettäjän lähettämä. Kun viestin lähettäjä on vastannut viestiin, alkuperäinen viesti päästetään käyttäjän sähköpostilaatikkoon. Tämän lisäksi lähettäjän sähköpostiosoite lisätään ohjelman ylläpitämään valkoiseen listaan, jolloin tämän varmennetun ihmisen lähettämät viestit ohittavat seuraavilla lähetyskerroilla varmennusjärjestelmän. Jos postiin ei saada vastausta tiettyyn aikaan mennessä, viesti joko tuhotaan tai siirretään erilliseen kansioon. Nämä hylätyt postit voidaan ajaa ensin toisten roskapostinestojärjestelmien kuten suodattimien tai mustien listojen läpi. Lopuksi, jos viesti, todetaan olevan kunnollinen, sen annetaan siirtyä käyttäjän postilaatikkoon. Tämän jälkeen hyväksytyn viestin lähettänyt henkilö lisätään valkoiseen listaan, jolloin kaikki samalta henkilöltä lähetetyt viestit ohittavat suodattimet sekä muut tarkastukset ja menevät suoraan vastaanottajan sähköpostikansioon.

Tarkistusviesteissä voi olla myös kysymyksiä tai tehtäviä, joilla pyritään varmentamaan, että viestiin vastaa todella ihminen eikä tietokone. Mahdollinen automaattinen vastausohjelma voisi tehdä tästä tekniikasta nopeasti hyödyttömän ja lisäisi huomattavasti sähköpostiliikennettä. Silti tämä on erittäin tehokas menetelmä roskapostin kitkemiseksi. Yksikään massaroskaposteja lähettävä ihminen ei kykenisi lähettämään vastauksia kaikkiin lähettämiinsä viesteihin siinäkään harvinaisessa tapauksessa, että olisi vielä samassa osoitteessa postituksen jälkeen.

Lähettäjän varmennus ei ole kuitenkaan ongelmaton roskapostin estotapa. Järjestelmä ei aiheuta mitään vaikeuksia normaalille satunnaiselle käyttäjälle, jonka viestintä tapahtuu samojen tuttujen ihmisten kanssa. Laajempikin tuttavapiiri on nopeasti listattu ystävällisiksi lähettäjiksi, ja uudet tuttavat tai sähköpostiosoitetta vaihtavat ystävät varmasti jaksavat

lähettää sen yhden varmennusviestin. Ongelmia alkaa syntyä, jos sähköpostiosoitteen omistaja saa paljon viestejä tuntemattomilta. Tällöin vastausviestien määrä sekä viestimiseen käytetty aika ja vaiva kasvavat helposti, mikä voi nostaa kynnystä lähettää sähköposteja. Todelliset ongelmat syntyvät postituslistojen tai haluttujen sähköpostimainosten kanssa, jotka molemmat lähettävät viestejä massapostituksina. Roskapostittajia torjuva tekniikka estää myös kunnollisten ja haluttujen palveluiden tuottajien toimintaa. (VISNETIC 2003.)

4.6.2 Lähettäjän tunnistus

Lähettäjän varmennustekniikoista poiketen lähettäjän tunnistusmenetelmissä pyritään luomaan järjestelmä, jolla kaikki lähetetyt sähköpostit voidaan jäljittää takaisin sen lähettäjälle tai oikeastaan lähettäjän sähköpostipalvelimeen tai ip–osoitteeseen. Näitä tekniikoita kutsutaan myös DNS lookup -tekniikoiksi ja ne vaativat yleensä lisäyksen SMTP-protokollaan. (Aladdin 2003.)

Eräs tällainen SMTP:n päälle asetettava lähettäjän tunnistusjärjestelmä on RMX (Reverse-MX). Tämä järjestelmä ei varsinaisesti tunnista lähettäjää, mutta se tekee mahdottomaksi tai vaikeaksi väärentää sähköpostin lähetysosoitetta; tätä väärentämistä käytetään roskapostittajien keskuudessa runsaasti. Tämä ei vähennä roskapostin määrää, mutta se helpottaa roskapostittajien seuraamista ja kiinniottamista. (Ahlm 2003.) Toimintaperiaate on yksinkertainen: jokainen arvoalue, domain, pitää yllä verkkotunnuspalvelinlistaa (DNS), joka kertoo, ketkä kaikki saavat käyttää tätä osoitetta sähköpostin lähetysosoitteena. Sähköpostiviestin lähetysvaiheessa viestin vastaanottava sähköpostipalvelin tarkistaa, onko viestin lähettäjä listattu palveluntarjoajansa listalla. Kielteinen vastaus tuottaa virheilmoituksen, mutta muuten viesti lähetetään perille normaalisti.

RMX:n kaltaisia järjestelmiä on alkanut ilmestyä roskapostin torjuntaan. Esimerkiksi Lumos-projekti (ESPC 2003) ja ePrivacy Groupin Trusted Open Email Standard (Schiavonne et al. 2003) pyrkivät kumpikin korjaamaan SMTP:n ”avoimuuden” ja tekemään sähköpostista jäljitettävää palvelintasolla. Kaikissa mainituissa järjestelmissä on kuitenkin samankaltaisia puutteita. Ne toimivat vain sellaisissa palvelimissa, jotka tarjoavat nämä palvelut. Väärennetyllä osoitteella lähetetyt postit voidaan edelleen lähettää sellaisten palvelimien kautta, jotka eivät tätä menetelmää tue. Ongelmia voi syntyä esimerkiksi postituslistojen tai

muiden sähköpostilehtien kohdalla, mutta nämä voidaan lisätä järjestelmän valkoiseen listaan, jolloin ne päästetään suoraan läpi.

Toinen ongelmatapaus ovat niin sanotut verkkovieraat (roaming users), joilla ei ole suoraan mitään tiettyä sähköpostipalvelinta, vaan jotka valitsevat itselleen sillä hetkellä sopivimman. Tämänkaltainen järjestelmä tekee mahdottomaksi sähköpostiosoitteiden väärentämiset. Kun tiedetään varmasti lähettäjän osoite, voidaan tietystä osoitteesta lähetetyt roskapostit suodattaa turvallisemmin pois. Myös mahdollisten roskapostilakien käyttäminen roskapostittajia vastaan on helpompaa, kun tiedetään mistä postit ovat tulleet. (Danisch 2003; Rubel 2003.)

4.7. Hyvät tavat ja käytännöt

Hyvillä käytännöillä voidaan estää paljon roskapostia. Nämä keinot auttavat etenkin sähköpostin arkikäyttäjiä, joilla ei ole halua tai osaamista asentaa suodattimia tai joiden sähköpostipalveluntarjoajat eivät vielä muita palveluita tarjoa.

4.7.1 Sähköpostiosoitteen suojeleminen

Sähköpostiosoitteet ovat roskapostittajien elinehto. Siksi kannattaa pitää omasta sähköpostiosoitteesta hyvää huolta. Omaa osoitetta ei kannata jaella missä vain tai kenelle vain. Sähköpostiosoitteen sijoittaminen nettiin vaikkapa kotisivulle tai muuhun julkiseen paikkaan takaa sen, että ennemmin tai myöhemmin siihen alkaa saapua roskapostia. On kuitenkin tilanteita, jolloin on ”pakko” laittaa osoite nettiin. Silloin se on syytä naamioida eli kirjoittaa osoitteeseen esimerkiksi ”no-spam”, jonka käyttäjä osaa poistaa mutta automaattinen osoitteenkerääjä ei: *Matti.Meikäläinen@no-spam.yritys.fi*. Toinen tapa vaikeuttaa osoitteen keräämistä on ilmoittaa, mitä muotoa osoite on, mutta ei kirjoittaa sitä mihinkään. Esimerkiksi jos osoite on muotoa *etunimi.sukunimi@yritys.fi*, kerro vain oma nimi, ihminen osaa kyllä muodostaa tästä sen oikean osoitteen. (NOIE 2002.)

