SvrVukk - Ei-toivottu viestintä Internetissä

Etusivu

Ryhmän sfnet.viestinta.roskapostit VUKK (FAQ)

Tälle sivulle on koottu **V**astauksia ryhmässä `sfnet.viestinta.roskapostit` **U**sein **K**ysyttyihin **K**ysymyksiin.

Sisällys

Yleistä uutisryhmään kirjoittamisesta

Ryhmän `sfnet.viestinta.roskapostit` kuvaus on:

> `sfnet.viestinta.roskapostit` Roskaviesteistä
>
> Ryhmä on tarkoitettu keskusteluun ns. SPAMmeistä eli eritasoisista sähköisistä massalähetyksistä joko uutisryhmiin, meilinä, tekstiviestinä tai vastaavilla tavoilla. Miten niihin tulisi suhtautua? Mitä teknisiä apuvälineitä on käytettävissä jne.
>
> Ryhmällä on kotisivu osoitteessa `http://www.iki.fi/kaip/spam/vukk.html`.

Ryhmään sfnet.viestinta.roskapostit kuuluu siis keskustelu sähköisesti lähetetystä roskapostista. Muita aiheeseen liittyviä ryhmiä:

- sfnet.atk.turvallisuus - Tietoturvakysymykset tietojenkäsittelyssä
- sfnet.atk.turvallisuus.kotikoneet - Kotikoneisiin liittyvät tietoturvakysymykset
- sfnet.keskustelu.kuluttaja - Kuluttajansuoja ja asema
- sfnet.keskustelu.laki - Lakiasiat ja oikeuskäytäntö Suomessa ja muualla
- sfnet.viestinta.meili - Sähköpostiin eli meiliin liittyvä keskustelu
- sfnet.viestinta.nyyssit - Keskustelua nyysseistä eli näistä uutisryhmistä

Lähetä viestisi **vain** siihen ryhmään, johon se sopii parhaiten. Sfnet-ryhmien kuvaukset löytyvät Sfnetin kotisivulta.

Lue ennen nyysseihin postaamista ainakin Jaana Heinon Seitsemän ohjetta nyysseihin kirjoittajalle tai Jukka Korpelan Seitsemän kieltoa nyysseihin kirjoittajalle, jotta vältät tavallisimmat netikettivirheet.

Tarkista tästä VUKKista ja Googlen webbi- ja nyyssihakukoneesta, että kysymykseesi ei ole vastattu tyydyttävästi aikaisemmin tai että argumenttiasi ei ole käsitelty puhki viimeksi edellisessä kuussa. Googlen avulla voi myös tarkistaa, onko joku muu saanut samanlaisen spämmin valitsemalla uutisryhmäksi `news.admin.net-abuse.sightings`.

Jos haluat puolustaa spämmäystä, niin lue ensin SpammerienKootutSelitykset.

Jos kysyt jotakin, niin pyri antamaan **riittävät tiedot**, jotta kysymykseen voidaan vastata. Jos olet esimerkiksi saanut spämmin ja haluat pyytää apua sen alkuperän ja oikean valitusosoitteen selvittämisessä, niin liitä artikkeliisi spämmiviestin täydelliset otsaketiedot.

Vältä kuitenkin turhaa postausta. Spämmin koko sisältöä ei ole yleensä tarpeen postittaa suomalaisessa roskapostiryhmässä, paitsi jos se on jostain syystä oleellista käsiteltävänä olevalle asialle. Poikkeuksen tähän muodostaa **kotimainen spämmi**, joka kannattaa julkaista kokonaisuudessaan joko ryhmässä `sfnet.viestinta.roskapostit` tai `news.admin.net-abuse.sightings`.

Julkaise mahdollisuuksien mukaan saamasi spämmi ryhmässä `news.admin.net-abuse.sightings` (NANAS). Spämmiviestin voi lähettää NANASiin kätevästi spämmivalituksen yhteydessä lähettämällä viestistä kopioi osoitteeseen news-admin-net-abuse-sightings@moderators.isc.org (ohjeet, esimerkki). Julkaistuista spämmeistä on hyötyä spämmikampanjan laajuuden tai pitkäkestoisuuden osoittamisessa. Tästä syystä varsinkin kaikki kotimainen spämmi kannattaa julkaista.

Mitä spämmäys tarkoittaa?

Spämmäys tarkoittaa saman viestin lähettämistä usealle vastaanottajalle tai useaan uutisryhmään ilman vastaanottajien ennakkosuostumusta tai hyväksyntää, viestin sisällöstä riippumatta.

Sähköpostispämmi

Tarkkaa rajaa sille sähköpostiviestien määrälle, jonka jälkeen kyseessä on spämmäys, ei voi antaa. Erään vakavasti otettavan mielipiteen mukaan sähköpostiviesti on spämmiä, jos oleellisesti samasisältöinen meili on lähetetty 24 tunnin aikana vähintään 25 vastaanottajalle ilman vastaanottajien ennakkosuostumusta.

Sähköpostiviesti on siis spämmiä (Unsolicited Bulk Email, UBE), jos *kaikki* seuraavista ehdoista toteutuvat:

- Viestejä on lähetetty usealle vastaanottajalle
- Viestien oleellinen sisältö on sama
- Viestien lähettämiselle ei ole vastaanottajien ennakkosuostumusta tai hyväksyntää

Viestien sisällöllä ei ole spämmin määritelmän kannalta väliä. Yleensä spämmiviestin sisältö on kaupallinen mainos (Unsolicited Commercial Email, UCE), mutta viestin sisältö voi olla myös esimerkiksi hyvää onnea toivottava ketjukirje, poliittinen tai uskonnollinen sanoma tai hyväntekeväisyysjärjestön rahankeräysviesti.

Viestin laillisuus ei myöskään ole spämmin määritelmän kannalta oleellinen. Spämmäystä koskeva lainsäädäntö vaihtelee maittain. Esimerkiksi Suomessa spämmäys voi olla joskus laillista (esim. ei-kaupallinen massapostitus), toisaalta kaikki laiton sähköpostimainonta ei ole spämmäystä (esim. yksittäinen yksityishenkilölle lähetetty sähköpostimainos).