4.7.2 Useat tai salaiset sähköpostiosoitteet

Helpoimpia ja tehokkaimpia tapoja vähentää roskapostia tai oikeastaan sen haittavaikutuksia on käyttää useampaa sähköpostiosoitetta ja käyttää niitä eri tilanteissa. Käyttäjä voi

esimerkiksi erotella työpostit ja henkilökohtaiset postit eri osoitteisiin ja käyttää erillistä roskapostiosoitetta, jota voi jakaa avoimesti verkossa surffatessa. Työosoitetta käytetään vain työhön tai opiskeluun liittyvissä aiheissa ja henkilökohtainen, yksityinen osoite varataan vain ja ainoastaan kavereiden ja perheen käyttöön. Monen sähköpostiosoitteen tekniikkaa voi laajentaa siten, että käyttäjä luo aina uuden osoitteen, kun joutuu antamaan sähköpostiosoitteen tuntemattomalle taholle. Jos tällainen osoite joutuu roskapostittajan hampaisiin, se on helppo lopettaa: käyttäjän tarvitsee ilmoittaa vain yhdelle henkilölle muuttuneesta sähköpostiosoitteesta.

Salaisen sähköpostiosoitteen idea on tietenkin se, että osoite pysyy mahdollisimman salaisena. Täysin salaisen osoitteen ongelmana on, että silloin kukaan ei voi lähettää sinulle postia. Tämä heikentää sähköpostin hyödyllisyyttä kommunikointivälineenä. Mahdollisimman salaisella tarkoitan tilannetta, jossa sähköpostiosite ei ole missään esillä: esimerkiksi netissä, lehdissä, julkaisuissa tai ilmoitustauluilla. Sähköpostiosoiteesi leviää eteenpäin vain silloin kun kerrot sen henkilökohtaisesti jollekin.

Uusia sähköposti osoitteita saa ilmaiseksi isoimmilta palveluntarjoajilta kuten Yahoo tai Hotmail tai sen saa pientä lisämaksua vastaan omalta palveluntarjoajalta. Ilmaisia osoitteita jakavissa palveluntarjoajissa on huonona puolena, että isot kohteet eli, paikat joissa on tarjolla miljoonia sähköpostiosoitteita, ovat myös oikeita herkkupaloja roskapostittajien hyökkäyksille. Tästä syystä ilmaiseen sähköpostiosoitteeseen voi alkaa ilmestyä roskapostia, vaikka et ole antanut sitä koskaan kenellekään. Tämä johtuu roskapostittajien käyttämästä *sanakirjahyökkäys*-menetelmästä, jolla pystytään etsimään sähköpostipalvelimelta sähköpostiosoitteita. Sanakirjahyökkäys (dictionary attack) on roskapostittajien käyttämä menetelmä, jossa järjestelmällisesti arvaamalla pyritään löytämään palvelimilta sähköpostitilejä. (Graham 2003b.) Palaan aiheeseen hieman myöhempänä.

4.7.3 Valittaminen

Vielä muutama vuosi sitten monessa roskapostia käsittelevässä teksteissä kehotettiin roskapostin saajia valittamaan saamastaan roskapostista roskapostittajalle. Artikkeleissa esiteltiin hyvinkin monimutkaisia tapoja, kuinka voi jäljittää roskapostittajan. Tämän salapoliisityön jälkeen ihmisiä kehotettiin lähettämään kovasanainen sähköpostiviesti

roskapostittajan palveluntarjoajalle. Nykyään on luovuttu tällaisesta käytännöstä, koska siitä ei ole enää juuri mitään hyötyä. Useimmat roskapostittajat lähettävät viestit palveluntarjoajan kautta ja häviävät sen jälkeen kuin tuhka tuuleen, tai viestit lähetetään kaapatuista tai varastetuista palvelimista tai yksityiskoneista. Näin ollen tuhannet valituskirjeet haittaavat vain palveluntarjoajan elämää ja huonoimmassa tapauksessa voivat hidastaa tai jopa kaataa pienen sähköpostipalvelimen.

5. Roskapostin levitys

Miltä roskapostittaminen näyttää lähettäjän kannalta? Monet luonnehtivat roskapostittajien ja roskan torjujien välistä kilpailua sodaksi, jossa toinen puoli pyrkii aina toisen edelle keinolla millä hyvänsä. Roskapostittajat pyrkivät saamaan viestinsä perille ihmisten postilaatikkoihin sekä saamaan ihmiset lukemaan niitä ja reagoimaan niihin. Tämän pitäisi tapahtua siten, että kustannukset jäävät mahdollisimman vähäisiksi. Samalla pyritään minimoimaan kiinnijäämisen riski vihaisten roskapostin uhrien suuntaan. Seuraavaksi selvitetään, miten roskaajat täyttävät postilaatikon.

5.1. Sähköpostiosoitteet ja niiden hankkiminen

Roskapostin lähettämisen ensimmäinen askel on sähköpostiosoitteiden kerääminen. Varsinkin oikeat, aktiiviset ja paljon käytetyt sähköpostiosoitteet ovat roskapostittajalle toiminnan lähtökohta. Tästä syystä kerättyjä osoitteita tarkistetaan eli pestään, jolloin listoista poistetaan huonot ja toimimattomat osoitteet. Tämä on tosin joidenkin roskapostittajien mielestä turhaa työtä, koska viestien lähettäminen on ilmaista, eivätkä muutamat huonot osoitteet postituslistassa vaikuta mitenkään.

Osoitteita myös myydään, ostetaan ja vaihdetaan roskapostittajien keskuudessa. On olemassa ”sähköpostimarkkinointikerhoja” joihin liittyvä voi hankkia satojatuhansia sähköpostiosoitteita sisältäviä listoja. Eräät tahot ovat keskittyneet keräämään sähköpostiosoitteita ja myymään niitä eteenpäin muun muassa roskapostittajille. Seuraavaksi käsittelen menetelmiä ja tapoja, kuinka ja mistä roskapostittajat keräävät osoitteita.

5.1.1 Kotisivut, irc, chat ja uutisryhmät

Helpoin ja nopein tapa hankkia ihmisten sähköpostiosoitteita on kerätä niinä Internetistä. Ihmisten, yritysten, järjestöjen ja oppilaitosten kotisivut suorastaan tyrkyttävät roskapostittajille sähköpostiosoitteita, kymmeniä ellei satoja osoitteita sivustoa kohden. FTC:n suorittaman tutkimuksen mukaan 86 prosenttiin kotisivuilla esillä olevista

sähköpostiosoitteista saa roskapostia yhtä suuri prosenttimäärä eli 86%. Myös Internetin chat-ryhmät ovat osoittautuneet roskapostittajille oikeiksi aarreaitoiksi. Saman tutkimuksen mukaan sähköpostiosoitteen kirjoittamisen jälkeen ensimmäinen roskaposti ilmestyy kyseiseen osoitteeseen parhaimmillaan tai pahimmillaan yhdeksän minuutin kuluessa. (FTC 2002a.)

Sähköpostiosoitteiden keräyksen kotisivuilta, keskusteluryhmistä ja chateista tekevät niin sanotut *kerääjäohjelmat* (harvester). Nämä kerääjät toimivat hyvin samalla tavalla kuin Googlen kaltaisten hakukoneiden kotisivuja tutkivat ohjelmat. Nämä kerääjäohjelmat liikkuvat kotisivuilla etsien sähköpostiosoitteita ja lähettävät niitä roskapostittajille. Näitä kerääjäohjelmia on Internetissä myynnissä tai jaossa useita.

5.1.2 Sanakirjahyökkäykset

Sanakirjahyökkäys on metodi, jossa uhriksi joutunutta sähköpostipalvelinta aletaan pommittaa kysymyksillä siellä olevista osoitteista. SMTP-protokollan mukaan sähköpostipalvelin vastaa kielteisesti, jos kyseistä osoitetta ei sieltä löydy. Läpimenevät kyselyt todetaan oikeiksi ja kunnollisiksi osoitteiksi ja lisätään roskapostittajien listaan.

Kysyttyjä osoitteita luodaan usealla eri tavalla. Yksi tapa on aloittaa kyseleminen jostain kirjaimesta, esimerkiksi A:sta. Kirjaimia lisäämällä luodaan tuhansia mahdollisia osoitteita kuten *a@domain.fi*, *aa@domain.fi*, *aaa@domain.fi*, *aaaa@domain.fi*. Kirjaimia ja numeroita lisäämällä yritetään arvata oikeita sähköpostiosoitteita. Hieman hienostuneempi tapa on käyttää tunnettuja sanoja satunnaisten kirjainten sijasta. Nimien, eläinten tai tavaroiden käyttö tai niiden yhdisteleminen toisiin sanoihin, kirjaimiin tai numeroihin tuottaa myös tulosta: *Jarno@domain.fi*, *Jarno1@domain.fi*, *Jarno2@domain.fi*. Yhdistelyä voidaan parantaa loputtomasti yhdistelemällä tunnettuja etunimiä ja sukunimiä. Monilla palvelimilla on myös omat käytäntönsä siihen, miten sähköpostiosoitteet muodostetaan. Tämän muodostussäännön käyttäminen helpottaa huomattavasti osoitteiden löytämistä. (Verisign 2003.)

5.1.3 Vakoiluohjelmat

Käyttäjien huonosti suojatuille kotikoneille voidaan asentaa monia vakoiluohjelmia, jotka muun pahan lisäksi keräävät ihmisilta sähköpostiosoitteita. Tietyn henkilön henkilökohtaisten

osoitteiden keräämisen hyötynä on niiden toimivuus. Samalla voidaan parantaa viestien avaamisprosenttia naamioimalla viestien lähettäjäksi se onneton henkilö, jonka osoitekirjasta osoitteet on varastettu.

5.1.4 ”Poista minut listalta” –linkit

Roskapostiviesteistä löytyy usein linkki, jonka luvataan poistavan käyttäjä mainospostilistalta tai lisäävän hänet ”ei saa roskapostittaa” -listoille. Useimmiten linkki ei tee muuta kuin varmistaa käyttäjän osoitteen olevan olemassa, varmistaa sen, että tämä lukee roskapostiviestejä ja että tämä on valmis käyttämään roskaposteista löytyviä linkkejä.

5.1.5 Ostaminen ja periminen

Sähköpostilistoja on myös siirtynyt kunnolliselta toimijalta roskapostittajalle yrityskauppojen yhteydessä, jolloin huomattavia määriä sähköpostiosoitteita voi kerralla joutua roskapostittajien käsiin. Sähköpostitietoja myydään ja ostetaan paljon varsinkin maissa, joissa yksityisyyden suojaaminen ei ole Suomen tasoa.

5.2. Suodattimien huijaaminen

Roskapostisuotimet ovat yleisimpiä roskapostin estovälineitä. Suodattimien perusidea on tutkia sille annetun sähköpostiviestin sisältöä, sanoja tai merkkejä ja päätellä, onko kyseessä roskaposti vai ei. Suodattimia on olemassa muutamaa päätyyppiä, mutta toimintaperiaate on niissä kaikissa kuitenkin sama, viestin sisällön tutkiminen. Tästä syystä roskapostiviestejä lähettävät pyrkivät muuntamaan tai naamioimaan viestien sisältöä niin, että suodattimet luulevat niitä kunnollisiksi sähköposteiksi muuttamatta kuitenkaan liikaa viestin merkitystä lukijalle.

5.2.1 Sanan vaihto

Suurin osa suodattimista toimii niin, että ne etsivät sähköpostiviesteistä sanoja, joita yleensä ilmenee roskapostiviesteissä. Siksi helpoin tapa huijata suotimia on olla käyttämättä tunnettuja roskapostisanoja. Sanoja kuten ”sex” tai ”free” voidaan esittää muilla samaa tai

lähes samaa tarkoittavilla sanoilla tai ilmaisuilla. Tämä on kuitenkin vain väliaikainen korjaus, sillä uusia sanoja lisätään koko ajan suodattimien tunnistuslistoille ja järkevät sanavaihtoehdot käyvät vähäisiksi. (Sophos 2003.)

5.2.2 Sanan naamiointi

Toinen tapa on naamioida sanat tietokoneelta. Esimerkiksi sanaan ”free” voidaan lisätä jokin merkki jokaisen kirjaimen väliin. Merkit voivat olla esimerkiksi välilyönti “f r e e” tai piste “f.r.e.e” tai alaviiva “f_r_e_e”. Muita käytettyjä merkkejä ovat myös tähti ja heittomerkki. Nyt sana eroaa alkuperäisestä sanasta “free” ja on siten näkymätön suotimille, mutta ihminen pystyy lukemaan ja ymmärtämään sen ilman vaikeuksia.

Toinen tapa on korvata kirjaimia, tavuja tai sanoja numeroilla. Esimerkkinä kirjain ”l” voidaan korvata helposti numerolla ”1”, jolloin sana ”live” voidaan esittää ”1ive”. Englannin kielessä numeroilla voi korvata tavuja tai kokonaisia sanoja: ”skate” voi olla muodossa ”sk8” ja ”for you” ymmärretään myös muodossa ”4u”. Tutut kirjaimet voidaan myös vaihtaa harvinaisempiin mutta samannäköisiin merkkeihin: “a” voidaan korvataan merkillä “å”. Näin pystytään naamioimaan avainsanat suotimelta ilman, että viestin sisältö muuttuu ihmisen kannalta ratkaisevasti.

Erilaisten HTML-tagien käyttö sanojen keskellä on myös tehokas tapa sotkea suotimet. ”Free” sana voidaan sotkea laittamalla vaikka lihavointimerkit keskelle sanaa: ”free” sana näkyy ruudulla entisellään, mutta pelkkää lähdekoodia tutkivat suotimet ovat hukassa. (Hird 2002; Sophos 2003.)