Sähköpostispämmin määrästä on esitetty useita arvioita. Esimerkiksi MessageLabsin mukaan lokakuussa 2004 76 % sähköpostista oli spämmiä. Ilmiön luonteen vuoksi arviot ovat kuitenkin epätarkkoja eivätkä aina vertailukelpoisia. Yksi pisimmän linjan arvioijista oli Brightmail, jonka arvioita spämmin osuudesta kaikesta sähköpostista vuosina 2001-2004 on esitetty alla.

Kuukausi	**Spämmin osuus kaikesta sähköpostista**
Heinäkuu 2004	65 %
Kesäkuu 2004	65 %
Toukokuu 2004	64 %
Huhtikuu 2004	64 %
Maaliskuu 2004	63 %
Helmikuu 2004	62 %
Tammikuu 2004	60 %
Joulukuu 2003	58 %
Marraskuu 2003	56 %
Lokakuu 2003	52 %
Syyskuu 2003	54 %
Elokuu 2003	50 %
Heinäkuu 2003	50 %
Kesäkuu 2003	49 %
Toukukuu 2003	48 %
Huhtikuu 2003	46 %
Maaliskuu 2003	45 %

Kuukausi	Spämmin osuus kaikesta sähköpostista
Helmikuu 2003	42 %
Tammikuu 2003	42 %
Joulukuu 2002	41 %
Syyskuu 2002	38 %
Helmikuu 2002	17 %
Syyskuu 2001	8 %

Spamlinks.netin sivulla on linkki suureen joukkoon tilastoja. 27.1.2006 kaikesta sähköpostista on spämmiä Postinin mukaan 71 %, MessageLabsin 68 %, DCC:n 54 %, Proofpointin mukaan yhteensä 68 % postista on spämmiä tai viruksia ja Ipswitchin prosentti on 74 %. Hajonta prosenttiluvuissa on suurta johtuen erilaisista mittaustavoista ja tiedonlähteistä, mutta kaikki ovat yksimielisiä siitä, että yli puolet sähköpostiviestinnästä on spämmiä.

Outona lintuna muiden joukossa Liikenne- ja viestintäministeriö (LVM) tiedotti 13.12.2005, että "Suomessa oli vuonna 2003 välitetyistä sähköpostiviesteistä roskapostia arviolta 80 prosenttia ja tänä vuonna enää noin kolmannes" - siis 33 %. Tiedote uutisoitiin laajalti.

Vuonna 2003 kahta ei-roskapostiviestiä kohden siis välitettiin LVM:n mukaan kahdeksan roskapostiviestiä ja vuonna 2005 kahta ei-roskapostiviestiä vastasi enää vain yksi roskaposti. Jos ei-roskapostiviestien määrä on 2003-2005 pysynyt suunnilleen vakiona, tarkoittaa tämä sitä, että LVM väittää spämmin määrän romahtaneen kahdessa vuodessa kahdeksasosaan entisestään.

LVM:n julkaisemalla Roskapostipaketti.fi -sivulla esitetään toinenkin käyrä, otsikolla "haitallisen sähköpostin määrän kehitys, välitetty liikenne - Viestintäviraston arvio":

-	2003	2004	2005
Muu maailma	90 %	60 %	50 %
Suomi	80 %	45 %	33 %

Viestintäviraston selvityksestä 2.3.2006 paljastui, että LVM:n spämmiluvut olivat hatusta vedettyjä. Ministeriön esittelemä suuri pudotus roskapostin määrässä oli saatu yhdistämällä vuoden 2003 huippuarvo kahden seuraavan vuoden keskiarvoihin. Tilastonikkaroinnin syy on epäselvä, eikä ministeriö ole julkaissut oikaisua. Roskapostin määrän väheneminen on yksi ministeriön tulostavoitteista.

(LVM:n roskapostilukuihin liittyviä asiakirjoja.)

Nyyssispämmi

Uutisryhmäspämmi määritellään yleensä niin sanotun Breidbartin indeksin (BI) avulla. Breidbartin indeksi lasketaan oleellisesti samanlaisista nyyssipostauksista, jotka on tehty 45 vuorokauden aikana. Breidbartin indeksi on niiden uutisryhmien määrän, joihin artikkeli on crosspostattu, neliöjuurien summa. Esimerkkejä:

- Jos oleellisesti samansisältöinen artikkeli postataan yhteen uutisryhmään viikottain (yhteensä seitsemän erillistä artikkelia 45 vuorokauden aikana), on postauksen Breidbartin indeksi *BI=sqrt(1)+sqrt(1)+sqrt(1)+s*
- Jos artikkelista on lähetetty kaksi kopiota, josta toinen on crosspostattu kolmeen uutisryhmään ja toinen neljään uutisryhmään, on Breidbartin indeksi *BI=sqrt(3)+sqrt(4)=1,73+2=3,73*.
- Yhden seitsemään uutisryhmään crosspostatun artikkelin Breidbartin indeksi on *BI=sqrt(7)=2,65*.

Nyyssiartikkelin postaaminen crosspostauksella ei siis ole niin paha asia kuin saman artikkelin postaaminen erikseen useaan ryhmään, koska nyyssipalvelimet ja -ohjelmat käsittelevät crosspostattua artikkelia yhtenä artikkelina. Yhteenvetona: jos nyyssiartikkelin postaamiselle useaan ryhmään on oikeasti hyvä syy, niin käytä crosspostausta.

Sfnettiin lähetetty viesti on spämmiä ja se voidaan cancelloida automaattisesti, jos sen Breidbartin indeksi on vähintään noin kuusi (eli jos sama viesti on esimerkiksi lähetetty kuuteen uutisryhmään ilman crosspostausta). Kansainvälisissä hierarkioissa cancellointiraja on noin BI=20.

Muut häiritsevät viestit

Viesti voi olla häiritsevä, vaikka se ei olisikaan spämmi. Esimerkkeinä tästä ovat nyysseihin postatut binääriviestit (poislukien ryhmät, joihin binäärien postaus on erikseen sallittu) ja mainokset, jotka on lähetetty väärään uutisryhmään. Sen lisäksi, että vääriin uutisryhmiin lähetetyt nyyssimainokset ovat törkeää käytöstä, kuluttaja-asiamies on kieltänyt elinkeinonharjoittajia lähettämästä tällaisia mainoksia.