5.2.3 Kirjoitusvirheet

Sanojen naamioimisen lisäksi tahallisia kirjoitusvirheitä käytetään yleisesti roskapostisuotimien huijaamiseen. Samalla tavalla kuin pisteiden lisääminen sanan kirjainten väliin myös väärinkirjoitus tuottaa saman tuloksen. Sanat ovat ihmisen ymmärrettävissä, mutta suodattimet putoavat nopeasti kärryiltä. Esimerkkinä “viagra” -> “viegra”. Tutkimusten mukaan sanan ensimmäisen ja viimeisen kirjaimen pysyessä paikoillaan voidaan keskellä olevia kirjaimia vaihtaa monin tavoin, mutta ihminen ymmärtää silti lukemaansa tarpeeksi hyvin (Sophos 2003).

5.2.4 Sanojen lisääminen ja piilottaminen

Suotimissa etsitään negatiivisten roskapostisanojen lisäksi usein myös positiivisia, harvemmin roskaposteissa esiintyviä sanoja. Näitä sanoja lisäämällä voidaan saada suodatin luulemaan kyseessä olevan kunnollinen posti, vaikka siinä esiintyykin jonkin verran kiellettyjä sanoja. Esimerkiksi päivän uutisotsikoiden kirjoittaminen tai tietosanakirjan luvun liittäminen viestiin muuttaa sen sisällön suotimen silmissä aivan toiseksi. Hämäystekstit sijoitetaan joko viestin loppuun tai HTML-viestissä teksti voidaan kirjoittaa ”näkymättömällä musteella” eli teksti kirjoitetaan samalla värillä kuin viestin pohja. Näin sanat vaikuttavat suotimeen, mutta viestin lukija ei niitä näe.

Samaa perusideaa voidaan muunnella käyttämällä hyväksi HTML:n muita ominaisuuksia. Esimerkiksi pienen vieritysikkunan luominen viestin reunaan <marquee> -tagilla mahdollistaa kunnollisten sanojen käyttämisen viestissä ilman, että käyttäjä näkee niitä. Hämäyssanoja voidaan myös laittaa HTML–tagin sisään. Näkymättömän musteen lisäksi tekstin voi naamioida samankaltaisella värillä. Näin lisätty teksti on juuri ja juuri näkyvä mutta ei häiritse varsinaista tekstiä.

Hämäystekstejä voidaan piilottaa myös HTML-viestin otsikkoon (<title>), joka jää yleensä sähköpostiviesteissä näkymättä. Viestiin voidaan myös kirjoittaa hämäyssanoja pienellä tai nollakokoisella fontilla, jolloin se on näkymätöntä tai ainakin luettavaksi kelpaamatonta viestin lukijalle, mutta suodattimet lukevat tekstin sivun ”lähdekoodista” ja menevät sekaisin. Häiriösanoja lisätään myös viestien otsikkoriville: varsinaisen otsikon ja lisätyn häiriösanan väliin sijoitetaan joukko tyhjiä merkkejä, jolloin häiriösana jää yleensä käyttäjältä näkymättömiin. (Sophos 2003.)

5.2.5 Suodattimien myrkyttäminen

Suodattimien myrkytysmenetelmä (filter poisoning, bayes poisoning) on sukua edellä kerrotulle kunnollisten sanojen lisäämismenetelmälle. Edellisen menetelmän suurin puute on sen tehottomuus kehittyneitä tilastollisia suodattimia vastaan. Tilastolliset suodattimet eivät tutki pelkästään yksittäisiä sanoja vaan niiden esiintymistä muiden sanojen kanssa roskaposteissa tai kunnollisissa posteissa, ja siksi muutamat kunnolliset sanat muuten selvässä roskapostiviestissä eivät saa huijattua suodatinta merkitsemään roskapostiviestiä kunnolliseksi

postiksi. Tämän tehokkuuden lisäksi tilastollisilla suodattimilla on vielä yksi etulyöntiasema sääntöpohjaisia suotimia vastaan. Tämä etu on niiden kyky oppia ja mukautua siihen, mikä on roskaa ja mikä ei. Vaikka yksittäinen kunnollisia sanoja täynnä oleva viesti pääsisi suodattimen ohi, käyttäjä voi nopeasti merkitä viestin roskaksi ja tästä eteenpäin vastaavanlainen viesti merkitään taas roskaksi.

Tähän oppimiskykyyn yrittää suodattimien myrkytysmenetelmä puuttua. Toimintaperiaate on sama: roskapostiviesteihin lisätään tai piilotetaan kunnollisia ei-roskaposteissa yleensä käytettyjä sanoja kuten neula, lanka, kehrätä. Tosinaan tällainen roskapostiviesti pääsee läpi suotimesta. Tämän tyyppisen viestin läpipääseminen nopeutuu, jos henkilö saa paljon kunnollista postia, jossa käytetään kyseisiä sanoja. Virheellisesti merkityn viestin huomatessaan käyttäjä kertoo suotimelle, että kyseinen viesti on roskapostia; suodatin oppii, että kyseisiä sanoja sisältävät viestit ovatkin roskapostia. Tästä eteenpäin esimerkin sanat neula, lanka ja kehrätä yhdistetään myös roskaposteihin. Viestin ei tarvitse edes mennä suotimesta läpi, koska suodatinohjelma oppii itsenäisesti, millaisia sanoja roskaposteissa liikkuu ja alkaa yhdistää kunnollisia sanoja roskapostiviesteihin. Mitä enemmän roskapostittajat saavat muutettua suodattimien kunnollisia sanoja roskapostisanoiksi, sitä useammin suodattimet merkitsevät kunnollisia viestejä roskapostiksi; mitä useammin suodatin merkitsee kunnollisen viestin roskaksi, sitä vähemmän ihmiset luottavat suodattimiinsa. Lopulta suodatin ei enää erota kunnollista viestiä roskapostista ja suodatin on hyödytön. Tämä on myrkytystekniikan perimmäinen tarkoitus. (Graham & Cumming 2003.)

5.2.6 Rivitys

HTML-koodin käyttäminen viesteissä mahdollistaa monia erilaisia hämäyskeinoja. Viestin teksti voidaan jakaa muutaman kirjaimen levyisiin sarakkeisiin. Tämä tarkoittaa, että HTML-koodissa sanat muuttuvat satunnaisiksi kirjainjonoiksi, joilla ei ole mitään merkitystä roskapostisuodattimille. Viestiä luettaessa koodissa oleva siansaksa muuttuu jälleen ymmärrettäväksi kieleksi, kun HTML-tulkki kokoaa taulukon ja näyttää sen käyttäjälle ehjänä. (Sophos 2003.)

5.2.7 Roskaaminen

Todennäköisyyslaskentaa, hahmontunnistusta tai sormenjälkitekniikkaa käyttävien suodattimien huijaamiseksi liitetään viesteihin usein satunnaisia tekstijonoja, esimerkiksi ”sddgfasd”, joka arvotaan jokaiseen lähtevään viestiin erilaiseksi. Näin jokainen viesti saa oman ainutlaatuisen sormenjäljen tai hahmon. Satunnaisjonon pituus riippuu viestin pituudesta. Liian lyhyt merkkijono pitkässä viestissä ei muuta siitä muodostettavaa jälkeä tarpeeksi. Näin viestien vertaaminen muihin vastaaviin viesteihin ei onnistu, vaan suodattimet päästävät ne läpi kunnollisena postina. (Sophos 2003.)

5.3. Roskapostiviestien lähetys

Kolmas askel roskapostittamisessa on viestien lähettäminen. Roskapostiviestejä lähetetään roskapostittajien omien palveluiden (spamhaus) kautta maksullisen tai ilmaisen palveluntarjoajan kautta, avoimien sähköpostipalvelimien tai proxien kautta, nettisivuilta löytyvien formmail-ohjelmien kautta tai kuolleiden ja kuopattujen yritysten jälkeensä jättämien nettialueiden (legacy blocks, zombie blocks) kautta.

5.3.1 Palveluntarjoajat

Palveluntarjoajat on kaikkein helpoin ja nopein tapa lähettää pieniä määriä roskapostia. Tämä tapahtuu yleensä ilmaisten tai maksullisten sähköpostipalveluiden tarjoajien kautta. Roskapostittaja hankkii itselleen yhden tai useamman sähköpostitilin ja alkaa joko manuaalisesti tai apuohjelmien kautta lähettää roskaposteja maailmalle. Tiettyjen palveluntarjoajien käyttö on hyödyllistä varsinkin silloin, kun roskapostia lähetetään saman palveluntarjoajan muihin osoitteisiin. Ilmaisten palveluntarjoajien kohdalla osoitteita hankitaan yleensä monia, jopa useita satoja. Tässä tapauksessa yksittäisistä osoitteista ei lähetetä kuin muutama sata sähköpostiviestiä päivässä. Sata sähköpostiviestiä päivässä ei vielä hälytä palveluntarjoajia ja roskapostittamista pystyy jatkamaan, kunnes ensimmäinen valituskirje ilmestyy palveluntarjoajalle. Väärillä tiedoilla avattu tili hylätään paljastumisen jälkeen ja avataan uusi tili, josta toimintaa voidaan jatkaa taas päivä tai pari. (Hird 2002.)

Roskapostin varhaisvuosina tämä oli paljon käytetty roskaamistapa, mutta viime vuosina palveluntarjoajat ovat kiristäneet suhtautumistaan roskapostittajiin ja usein aloittaneet taistelun roskapostittajia vastaan omilla palvelimillaan. Palveluntarjoajat ovat ryhtyneet suodattamaan myös uloslähtevää postia, esimerkiksi vuorokauden aikana lähetettävien postien määrää on rajoitettu. Roskapostittajilla voi olla tapana automatisoida koko roskaamisprosessi aina uusien tilien avaamista myöten. Tästä syystä monissa isoimmissa palveluntarjoajien tilien avauskyselyissä on mukana tehtävä tai kysymys, jonka vain ihminen voi tehdä tai vastata. Tämä usein kuvan tulkitsemiseen liittyvä kysymys tekee automaattisen eli ohjelmallisen tilien massa-avauksen mahdottomaksi.

5.3.2 Avoimet sähköpostipalvelimet ja proxyt

Sähköpostiviestien lähettämiseen tarvitaan sähköpostipalvelin ja Internet-yhteys. Varsinkaan pienet roskapostittajat eivät yleensä perusta omia sähköpostipalvelimia niiden kalleuden ja niiden jäljittämisriskin takia. Kun viime aikoina palveluntarjoajat ovat alkaneet kiinnittää kasvavaa huomiota siihen, mitä heidän palvelimillaan tapahtuu, roskapostittajat ovat alkaneet etsiä avoimia ja turvattomia sähköpostipalvelimia muualta.

Aikaisemmin isotkin sähköpostipalvelimet kuten yliopistot antoivat ulkopuolisten lähettää sähköpostia omilta palvelimiltaan. Oikeastaan SMTP-protokollan mukaan kaikki sähköpostipalvelimet hyväksyvät ja lähettävät edelleen kaikki niille annetut sähköpostiviestit. Roskapostittajat käyttivät sähköpostipalvelimien avoimuutta armotta roskan levittämiseen ja tästä syystä nykyään lähes kaikki palvelimet sulkevat ovensa oman alueensa ulkopuolelta tuleville sähköpostin lähetys- tai välityspyynnöille. Avoimia sähköpostin välityspalvelimia eli proxyja löytyy kuitenkin Internetistä runsaasti. Nämä usein väärin tai huolimattomasti asennetut palvelimet listataan ja roskapostittajat käyttävät niitä tehokkaasti hyväksi.

Toinen samankaltainen ongelma ovat yksityisten ihmisten koneilleen vahingossa tai muuten huonosti asentamat sähköpostipalvelimet. Ihmiset voivat vahingossa asentaa sähköpostipalvelimen asentaessaan muita palvelinohjelmistoja tai työkaluja koneelleen. Tästä syystä monet näitä ohjelmia myyvät tai jakelevat yritykset ovat muuttaneet oletusasetuksia omissa tuotteissaan niin, että vahingossa asennettu palvelin ei edelleenlähetä ulkopuolelta tulevia sähköposteja. Näitä vahinkopalvelimia asentavat ihmiset eivät yleensä edes huomaa

sellaisen olemassaoloa, koska he käyttävät toista, esimerkiksi Internet-yhteyden tarjoavan yrityksen sähköpostipalvelinta. Siksi tällaiset palvelimet pysyvät tihutöitä tekevien kuten roskapostittajien iloksi pitkiä aikoja Internetissä. (Ahlm 2003; Tompsett 2003.)

Vahinkopalvelimien rinnalle on noussut uusi ja pelottava tapa levittää roskaposteja. Virusmaailmassa on tullut ilmi sähköpostissa liikkuvia matoja, jotka asentavat pienen sähköpostipalvelimen saastuttamalleen koneelle. Näitä palvelimia virukset käyttävät itsensä levittämiseen tai muihin tihutöihin. Vastaavanlaisia palvelimia kylväviä matoja voitaisiin käyttää ja varmasti käytetäänkin roskapostien levittämiseen. Pahaa arvaamaton ADSL-yhteyden omistava Pentti Peruskäyttäjä voi toimia huomaamattaan roskapostittajan reippaana pikku apulaisena. (BBC 2003.)

5.3.3 Postikorttisivut

Internetissä löytyviä sähköisiä postikortteja lähettäviä sivustoja voidaan käyttää myös roskapostittamiseen. Sivustot toimivat niin, että käyttäjät voivat lähettää sen kautta hauskoja viestejä tai kortteja ystävilleen ja tuttavilleen ilmaiseksi. Kortin saajan sähköpostiin ilmestyy ilmoitus, jossa kerrotaan palveluntarjoajan sivuilla odottavasta viestistä. Normaalisti täältä löytää ystävänpäivän tai syntymäpäivän tervehdyksen, mutta roskapostittajien tapauksessa kortissa on mainoksia tai muuta ilmoitusasiaa. Roskapostittajan kannalta korttien lähettäminen manuaalisesti olisi liian hidasta ja kallista, siksi on olemassa ohjelmia, jolla sen voi tehdä automaattisesti ja halvalla. (Herbert 2002.)