Lisätietoja

- NANAE FAQ: What is SPAM?
- The Spamhaus Project: The Definition of Spam

Onko spämmäys laitonta?

Spämmäyksen laillisuudesta kerrotaan tyhjentävästi sivulla SpamLaki.

Miksi spämmi on paha?

Internet-viestinnän ja perinteisen viestinnän yksi suurista eroista on, että Internet-viestinnässä saman viestin lähettäminen jopa sadoille tuhansille tai miljoonille vastaanottajille on suhteellisen helppoa eikä se maksa käytännössä mitään. Kulut maksaa viime kädessä vastaanottaja Internet-yhteysmaksuinaan ja viestien lukemiseen kuluvana aikana. Perinteistä mainontaa kannattaa yrittää kohdentaa todennäköisimmille asiakkaille, koska mainosten lähettämisestä aiheutuu kuluja mainostajalle. Spämmiä voi sen sijaan halvalla ja "huoletta" lähettää huomattavasti laajemmallekin kohderyhmälle.

Tämä verkon rakenteesta johtuva kustannusrakenne (vastaanottaja maksaa) ja viestien lähettämisen helppous on pääsyynä siihen, miksi ei-toivotusta massaviestinnästä tulee helposti suuri ongelma.

Euroopan komission mukaan spämmäys maksaa Internetin käyttäjille kymmenen miljardia euroa vuodessa. Spämmin vastaanottamisesta aiheutuu useiden eri arvioiden mukaan keskimääräiselle käyttäjälle suuruusluokaltaan parin euron kulut kuukaudessa. Spämmi on siis pohjimmiltaan taloudellinen ongelma: viestien lähettäminen on hyvin halpaa, mutta vastaanottaminen kallista.

Eräiden arvioiden mukaan jo yli puolet sähköpostiviestinnästä on spämmiä. Monen sähköpostilaatikko on muuttunut käyttökelvottomaksi roskapostin takia. Lisäksi on nähtävissä, että spämmi haittaa vakavasti sähköisen viestinnän käyttöä myös toisella tapaa: ihmiset eivät uskalla roskapostin saamisen pelossa antaa yhteystietojaan silloinkaan kuin se olisi aiheellista. Jos ihmisillä on pienikin epäilys, että sähköpostiosoitetta tullaan käyttämään ei-toivottujen mainosten lähettämiseen, ei osoitetta anneta yhteystiedoksi. Tämä uhkaa koko sähköpostijärjestelmän toimivuutta. Sähköisen viestinnän kehittymiselle on tärkeää, että ihmiset uskaltavat antaa sähköiset yhteystietonsa.

Lisäksi:

- Henkilökohtainen sähköpostilaatikko on tarkoitettu henkilökohtaiseen viestintään, ei joillekin edulliseksi tavaksi mainostaa tuotteita ja palveluja. Vastaanottajan ja vastaanottajan Internet-palveluntarjoajan sähköpostijärjestelmä on yksityistä omaisuutta. Sähköpostilaatikko ei ole "julkinen ilmoitustaulu", johon jokainen saa käydä niittaamassa haluamiaan ilmoituksia.
- Spämmi kuormittaa verkkoa ja varsinkin sähköposti- ja nyyssijärjestelmää.
- Spämmäys aiheuttaa lisäkuluja Internet-palveluntarjoajille ja näiden asiakkaille myös spämmistä aiheutuvien valitusten vuoksi. Usein spämmin otsikkotietoja on yritetty väärentää, jolloin valitukset ja virheilmoitukset voivat mennä väärään osoitteeseen.

- Spämmäämällä mainostetut tuotteet tai palvelut ovat usein kyseenalaisia (pyramidiskeemoja, huijauksia, ihmelaihdutuslääkkeitä, ...). FTC:n mukaan kahdessa kolmesta spämmiviestistä on harhaanjohtavia väitteitä.
- Ei-toivotun bulkkisähköpostin säätelemiseksi ei ole toimivia mekanismeja. Ainoa oikeasti toimiva tapa käyttää sähköpostia bulkkimainontaan ovat opt-in-sähköpostilistat, joissa listalla olijat ovat pyytäneet yksiselitteisesti tulla liitetyksi postituslistalle.
- Spämmäys voi olla laitonta, ks. SpamLaki.

Lisätietoja

- CAUCE: About the Problem
- Spam.abuse.net: Why is spam bad?
- Gartner Groupin tutkimus suhtautumisesta spämmiin ja sen kustannuksista
- Euroopan komission tiedonanto ei-toivotusta kaupallisesta viestinnästä eli roskapostista ("spam")

Voiko sähköpostitse tai nyysseissä mainostaa?

Sähköpostia ja nyyssejä voi käyttää mainontaan, kunhan noudattaa lakeja ja yleisesti hyväksyttyjä käyttäytymissääntöjä. Muuten voi varautua hyvän karman huomattavaan vähenemiseen ja mahdollisesti vastaamaan teoistaan oikeudellisesti ja/tai rahallisesti.

Sähköpostimainonta

Sähköpostimainonta on yleensä hyväksyttävää vain, jos mainosten vastaanottajat ovat antaneet sille yksiselitteisen suostumuksensa (opt-in).

Nyyssimainonta

Nyyssimainonnassa on tärkeää kaikenlainen toiston välttäminen (ilmoita vain uutisryhmän aihepiiriin kuuluvista uutuuksista, mitään hinnastoja tai viikottaisia postauksia ei ole syytä lähettää), tarkka uutisryhmien valinta (mieluumin vain yksi ryhmä, ja sekin ilmoitusryhmä, jos sellainen on), crosspostauksen käyttö ja vastausten ohjaaminen yhteen uutisryhmään Followup-To-headerikentän avulla. Viestin on hyvä olla lyhyt ja selkeä ja sen pitää kuluttaja-asiamiehen ohjeen mukaan ilmetä mainokseksi jo otsikosta. On hyvä muistaa, että keskusteluryhmät ovat olemassa ensisijaisesti keskustelua varten, eivät siksi, että ne olisivat joillekin edullinen ilmoituskanava.