5.3.4 Zombie Blocks

Aiempaa erikoisempi ja monimutkaisempi tapa lähettää roskapostia ovat Internetissä roikkuvien, unohdettujen tai kuolleiden yritysten tai järjestöjen nettialueet (block). Tällainen unohdettu nettialue (zombie block) otetaan käyttöön esiintymällä alueen laillisena omistajana ja pyydetään sen liittämistä runkoverkkoon (backbone). Runkoverkot ovat nopeita valokaapeliyhteyksiin perustuvia tietoverkkoja, jotka yhdistävät pienempiä tietokonejärjestelmiä toisiinsa ja muodostavat Internetin selkärangan. Yleisesti runkoverkot omistavat suuret teleoperaattorit tai muut järjestöt. Runkoverkkoon liittämisen jälkeen alue ja sen ip-osoitteet ovat roskapostittajien käytössä, tätä kutsutaan myös termillä *ip-kaappaus* (ip-hijacking). Roskapostittajat perustavat tiettyyn ip-osoitteeseen postipalvelimen, jolta alkavat

kylvää roskapostia. Tämän osoitteen ilmestyttyä mustille listoille siirrytään seuraavaan hallussa olevaan osoitteeseen ja jatketaan toimintaa. Kun alueen kaikki ip-osoitteet on mustalistattu, alue voidaan joko unohtaa tai se myydään pahaa aavistamattomalle henkilölle, jolloin roskapostittajat siirtyvät seuraavaan kaapattuun alueeseen ja jatkavat toimiaan. Kaapatut alueet ovat roskapostittajille turvallisia myös niiden tarjoaman nimettömyyden takia. Alueet voidaan helposti jäljittää, mutta henkilöt niiden takana pysyvät salassa. (Completewhois 2003; SORBS 2004.)

6. Roskaposti ja laki

Roskapostista on kasvanut niin suuri ja vaikeasti torjuttava uhka sähköpostille, että on syntynyt tarve luoda lakeja roskapostia ja niiden levittäjiä vastaan. Monissa maissa roskapostittaminen on sallittua tai se ei ole laissa erikseen kiellettyä. Esimerkkinä Suomessa yksityishenkilöille lähetetty massamuotoinen sähköinen mainosposti on kiellettyä (Puolamäki 2002).

Monet pitävät hyvää roskapostilakia ja sen tehokasta toteuttamista ainoana toimivana lääkkeenä roskaposteja vastaan. Lakien heikkous on niiden paikallisuus. Internet on globaali verkko ja niin kauan kun löytyy sellainen maailmankolkka, joka ei kriminalisoi roskapostin lähettämistä, voivat roskapostittajat siirtää toimintansa sinne ja jatkaa roskaamista. Suomessa roskapostittaminen on laissa kiellettyä, mutta silti lähes jokainen sähköpostinomistaja on joskus saanut yhden tai useamman roskapostiviestin ulkomailta. Roskapostin subjektiivinen luonne on myös lakien kannalta vaikea asia. Liian löysä roskapostin määre tekee roskapostilaista nopeasti tehottoman. Roskapostittajat mukauttavat toimintansa lain mukaan ja jatkavat roskaamista. Liian tiukka laki taas voi hankaloittaa kunnollisten postien lähettämistä: postituslistat, sähköpostilehdet ja kunnollinen sähköpostimainonta kärsisivät varmasti liian ankarasta laista. Lopullinen määrittelyvalta roskapostin suhteen pitäisi ihanteellisesti olla viestien vastaanottajalla itsellään.

Esimerkiksi Yhdysvalloissa paine kunnolliselle kansalliselle roskapostilaille on erittäin suuri. Roskaposti on menestynyt siellä hyvin ja uusia roskapostittajia syntyy koko ajan lisää. Suurin osa maailman roskapostista syntyy juuri Yhdysvalloissa. Eri osavaltiot ovat ottaneet käytäntöön erivahvuisia roskapostilakeja ja –säädöksiä, mutta tehokkaan roskapostilain tulee olla kansallinen, jolloin roskapostittajat ympäri maata voidaan tuomita samojen lakien mukaan. Kansallinen laki estää myös roskapostiparatiisien muodostumista sellaisista osavaltioista, joiden roskapostilait ovat tehottomia.

Roskapostin vastustajat ovat arvostelleet Yhdysvaltain roskapostilakiehdotusta liian löysäksi. (CAUCE 2003; MARK 2003). Lakiehdotus märittää roskapostiksi sokeasti suurelle satunnaiselle joukolle lähetetyt mainokset, ilman peruutusmahdollisuutta lähetetyt mainokset

ja valheelliset mainossähköpostit. Valheellisuudeksi käsitetään lähinnä lähetystietojen väärennös tai muuten lainvastainen mainonta. Lakiehdotuksen mukaisesti roskapostia pystyisi edelleen lähettämään ilman vastaanottajan lupaa tai ilman aikaisempaa suhdetta – tätä kutsutaan myös opt-out -mainospostiksi. Roskapostin vastustajat haluaisivat Yhdysvaltojen ottavan käyttöön EU:n direktiivin käyttämän opt-in –metodin, jossa mainospostiviesti pitää pyytää ennen kuin se voidaan lähettää vastaanottajalle. Muuten EU:n roskapostidirektiivi on sisällöltään samansuuntainen kuin Yhdysvaltojen vastaava laki. (EU 2002; Sorking 2003.)

7. Yhteenveto

Ongelman ratkaisun etsiminen alkaa ongelman mahdollisimman tarkasta määrittelystä. Tämä tarkan ja kaikenkattavan määritelmän puuttuminen on yksi roskapostintorjunnan suurimmista haasteista. Ei voida tehdä muottia tai kaavaa, jolla pystyttäisiin erottelemaan roskaposti kunnollisesta postista varmasti ja yleisesti.

Roskaposti tarkoittaa eri asiaa eri ihmisille. Pelkästään roskapostia vastaan taistelevien tahojen keskuudessa löytyy eroja, jopa ristiriitoja roskapostin määritelmästä normaalista sähköpostinkäyttäjistä puhumattakaan. Tästä syystä roskapostiongelman ratkaisu pitäisi siirtää mahdollisimman lähelle sähköpostiviestin saajaa eli loppukäyttäjää.

Kaukana käyttäjistä olevien estomenetelmien haittana ovat käyttäjän pienet mahdollisuudet vaikuttaa siihen, mikä on roskaa ja mikä ei. Yhden tahon roskapostimääritelmän pakottaminen suurelle joukolle muistuttaa liiaksi sensuuria ja siksi sitä pitää välttää.

Palveluntarjoajien suosimat nopeat, halvat ja laajat tekniset ratkaisut kuten mustat listat tai muut palvelintasolla olevat estomenetelmät ovat huonoja ratkaisuja ongelmaan, joka on loppujen lopuksi henkilökohtainen ja ei-tekninen.

Ei-teknisistä ratkaisuista eniten käytettyjä ovat lait. Lait ovat myös kaukana loppukäyttäjästä ja se tekee myös lakien käyttämisen roskapostitaistelussa vaikeaksi. Liian tiukat lait ovat sensuuria ja liian löysät lait taas helposti kierrettäviä ja tehottomia. Parhaiten lait sopivat estämään roskaposteissa liikkuvia, jo lailla kiellettyjä roskapostimuotoja kuten erilaisia huijauksia.

Teknistä ratkaisuista paras malli on henkilökohtainen suodatin. Se on ohjelma, joka asennetaan käyttäjän omalle koneelle ja se järjestelee postit käyttäjän omien määritelmien mukaan. Näin varmistetaan, että käyttäjät saavat juuri sellaista postia kuin itse haluavat. Haittana näissä suotimissa on niiden asentamisen ja ylläpitämisen vaikeus ja se seikka, että näin torjutut roskapostit kuluttavat edelleen palveluntarjoajien resursseja.

Roskapostin suurin ongelma on postin suuri määrä ja määrän aiheuttamat haitat. Suurimman osan maailmalla liikkuvasta roskapostista muodostavat mainospostit. Mainosposteja lähetetään, koska niistä saadaan rahaa. Rahaa taas saadaan, kun ihmiset ostavat tuotteita, joita mainostetaan roskaposteissa. Olisiko siksi tehokkain tapa lopettaa roskapostin vyöry tekemällä siitä taloudellisesti kannattamatonta?

Roskapostitaloudesta tekee erikoisen ja viestien vastaanottajien kannalta ikävän se tosiseikka, että toisin kuin muissa mainonnan muodoissa, mainosroskapostissa kulut maksavat viestien vastaanottajat eivätkä niiden lähettäjät. Ehkä roskapostittajien voittoja voitaisiin vähentää myös valistamalla ihmisiä ja neuvomalla heitä olemaan ostamatta tavaraa roskapostittajilta? Tämä sulkisi heidän kassavirtansa ja vähentäisi roskapostin määrää niin, että se ei enää olisi koko sähköpostijärjestelmää uhkaava ongelma. Tämä ratkaisu on hidas ja epärealistinen eikä se ole suora ratkaisu ongelmiin, joita roskapostivyöry nyt aiheuttaa.

Suodattimet ja estolistat pyrkivät estämään roskapostittajien rikastumasta pysäyttämällä mainosviestien pääsyn ihmisten postilaatikoihin. Tästä seuraa kuitenkin muita ongelmia kuten hävinneet kunnolliset viestit. Kadonneet viestit ovat roskapostintorjunnan ongelma, jota ei voida mielestäni painottaa liikaa. Roskapostiongelman ratkaisuna voisi toimia yhdistelmä henkilökohtaisia suotimia, sopivia lakeja, valistusta ja tervettä järkeä.

Lähteet

Internet-lähteet tarkastettu 7.-8.2.2004

Ahlm, Eric 2003: *SPAM: Defining the Issues and Methods of Defense*, Internet WWW-sivu, URL: http://cnscenter.future.co.kr/resource/security/application/SPAMWhitePaper.pdf.

Aladdin Knowledge Systems 2003: *Anti Spam White Paper*, Internet WWW-sivu, URL: http://www.esafe.com/pdf/esafe/esafe_antispam_whitepaper.pdf.

BBC 2003a: *Spammers and Virus Writers Unite*, Internet WWW-sivu, URL: http://news.bbc.co.uk/1/hi/technology/2988209.stm.

BBC 2003b: *Spam Virus 'Hijacks' Computers*, Internet WWW-sivu, URL: http://news.bbc.co.uk/2/hi/technology/2987558.stm.

Borenstein, Bellcore & Freed 1993: *MIME (Multipurpose Internet Mail Extensions) Part One*, Internet WWW-sivu, URL: http://www.ietf.org/rfc/rfc1521.txt.

Bray, Hiawatha 2003: *Collateral Damage in the War on Spam*, Internet WWW-sivu, URL: http://www.dotcomeon.com/boston_collateral_damage.html.

Brightmail 2004: http://www.brightmail.com/spamstats.html.

Canter, Lawrence & Martha Siegel 1994: *How to Make a Fortune on the Information Superhighway: Everyone's Guerrilla Guide to Marketing on the Internet and Other On-Line Services*. New York: HarperCollins.

CAUCE 2003: *CAUCE Statement on House Spam Bill Vote*, Internet WWW-sivu, URL: http://www.cauce.org/news/index.shtml.

CDT 2003: *CDT's Analysis of S. 877*, Internet WWW-sivu, URL: http://www.cdt.org/speech/spam/030624cdtanalysis.pdf.

Completewhois 2003: *Questions and Answers on IP Hijacking*. http://www.completewhois.com/hijacked/hijacked_qa.htm.

Cunningham, Nowlan, Jane Delany & Haahr 2003: *A Case-Based Approach to Spam Filtering that Can Track Concept Drift*. http://www.cs.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-16.pdf.

Danisch, Hadmut 2003: *The RMX DNS RR and Method for Lightweight SMTP Sender Authorization*, Internet WWW-sivu, URL: http://www.ietf.org/Internet-drafts/draft-danisch-dns-rr-smtp-03.txt.

Edelson, Eve 2003: *The 419 Scam: Information Warfare on the Spam Front and a Proposal for Local Filtering*, Internet WWW-sivu, URL: http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V8G-492V5TV5&_coverDate=07%2F31%2F2003&_alid=131024929&_rdoc=1&_fmt=&_orig=search&_qd=1&_cdi=5870&_sort=d&view=c&_acct=C000049117&_version=1&_urlVersion=0&_userid=949127&md5=5979ad59bbe950000a4be6b1f9919a71#toc2.

ESPC Email Service Provider Coalition 2003: *Project Lumos*, Internet WWW-sivu, URL: http://www.networkadvertising.org/espc/Project_Lumos_White_Paper.pdf.

EU 2002: *Directive 2002/58/EC Of The European Parliament*, Internet WWW-sivu, URL: http://register.consilium.eu.int/pdf/en/02/st03/03636en2.pdf.

Fallows, Deborah 2002: *Email at Work*, Internet WWW-sivu, URL: http://www.pewInternet.org/reports/pdfs/PIP_Work_Email_Report.pdf.

Fallows, Deborah 2003: *Spam: How It Is Hurting Email and Degrading Life on the Internet*, Internet WWW-sivu, URL: http://www.pewInternet.org/reports/pdfs/PIP_Spam_Report.pdf.

Ferris Research 2003: *The Cost of Spam False Positives*, Internet WWW-sivu, URL: http://www.brightmail.com/pdfs/Cost_of_Spam_False_Positives___Ferris_Research_8_2003.pdf.

Fontana, John 2002: *Spam Filters Revealing Their Darker Side*, Internet WWW-sivu, URL: http://www.nwfusion.com/news/2002/0909spam.html.

FTC Consumer Feature 2002: *Chain Emails: Just Another Ploy or the Real McCoy?* http://www.ftc.gov/bcp/conline/features/chainmail.pdf.

FTC Consumer Alert 2002: *Email Address Harvesting: How Spammers Reap What You Sow*, Internet WWW-sivu, URL: http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.pdf.

FTC 2003: *False Claims in Spam*, Internet WWW-sivu, URL: http://www.ftc.gov/reports/spam/030429spamreport.pdf.

Gauthronet, Serge & Etienne Drouard 2001: *Unsolicited Commercial Communications and Data Protection*, Internet WWW-sivu, URL: http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamstudy_en.pdf.

Garfinkel, Simson; Schwarts, Alan 1999: *Internet ja roskaposti*. Helsinki: Suomen ATK-kustannus Oy

Goldman, Jim 2003: *Symantec Fights Evil Spammers: Bogus Offers of Cheap Security Software Could Open Your PC to Attack*, Internet WWW-sivu, URL: http://abcnews.go.com/sections/scitech/Business/techtv_symantecspam030625.html.

Graham, Paul 2003a: *Filters That Fight Back*, Internet WWW-sivu, URL: http://www.paulgraham.com/ffb.html.

Graham, Paul 2003b: *Filters That Fight Back Faq*, Internet WWW-sivu, URL: http://www.paulgraham.com/ffbfaq.html.

Graham, Paul 2003c: *Stopping Spam*, Internet WWW-sivu, URL: http://www.paulgraham.com/stopspam.html.