Ehkä paras tapa mainostaa nyysseissä on kirjoittaa mielenkiintoisia artikkeleja ja lisätä mainos omien nyyssiartikkelin signatureen.

Lisätietoja

- Lars Wirzeniuksen kirjoitus Tehokas tiedottaminen Internetissä
- Jukka Korpelan kirjoitus Nyyssien kaupallisesta käytöstä
- Spam.abuse.netin ohje
- Euroopan komission raportissa annetaan hyvä yhteenveto opt-in-markkinoinnin mahdollisuuksista.
- Kuluttajaviraston kirje erään nyyssispämmin johdosta

Mitä postituslistalta vaaditaan? (Eli miten lähetän bulkkisähköpostia laillisesti)

Postituslista muodostaa henkilörekisterin, jonka käyttöä säätelee henkilötietolaki ja jonka keräämiseen saatetaan vaatia muun muassa rekisteriseloste ja ennakkoilmoitus tietosuojavaltuutetulle. Postituslistan käyttöä markkinointiin säätelee lisäksi sähköisen viestinnän tietosuojalaki ja kuluttajansuojalaki.

Ainoa hyväksyttävä tapa käyttää massasähköpostilähetyksiä ovat *opt-in*-postituslistat. Kunniallisen postituslistan on täytettävä seuraavat vähimmäisvaatimukset, joiden noudattamista vaatii ainakin osittain myös laki:

- Massasähköpostilähetyksiä saa lähettää vain sellaisille henkilöille, jotka ovat antaneet siihen yksiselitteisen suostumuksensa ("opt-in"). Kuluttaja-asiamiehen mukaan suostumuspyyntö markkinointiaineiston lähettämiseen on muotoiltava niin, että kuluttaja tietää minkälaista ja kuinka laajaa markkinointiaineistoa hän voi odottaa saavansa.

- Ennen sähköpostiosoitteen lisäämistä postituslistalle on varmistuttava siitä, että postituslistan tilaaja on todella annetun sähköpostiosoitteen omistaja. Tämän varmistuksen voi tehdä monella tapaa. Useimmat postituslistaohjelmistot tekevät varmistuksen varmistuksen automaattisesti: käyttäjä liitetään listalle vasta sen jälkeen, kun hän on reagoinut liittymispyynnön seurauksena omaan sähköpostiosoitteeseensa lähetettyyn vahvistusviestiin. Jos mainosten vastaanottaja väittää, että hän ei ole antanut suostumusta markkinointiaineiston lähettämiseen, on todistustaakka suostumuksen olemassaolosta mainostajalla. Jos muutkin kuin sähköpostiosoitteen omistaja voivat antaa suostumuksen markkinointiaineiston lähettämiseen tähän sähköpostiosoitteeseen, ei mainostaja voi mitenkään väittää, että juuri sähköpostiosoitteen omistaja olisi antanut luvan mainosten lähettämiseen.

- Postituslistalta poistumisen pitää olla helppoa ja vaivatonta.

- Nimiä ja sähköpostiosoitteita ei saa luovuttaa kolmansille osapuolille ilman rekisteröityjen suostumusta.

- Postituslistaa saa käyttää vain siihen tarkoitukseen, johon rekisteröity on antanut luvan (mm. henkilötietolain 7 §: käyttötarkoitussidonnaisuus).

- Henkilötietolain 25 § mukaan suoramarkkinointimateriaalissa on ilmoitettava käytetyn henkilörekisterin nimi, rekisterinpitäjä ja tämän yhteystiedot.

- Voi olla järkevää tallentaa tiedot listalle liittymisistä (missä yhteydessä, mistä IP-osoiteesta ja milloin liittymispyyntö tehtiin, koska vahvistusviesti vastaanotettiin jne.). Nämä tiedot voivat olla hyödyllisiä, jos listanpitäjää epäillään väärinkäytöksistä, kuten ihmisten lisäämisestä postituslistalle ilman heidän suostumustaan. Varsinkin laajalevikkisten listojen yhteydessä joku unohtaa kuitenkin liittyneensä listalle tai useampi henkilö on käyttänyt samaa sähköpostiosoitetta toisistaan tietämättä. On hyvä muistaa, että riitatapauksissa todistustaakka suostumuksen olemassaolosta on rekisterinpitäjällä.

Suomen laki ei kiellä muille kuin luonnollisille henkilöille (yritykset ja yhteisöt) lähetettyä spämmiä. Yritys- ja yhteisömainonnassakin on kuitenkin otettava huomioon mm. henkilötietolaki. Lisäksi selvitysvelvollisuus siitä, kuuluuko sähköpostiosoite luonnolliselle henkilölle vai ei, on mainostajalla. Lähtökohtaisesti myös yrityksen työntekijöiden osoitteet (`etunimi.sukunimi@yritys.example`) kuuluvat luonnollisille henkilöille, eikä niihin saa lähettää mainoksia ilman vastaanottajien ennakkosuostumusta. Rooliosoitteet, kuten `myynti@yritys.example`, kuuluvat sen sijaan selvästi muille kuin luonnollisille henkilöille. Yritysten ja yhteisöjen spämmäys voi siis olla joissain tapauksissa laillista, mutta se on silti epäeettistä liiketoimintaa.

Sähköpostiosoitteiden käyttöä kannattaa suunnitella jo niitä kerättäessä, tätä edellyttää myös henkilötietolaki (käyttötarkoitussidonnaisuus). Toisin sanoen, lupa mainosten lähettämiseen kannattaa pyytää jo henkilötietojen keräämisen yhteydessä.

Opt-out (mainosten lähettämiseen ei ole vastaanottajan suostumusta, mutta vastaanottaja voi halutessaan aina erikseen kieltää mainosten lähettämisen) ei ole toimiva ratkaisu:

- Kokemus on osoittanut, että spämmerit käyttävät poistopyyntöjä osoitelähteenä spämmäykseen. Tietenkään yksikään spämmeri ei julkisesti myönnä syyllistyvänsä tällaiseen. Miksi spämmin vastaanottajan pitäisi uskoa, että juuri sinä (jos olet lähettänyt spämmiä) et syyllistyisi poistopyynnöistä tai spämmivalituksista kerättyjen osoitteiden spämmäykseen, kun jopa Financial Times on syyllistynyt tällaiseen? Eikä listalta poistuminen ole useinkaan niin helppoa kuin spämmeri antaa ymmärtää. Poistumispyynnön jättäminen voi esimerkiksi vaatia nettiyhteyden avaamista kommunikaattorilla. Ihmisillä voi olla useita sähköpostisoitteita - pitäisikö ne kaikki "poistaa" listoilta?
- Jos jokainen mainostaja lähettäisi yhdenkin spämmin kaikille, riittäisi se tukkimaan sähköpostijärjestelmän.
- Jokaisen spämmerin opt-out-listalle hankkiutuminen ei ole käytännöllistä tai edes mahdollista. Erilaisille opt-out-listoille hankkiutuminen olisi kokopäiväinen työ. (Opt-out-periaate on esimerkki siitä, miten spämmerit haluavat siirtää kaikki kulut ja vaivat spämmäyksen uhreille. Vastaanottajat maksavat spämmäyksestä aiheutuneet kulut. Opt-out-periaate tarkoittaa, että spämmin vastaanottajien pitäisi myös nähdä vaivaa spämmerien yleensä laittomien henkilörekisterien ylläpitämiseksi.)

Lisätietoja

- MAPS: Guidelines for proper mailing list management
- NANAE FAQ: Advertising by email
- The Spamhaus Project: Mailing Lists -vs- Spam Lists

Sain spämmin. Mitä minun pitäisi tehdä?

Katso sivua SpammiinReagoiminen.

Miten voin suodattaa spämmit pois automaattisesti?

Katso sivua SpammiltaSuojautuminen.

Keksin uuden tavan ratkaista spämmiongelma!

> Olen keksinyt uuden ratkaisun spämmiongelmaan. Spämmin tulo loppuu, kun tietokoneesta irrottaa verkkojohdon!

Usein näkee ehdotettavan mitä erilaisimpia keinoja spämmiongelman ratkaisemiseksi. Edellä mainitulla ratkaisulla (verkkojohdon irrottaminen) - kuten monilla muillakin "ratkaisuilla" - on ilmeiset huonot puolensa. Ehdotettuja ratkaisuja on melkein aina esitetty monta kertaa aikaisemmin.

Sivulla SpammerienKootutSelitykset on lueteltu joitakin usein ehdotettuja "ratkaisuja" spämmiongelmaan, kuten:

- "Spämmi on helppo tuhota"
- "Meidän listaltamme pääsee helposti pois"
- "Osoitteesihan oli julkinen!"
- "Spämmistä pääsee eroon vaihtamalla sähköpostiosoitteen"

Millaisen hyvän ratkaisun spämmiongelmaan pitäisi siis olla?

Aluksi on hyvä muistaa sähköpostijärjestelmän perussuunnitteluperiaatteet, joita ovat muun muassa:

- Jokainen voi helposti ja maksutta lähettää jokaiselle sähköpostiviestin.
- Sähköpostiviestintä on luotettavaa. Sähköpostin lähettäjä voi olla varma siitä, että vastaanottaja *joko* saa viestin *tai* lähettäjä saa virheilmoituksen, jossa kerrotaan, että viestiä ei voitu toimittaa perille. Sähköposti ei siis "katoa mustaan aukkoon".

Hyvän ratkaisun spämmiongelmaan tulee mahdollisuuksien mukaan säilyttää edellä mainitut sähköpostijärjestelmän perussuunnitteluperiaatteet. Kun spämmiongelmaan mietitään ratkaisuja, tulee hyödyn (spämmin väheneminen) olla tasapainossa haittojen (viestinnän vaikeutuminen, sähköpostijärjestelmän perussuunnitteluperiaatteiden romuttaminen) kanssa.

Spämmiongelman ratkaisukeinot voi jakaa ainakin seuraaviin luokkiin:

- Yhteisöllinen vaikuttaminen. Internetissä on vahva spämmin vastainen kulttuuri. Käyttäjäyhteisö valistaa muita käyttäjiä, palveluntarjoajia ja mainostajia. Tarvittaessa vaikuttamiseen voidaan käyttää estolistoja ja kuluttajaboikotteja.
- Tekniset keinot:
  - Suodatus. Spämmiongelmaa voi yrittää lievittää suodattamalla roskapostia. Suodattaminen ei välttämättä ole helppoa eikä ilmaista. Täydellistä spämmisuodatinta, joka suodattaisi kaikki spämmit, mutta ei muuta kuin spämmiä, ei ole olemassa.
  - Sähköpostijärjestelmän kehittäminen. Postinvälityksen arkkitehtuuriin on esitetty monen kaltaisia muutoksia. Jotkut ehdotuksista ovat hyviä, useimmat huonoja. Esimerkkejä ehdotuksista:
    - Daniel Bernsteinin Internet Mail 2000
    - Microsoftin Sender ID -ehdotus, joka kaatui siihen, että Microsoft väitti omistavansa ehdotuksen toteuttamiseen tarvittavia ohjelmistoideapatentteja, joita ei olisi saanut vapaasti käyttää standardin toteuttamiseen
- Internet-palveluntarjoajat. Internet-palveluntarjoajien käyttöehdot kieltävät yleensä spämmäyksen.
- Viranomaistoiminta. Viranomaiset valvovat, että spämmäyksen kieltäviä lakeja noudatetaan.
- Yhteiskunnallinen vaikuttaminen. Spämmiasioissa vaikuttavia järjestöjä ovat muun muassa EuroCAUCE ja EFFI.

Edellä mainitut keinot eivät ratkaise roskapostiongelmaa kokonaan, mutta yhdessä ne kuitenkin mahdollistavat tehokkaan puuttumisen asiaan.