Graham-Cumming, John 2003: *Fooling and Poisoning Adaptive Spam Filtering*, Internet WWW-sivu, URL: http://www.sophos.com/sophos/docs/eng/papers/WP_PMFool_US.pdf.

Herbert, George William 2002: *Greeting Card Website*, Internet WWW-sivu, URL: http://mail-abuse.org/gc_rbl.html.

Hird, Shane 2002: *Technical Solutions for Controlling Spam*, Internet WWW-sivu, URL: http://security.dstc.edu.au/papers/technical_spam.pdf.

Jacobsson, Andreas & Carlsson, Bengt 2003: *Privacy and Spam: Empirical Studies of Unsolicited Commercial E-Mail*, Internet WWW-sivu, URL: http://www.cs.kau.se/IFIP-summerschool/preceedings/jacobsson.pdf.

Järvinen, Petteri 2000: *Sinulle on sähköpostia. Sähköpostin tehokäyttö*. Jyväskylä: Teknolit Oy.

Karvinen, Matias 1997: *SMTP*, Internet WWW-sivu, URL: http://www.tml.hut.fi/Studies/Tik-110.300/1998/Essays/smtp.html.

Kraut, Robert. E; Sunder, Shyam; Telang, Rahul; Morris, James 1999: *Pricing Electronic Mail To Solve the Problem of Spam*, Internet WWW-sivu, URL: http://www.som.yale.edu/Faculty/sunder/Email/PricingEmail.pdf.

Kupiainen, Jari 2002: *Internet ja translokaalit yhteisöverkostot Melanesiassa*, Internet WWW-sivu, URL: http://www.utu.fi/hum/mediatutkimus/paivat/kupiainenpaperi.html.

Lindberg, G. 1999: *RFC2505: Anti-Spam Recommendations for SMTP MTAs*, Internet WWW-sivu, URL: http://www.faqs.org/rfcs/rfc2505.html.

Lo, Joseph 2003: *Trojan Horse Attacks*, Internet WWW-sivu, URL: http://www.irchelp.org/irchelp/security/trojan.html.

Mail-Abuse MAPS 2000: http://mail-abuse.org.

Mark, Roy 2003: *Lawmakers: Spam Bill Is a Turkey*, Internet WWW-sivu, URL: http://www.Internetnews.com/bus-news/article.php/3113941.

NOIE 2002: *Spam*, Internet WWW-sivu, URL: http://www.noie.gov.au/publications/NOIE/spam/final_report/SPAMreport.pdf.

Nua Internet Surveys 2003: *One in Five European Seniors Online*, Internet WWW-sivu, URL: http://www.nua.com/surveys/index.cgi?f=VS&art_id=905358750&rel=true.

Nucleus 2003: *Spam: The Silent ROI Killer*, Internet WWW-sivu, URL: http://www.nucleusresearch.com/research/d59.pdf.

Olsen, Stefanie 2002: *Spam Blocklists Going too Far?* http://zdnet.com.com/2100-1106-943348.html.

Pastore, Michael 2000: *E-Mail Taking Over Office Communication*, Internet WWW-sivu, URL: http://cyberatlas.Internet.com/markets/professional/article/0,,5971_431931,00.htm.

Pastore, Michael 2001: *E-Mail Continues Dominance of Net Apps*, Internet WWW-sivu, URL: http://cyberatlas.Internet.com/big_picture/applications/article/0,,1301_808741,00.html.

Puolamäki, Kai 2002: *Ei-toivottu viestintä Internetissä*, Internet WWW-sivu, URL: http://www.cis.hut.fi/kaip/spam/.

Rice, Cindy M. 2002: Unsolicited Commercial E-mail: Why is it Such a Problem? *North Carolina Journal of Law & Technology*. 3:2.

Roberts, Paul 2002: *Holidays Bring 'Tsunami of Spam'*, Internet WWW-sivu, URL: http://archive.infoworld.com/articles/hn/xml/02/12/23/021223hnspam.xml?s=IDGNS.

Rubel, Mike 2003: *The Case for RMX Records*, Internet WWW-sivu, URL: http://www.mikerubel.org/computers/rmx_records/.

Saarni, Tero 1998: *Internet-sähköposti*, Internet WWW-sivu, URL: http://www.dc.turkuamk.fi/graduation/email-tsaarni.pdf.

Sauver, Joe 2003: *The Economics of Spam: the Spam Business Isn't Always What You'd Think*, Internet WWW-sivu, URL: http://cc.uoregon.edu/cnews/summer2003/spameconomics.html.

Schiavonne, Vincent, David Brussin, James Koenig, Stephen Cobb & Ray Everett-Church 2003: *Trusted Email Standard*. http://www.eprivacygroup.net/teos/TEOSwhitepaper1.pdf.

SMTP Protocol Overview 2004: http://www.freesoft.org/CIE/Topics/94.htm.

Sophos 2003: *Spam: a Many Rendered Thing*, Internet WWW-sivu, URL: http://www.sophos.com.au/sophos/docs/eng/papers/WP_PMSpam_US.pdf.

SORBS 2004: *Zombie/Hijacked Netblock Info*, Internet WWW-sivu, URL: http://www.dnsbl.au.sorbs.net/Zombie-FAQ.html.

Sorking, David 2003: *Spam Laws*, Internet WWW-sivu, URL: http://www.spamlaws.com/.

SpamCop 2003: Internet WWW-sivu, URL: http://www.spamcop.net/.

Spamhaus 2004: *The Spamhaus Block List FAQ*, Internet WWW-sivu, URL: http://www.spamhaus.org/sbl/sbl-faqs.lasso.

Tompsett, Brian 2003: *The Role of Insecured Proxies in Internet Abuse*, Internet WWW-sivu, URL: http://www.apcauce.org/meetings/030825/proceedings/Brian_Tompsett_Paper.pdf.

Trudeau, Paris; Cullen, Richard; Zwieback, Dave 2003: *Major Techniques for Classifying Spam*, Internet WWW-sivu, URL: http://www.surfcontrol.com/general/assets/whitepapers/4ClssfySpm_Apr03.pdf.

Trudeau, Paris 2003: *Fighting the New Face of Spam*, Internet WWW-sivu, URL: http://www.surfcontrol.com/general/assets/whitepapers/New_Face_of_Spam.pdf.

Vault.com 2000: *Email Behavior: Vault Workplace Survey*, Internet WWW-sivu, URL: http://www.vault.com/surveys/email_behavior/email_behavior.jsp.

Verisign 2003: *A Plan for No Spam*, Internet WWW-sivu, URL: https://www.verisign.com/resources/wp/spam/no_spam.pdf.

VISNETIC 2003: *Best of Class Anti-spam Solution*, Internet WWW-sivu, URL: http://imageserver.deerfield.com/marcom/visnetic_mailpermit/VisNetic_MailPermit_White_Paper_letter.pdf.

Westley, Christopher 2003: *The Economics of Spam*, Internet WWW-sivu, URL: http://www.fee.org/vnews.php?nid=5662.

Wired News 2003: *Kids Bombarded With Spam Porn*, Internet WWW-sivu, URL: http://www.wired.com/news/culture/0,1284,59164,00.html.

Wood, Paul 2003: *A Spammer in The Works*, Internet WWW-sivu, URL: http://security.iia.net.au/downloads/aspammerintheworks.pdf.