Erilaiset spämmisuodattimet ovat tällä hetkellä luultavasti useimmille helpoin keino helpottaa spämmiongelmaa. **Hyvän spämmisuodattimen ainoa suunnittelukriteeri ei voi olla mahdollisimman vähäinen läpi päässeen spämmin määrä.** Mitä ominaisuuksia hyvältä spämmisuodattimelta voi vaatia:

- Suodatin ei estä muiden kuin spämmiviestien vastaanottamista (ei "vääriä positiivisia", ilman tätä ominaisuutta verkkojohdon irrottaminen olisi helpoin ratkaisu)
- Suodatin estää spämmiviestien vastaanottamisen (ei "vääriä negatiivisia")
- Suodatin vaikeuttaa mahdollisimman vähän tavallista viestintää (viestintä voi esimerkiksi vaikeutua kohtuuttoman paljon, jos vastaanottajalla käytössä on vahvistuspyyntöviestejä lähettävä suodatin)

- Suodatin ei aiheuta haittaa kolmansille osapuolille (Esimerkiksi monet sähköpostivirusten suodatusohjelmat lähettävät virusvaroituksen viestin lähettäjälle, vaikka suodatusohjelman tekijät tietävät, että kyseinen haittaohjelma väärentää lähettäjän sähköpostiosoitteen. Parempi vaihtoehto olisi esimerkiksi tallettaa viesti (haittaohjelma poistettuna) viestin vastaanottajan spämmikansioon.)
- Suodatin toimii luotettavasti (tästä syystä ostettu suodatuspalvelu voi olla parempi kuin itse rakennettu, jos ei halua käyttää aikaa spämmisuodattimen ylläpitoon)
- Suodatin ei vaaranna sähköpostiviestinnän luotettavuutta (luotettavuus tarkoittaa sitä, että sähköpostin lähettäjä voi olla varma siitä, että vastaanottaja ”joko” saa viestin ”tai” lähettäjä saa virheilmoituksen, jossa kerrotaan, että viestiä ei voitu toimittaa perille)
- Suodatin ei vaaranna viestinnän luottamuksellisuutta (suodatin ei saa esimerkiksi lähettää suodattimen ylläpitäjälle kopiota jokaisesta sähköpostiviestistä suodatussääntöjen kehittämistä varten)
- Suodattimen käyttö ei kasvata viestinnän kustannuksia (muuten kannattaisi palkata sihteeri käymään sähköpostiviestit läpi)

Täydellistä suodatinta, joka toteuttaisi kaikki edellä luetellut ehdot, ei ole olemassa. Vaikka täydellistä ratkaisua spämmin suodattamiseen ei olekaan olemassa, on spämmin suodattamiseen kuitenkin saatavana tehokkaita ja varsin hyviä vaihtoehtoja, jotka suurimmaksi osaksi täyttävät edellä luetellut ehdot.

Alla on suomennettuna arviointilomake spämmiongelman ratkaisuille (alkuperäinen tekijä tuntematon), hiukan mukailtuna. Arviointilomake on kirjoitettu kieli poskessa, mutta se voi silti olla monessa tapauksessa varsin valaiseva.

```
SPÄMMIONGELMAN RATKAISUN HYLKÄYSKIRJE

Artikkelisi ehdottaa
 ( ) teknistä
 ( ) oikeudellista
 ( ) taloudellista
 ( ) oman käden oikeuteen perustuvaa
ratkaisua spämminvastaiseen taisteluun. Ajatuksesi ei toimi. Kerron,
miksi se ei toimi:

 ( ) Spämmerit voivat käyttää sitä sähköpostiosoitteiden keräämiseen
 ( ) Se vaikuttaisi postituslistoihin ja muihin oikeutettuihin
     sähköpostin käyttötarkoituksiin
 ( ) Kukaan ei voi löytää sitä tyyppiä tai rahastaa häntä
 ( ) Se on haavoittuvainen brute force -hyökkäykselle
 ( ) Se pysäyttää spämmin kahdeksi viikoksi ja sen jälkeen olemme
     lirissä sen kanssa
 ( ) Sähköpostin käyttäjät eivät hyväksy sitä
 ( ) Microsoft ei hyväksy sitä
 ( ) Poliisi ei hyväksy sitä
 ( ) Vaatii liikaa yhteistyötä spämmereiltä
 ( ) Vaatii välitöntä ja täydellistä yhteistyötä kaikilta
 ( ) Monilla sähköpostin käyttäjillä ei ole varaa vaarantaa
     yritystoimintaansa tai vieraannuttaa potentiaalisia työnantajia
 ( ) Spämmerit eivät välitä listoillaan olevista toimimattomista
     osoitteista
 ( ) Kuka tahansa voisi anonyymisti tuhota kenen tahansa uran tai
     yrityksen
```

Erityisesti, suunnitelmasi ei ota huomioon

( ) Sitä erityisesti kieltäviä lakeja
( ) Sähköpostia valvovan tahon puuttumista
( ) Ulkomailla olevia avoimia releitä
( ) Kaikkien numeroista ja kirjaimista koostuvien
    sähköpostiosoitteiden kokeilun helppoutta
( ) Typeryksiä
( ) Eri maiden erilaisia oikeusjärjestelmiä
( ) Uusien verojen vähäistä suosiota
( ) Uusien outojen rahamuotojen hyväksymisen vaikeutta
( ) Valtavaa olemassa olevaa investointia nyikyiseen
    sähköposti-infrastruktuuriin
( ) Muiden protokollien kuin SMTP:n haavuittuvuutta hyökkäykselle
( ) Käyttäjien haluttomuutta asentaa sähköpostitse saapuneita
    käyttöjärjestelmäpäivityksiä
( ) Laajakaistayhteyksiin kiinnitettyjen haittaohjelmien
    saastuttamien Windows-koneiden armeijaa
( ) Ikuista kaikkiin suodatusmenetelmiin liittyvää kilpavarustelua
( ) Spämmin äärimmäistä kannattavuutta
( ) Joe-jobeja ja/tai identiteettivarkauksia
( ) Tekniikasta mitään ymmärtämättömiä poliitikkoja
( ) Spämmereitten kanssa asioivien tyhmyyttä
( ) Spämmereitten epärehellisyyttä
( ) Tietoliikennekaistan käytöstä aiheutuvia kustannuksia, joihin
    vastaanottajan suorittama suodatus ei vaikuta
( ) Outlookkia

ja myös seuraavat filosofiset vastaväitteet voivat olla relevantteja:

( ) Ehdottamasi kaltaisia ajatuksia on helppo keksiä, silti mikään
    niistä ei koskaan ole osoittautunut käytännölliseksi
( ) Mikään opt-out-periaatteeseen pohjautuva menetelmä ei ole
    hyväksyttävä
( ) Sähköpostin otsaketietoja ei pitäisi säädellä lailla
( ) Mustat listat ovat huono asia
( ) Valkoiset listat ovat huono asia
( ) Meidän pitäisi voida keskustella Viagrasta ilman sensuuria
( ) Tili- tai luottokorttipetoksen ei pitäisi sisältyä vastatoimiin
( ) Julkisten verkkojen sabotoinnin ei pitäisi sisältyä vastatoimiin
( ) Vastakeinojen pitäisi toimia, jos ne otetaan käyttöön vaiheittain
( ) Sähköpostin lähettämisen pitäisi olla ilmaista
( ) Miksi meidän pitäisi luottaa sinuun ja palvelimiisi?
( ) Epäyhteensopivuus avoimen lähdekoodin tai avoimen lähdekoodin
    lisenssien kanssa
( ) Näennäiset vain tekemisen vuoksi tehdyt ratkaisut eivät ollenkaan
    auta ongelman ratkaisussa
( ) Väliaikaiset/kertakäyttöiset sähköpostiosoitteet ovat kömpelöitä
( ) En halua virkavallan lukevan sähköpostejani
( ) Ratkaisu on liian lempeä

Lisätietoja

- SpammiltaSuojautuminen - lisätietoa spämmisuodattimista
- Bruce Schneier: The Economics of Spam, Crypto-Gram 15.2.2004 - Bruce Schneier kommentoi joitakin ehdotuksia
- Brad Templeton: The Spam Solutions - Yksi näkemys eri spämmiongelman ratkaisuehdotuksista (huomautettakoon, että tämän VUKKin kirjoittaja ei ole kaikista Templetonin teeseistä samaa mieltä, Templeton ei esimerkiksi kannata spämmäyksen kieltävää lainsäädäntöä)

Spämmissä sanottiin, että se ei ole spämmiä, spämmäys on laillista tai muuten vain uhkailtiin

Jos meilissä sanotaan ensimmäisellä rivillä, että se ei ole spämmiä, niin silloin se on melkein varmasti spämmiä.

Spämmeissä viitataan usein amerikkalaiseen lainsäädäntöön, jonka väitetään sallivan spämmäyksen. Usein spämmerit viittaavat rauenneisiin tai vasta vireillä oleviin lakiehdotuksiin Joka tapauksessa Suomessa spämmäys on laitonta.

Joskus spämmeissä esitetään erilaisia uhkauksia siitä, mitä tulee tapahtumaan, jos spämmistä erehtyy valittamaan. Uhkaukset kannattaa yleensä jättää omaan huumoriarvoonsa. Jos uhkaukset ovat vakavia (mikä onneksi kuitenkin lienee erittäin harvinaista) - esimerkiksi henkeä tai terveyttä koskevia - niin silloin asiasta voi olla syytä tehdä rikosilmoitus.

Mikä on avoin rele (open relay) ja miten se korjataan? Entä avoin välityspalvelin (open proxy)?

Avoimeksi releeksi (open relay) kutsutaan postipalvelimia, jotka välittävät sähköpostiviestejä, kuten spämmiä, oman organisaation ulkopuolelta toisiin oman organisaation ulkopuolisiin palvelimiin. Oikein konfiguroidusta postipalvelimesta voi lähettää postia vain oman organisaation sisältä.

Spämmerit käyttävät avoimia releitä spämmin alkuperän piilottamiseen ja tietoliikennekulujen siirtämiseen avoimen releen ylläpitäjälle: avointa relettä voi käyttää yhden spämmin kopioimiseen usealle vastaanottajalle.

Abuse.net:in avulla voi testata onko oma postikone avoin rele. Mahdollisimman kattavan releteston voi tehdä antamalla postipalvelimensa ORDB:n testattavaksi.

Spämmiä voi myös lähettää avointen välityspalvelimien (open proxy) kautta. Välityspalvelimen avulla voi ottaa TCP/IP-yhteyden SMTP-palvelimeen (joko avoimeen releeseen tai suoraan vastaanottajan postikoneeseen). SMTP-palvelin lisää Received-rivilla avoimen välityspalvelimen IP-osoitteen. Välityspalvelin välittää siis pelkästään TCP/IP-yhteyden, minkä vuoksi se ei lisää Received-riviä, joka sisältäisi spämmin lähettäjän IP-osoitteen - toisin kuin useimmat avoimet releet. Spämmerit käyttävät avoimia välityspalvelimia viestin alkuperän piilottamiseen.

Nykyään merkittävä osa roskapostista välitetään Windows-koneilta, joihin netissä leviävät haittaohjelmat ovat asentaneet spämmipalvelimen.

Avoimista releistä ja välityspalvelimista tulevaa spämmiä voi suodattaa automaattisesti (SpammiltaSuojautuminen).

Lisätietoja

- Helsingin yliopiston spämmintorjuntasivuilla kerrotaan lyhyesti avoimista releistä
- MAPS: How to secure your mail system against third-party relay
- RFC 2505: Anti-Spam Recommendations for SMTP MTAs

- Jouni Heikniemi: ISPien postipalveluiden ristiinkäyttö, kertoo mm. postiohjelmien konfiguroinnista ja avoimista releistä.
- SpamCop FAQ: Open Relay Servers
- Avoimista välityspalvelimista:
  - SpamCop FAQ: HTTP Proxies (Cisco and Squid)
  - SpamCop FAQ: Formmail
  - SpamCop FAQ: SOCKS Proxy Servers

Mitä ketjukirjeiden kanssa pitäisi tehdä?

Katso sivua KetjuKirjeet.

Miten voin estää sähköpostiosoitteeni joutumisen spämmerien listoille? Miten spämmerit keräävät sähköpostiosoitteita?

Jos käytät sähköpostiosoitettasi, niin se päätyy todennäköisesti ennen pitkää spämmilistoille. Osoitteen salassa pidosta ei pitkällä tähtäimellä ole käytännön hyötyä, koska osoite voi päästä julkisuuteen niin monia sellaisiakin reittejä, joihin osoitteen haltijalla ei ole mitään kontrollia. Osoitteen salaaminen tai sotkeminen häiritsee viestintää.

Vaikka välttäisitkin osoitteesi julkistamista esimerkiksi sotkemalla sähköpostiosoitteesi nyyssipostauksissa NOSPAM-lisäyksillä (mikä ei välttämättä ole hyvä ajatus), niin joku kaverisi lähettää sinulle kuitenkin sähköisen onnittelukortin käyttäen jotakin epämääräistä palvelua tai laittaa osoitteesi webbisivulleen, josta spämmerin osoitteidenkerääjä sen löytää. Jotkut Windows-ympäristössä leviävät haittaohjelmat kaivavat osoitteita ihmisten henkilökohtaisista sähköpostikirjoista, ilman että osoitetta itse olisi kertaakaan julkistanut.

Usein spämmiä lähetetään myös satunnaisesti luoduille tunnuksille. Varsinkin suositut ilmaissähköpostiosoitteiden tarjoajat ovat suotuisia kohteita tällaiselle toiminnalle, koska näissä tapauksissa satunnaisesti luotu tunnus on kohtuullisella todennäköisyydellä jonkun käytössä oleva toimiva osoite. Joskus näkee esimerkiksi spämmejä, jotka on lähetetty seuraavantyylisiin osoitteisiin: `aaaa@hotmail.com`, `aaab@hotmail.com`, `aaac@hotmail.com`, ...

Sähköpostiosoitteen leviämistä spämmi-CDeille voi yrittää hidastaa esimerkiksi välttämällä sähköpostiosoitteen antamista erilaisilla epämääräisille rekisteröitymislomakkeilla. Hyvä keino on perustaa tarkoitusta varten sähköpostitunnus käyttäen jotakin ilmaisista sähköpostipalveluntarjoajista, jotka tarjoavat muun muassa webbipohjaisia palveluja ja sähköpostin uudelleenohjauspalveluja, joissa ilmaisosoitteeseen lähetetty sähköposti lähetetään automaattisesti edelleen suoraan vakituiseen sähköpostilaatikkoosi. Myös nyyssipostauksissa NOSPAM-lisäyksiä parempi vaihtoehto voi olla väliaikaisten, mutta toimivien, sähköpostiosoitteiden tai -aliasten käyttäminen. Väliaikaisen osoitteen voi sitten hylätä siinä vaiheessa, kun spämmiä alkaa tulla liikaa.

Myös spämmistä valittaminen auttaa roskapostitulvan vähentämisessä. Euroopan unionissa spämmirekistereihin voi yrittää puuttua tietosuojavaltuutetun kautta, katso sivua SpammiinReagoiminen.

Sähköpostiosoitettaan kannattaa toki jaella harkiten, eikä sitä pidä antaa turhaan esimerkiksi erilaisiin webbilomakkeisiin. Muista kuitenkin, että sähköpostiosoite on olemassa yhteydenpitoa varten. Käytä oikeaa sähköpostiosoitettasi, kun siihen on aihetta.

Osoitteen jakamisesta ja sotkemisesta kerrotaan enemmän sivulla SpammiltaSuojautuminen.

Lisätietoja

- Spam Address FAQ -- How To Fight Back kertoo miten spämmerit keräävät sähköpostiosoitteita.
- Uri Raz: How do spammers harvest email addresses?

- Email Addressing FAQ neuvoo kuinka loppukäyttäjä voi helposti tehdä väliaikaisia sähköpostialiaksia.
- Oikeaoppinen osoitteen sotkeminen
- Mista spammerit keraavat osoitteet?
- The Spamhaus Project: Spam 'Remove' Lists

Joku on ilmoittanut osoitteeni useille spämmäyslistoille, mitä voin tehdä?

Katso keskustelusäikeitä Apua spämmit ja Luvaton rekisteröinti.

Spämmeri on väärentänyt osoitteemme ja postipalvelimemme ylikuormittuu, mitä voin tehdä?

Spämmien otsikkotiedoissa ja rungossa olevat osoitteet, sekä reverse-path-osoite, johon viestistä aiheutuvat virheilmoitukset lähetetään, ovat usein väärennettyjä. Spämmistä aiheutuvat valitukset ja virheilmoitukset päätyvät näihin väärennettyihin osoitteisiin. Nämä virheilmoitukset voivat johtaa postipalvelimen ylikuormittumiseen.

Lisätietoja

- SPAM-DoS-hyökkäys, CASEna Helsingin yliopisto 21-22.9. 2000
- Uutisryhmäsäie roskaposti
- Joel Yliluoma: Palvelimemme joutui spammerien uhriksi.

Mitä Internet-palveluntarjoan pitää tehdä verkossaan oleville spämmereille?

Dokumentissa PalveluntarjoajanVelvollisuudet annetaan yhteenveto siitä, mitä Internet-palveluntarjoajan pitää Internetin käytännesääntöjen mukaan tehdä, jos heidän asiakkaansa syyllistyy spämmäykseen.

SPEWS FAQ (oma suomennos):

> K23: Palveluntarjoajana, mikä on paras tapa pitää verkkomme poissa SPEWSin estolistoilta?
>
> V23: Se on varsin yksinkertaista, pysy erossa spämmereistä, spämmerien palveluntarjoajista ja spämmäysohjelmistojen myyjistä. Jos joku näistä ilmestyy verkkoosi, katkaise heidän yhteytensä heti ennen kuin valitusten määrä kasvaa. Etsi ja kopioi itsellesi parhaat käyttöehdot (AUP) ja valvo että niiden kirjainta noudatetaan. Ja kaikista ilmeisin tapa; seuraa ja reagoi abuse@-laatikkoosi tulevaa postia!

Mistä saan aiheesta lisää tietoa?

Muilla tämän sivuston sivuilla on lisää tietoa. Webissä on valtavasti tietoa spämmistä. Voit hakea haluamaasi tietoa suoraan Googlella. Googlen hakemistossa on oma osio spämmille. Suomenkielisessä Wikipediassa on myös runsaasti artikkeleita roskapostista.

[PDF, TXT]
http://kaip.iki.fi/spam/SvrVukk.html
Puolusta sähköisiä oikeuksiasi. Liity EFFIn jäseneksi.
Kai Puolamäki, Kai.Puolamaki@iki.fi