



BitoS initiativ mot oönskad e-post

Bakgrund

Få, om någon, användare vill ha oönskad, obeställd e-post, det som brukar kallas spam. Det ligger i BitoS uppdrag att marknadsföra innehålls- och tjänstebranschen på onlinemarknaden i Sverige. I detta uppdrag ligger bland annat att öka förtroendet för och stimulera användningen av såväl fasta som mobila tjänster hos slutanvändaren.

Otillbörlig e-post kan skickas i bulk, det vill säga till en stor mängd mottagare eller ett i taget. Ofta handlar det om meddelanden som skickas från en avsändare utanför Sverige och innehållet kan vara ett tips om en pornografisk webbplats eller tips om hur man mycket snabbt skall tjäna pengar utan någon kapital- eller arbetsinsats. Ibland är det annan typ av oönskad reklam som skickas på detta sätt.

Som användare vill man filtrera bort många av dessa meddelanden och helst vill man inte ha dem alls. Vissa meddelanden i meddelandefloden vill man dock läsa, då det kan handla om ett meddelande som man efter att ha läst det trots allt är intresserad av. Vidare är det svårt att via lagstiftning lösa problemet med otillbörlig e-post, då alla åtgärder för att begränsa e-post-användning dels riskerar hindra den långtgående yttrandefriheten på Internet, dels kan komma att införas före dess branschen funnit egna lösningar på de problem som kan finnas. Ytterligare en komplikation är att hård filtrering eller liknande åtgärder kan leda till att även önskad e-post försvinner. Framförallt biter nationell lagstiftningen dåligt på spammare ute i världen.

BitoS har mot bakgrund av det sagda tagit fram en Spam-hund. Spam-hunden är en lathund som den användare som vill undvika oönskad, obeställd e-post kan använda. Genom att använda Spam-hunden kan du alltså minska riskerna för att få otillbörlig e-post. Skicka gärna tips och kommenterar till info@bitos.org. Dokumentet kommer att uppdateras efter behov.

Så undviker du oönskad, obeställd e-post

1. Lämna inte ut din e-post-adress till okända aktörer på Internet. Aktörer är allt från privatpersoner till företag, myndigheter och organisationer. Om du ändå vill lämna ut din e-post-adress till aktörer som du inte känner till, undersök om du kan få reda på varför de vill ha din e-post-adress. Lämna inte ut din adress till kända aktörer heller utan att veta hur de ska använda din adress. Infoga som standard en passus om att du motsätter dig utskickade av UCE/UBE/spam (UCE = 'Unsolicited Commercial Email' och UBE = 'Unsolicited Bulk Email') till den adress de fått i de fall du väljer att lämna ut den. Och lämna aldrig ut någon annans epostadress heller (inte kollegans, inte kompisens, inte släktens). Inte ens - i synnerhet inte - om det gäller en tävling av något slag och det inte framgår hur din e-post-adress skall användas i framtiden.

2. I de fall du måste lämna ut en e-post-adress till en okänd aktör eller någon aktör som du inte riktigt vet kommer använda din e-post-adress på det sätt som du önskar - registrera en separat e-post-adress för detta ändamål. Det finns gratis e-post-konton som är lämpliga för detta ändamål på en mängd ställen på Internet.

3. Om du använder Hotmail kan du ställa in alternativet "block sender" om du får ett obeställt, oönskad e-post-meddelande. Då stoppas all e-post från den avsändaren i framtiden. Hotmail-konton drabbas dock generellt av väldigt mycket obeställd, oönskad e-post. Även Yahoo har spamskydd. Det kallas "spam guard" och fungerar automatiskt om du har konto hos Yahoo.

4. Om du debatterar i Usenet eller chattar på en webbplats eller på annat ställe - använd en särskild e-post-adress för detta ändamål. Ett alternativ som är något mer avancerat är att ändra adressen så att den inte är maskinellt läsbar, men som gör att meddebattörer lätt kan få din riktiga adress. Så här kan det se ut:

mikael@tabortdetharinklusivepunktenefter.pawlo.com

Ett mer internetvänligt sätt att förvanska adressen föreslogs ursprungligen av Claes Tullbrink och det är att avsluta med ".invalid", dvs *claes@tabortdettaochinvalid.hotmail.com.invalid*

5. Använd filter i e-post-programmet. Det går att filtrera på olika nivåer. Ett sätt är att ställa in att alla brev som inte innehåller din adress i TO:-adressfältet skall filtreras till en särskild mapp. Resten av breven kan hamna i en annan mapp vars innehåll kan raderas efter att du tittat att ingen intressant avsändare finns med bland breven. Risker

är dock att du missar massor av brev som du verkligen vill ha. Om möjligt, filtrera bort spam redan i servern. En funktion som heter 'reverse look-up' verifierar att avsändarservern är vad den utger sig för att vara. Annars släpps inte mailen igenom. På så sätt får också avsändaren ett meddelande om att adressen inte fungerar, vilket förhoppningsvis gör att du blir bortplockad från utskickslistan.

Några tips på resurser:

SpamAssassin: <http://www.spamassassin.org/>

SpamCop: <http://www.spamcop.net>

SpamSieve: <http://www.c-command.com/spamsieve/index.shtml>

6. Om någon upprepat skickar obeställd, oönskad e-post till dig kan du klaga hos den Internet-operatör utskicket kommer ifrån. För att ta reda på vilken operatör som administrerar ett visst IP-nummer kan Du gå in på www.ripe.net (för Europa, Mellanöstern och delar av Afrika), www.arin.net (för Amerika, Karibien och delar av Afrika) eller www.apnic.net (för Asien). Ett sådant klagomål skall ställas till ansvarig leverantör, inte till din egen leverantör. Det gör du enklast med ett brev till abuse@internetleverantörensnamn.se. Skicka med hela det/de brev, inklusive brevhuvud, som besvärat dig med din anmälan. Internetleverantören kan antingen hjälpa dig direkt eller säga till vilken annan internetleverantör du skall vända dig med din anmälan.

7. Om du gör en egen hemsida, publicera inte din e-post-adress på hemsidan. Använd istället en speciell e-post-adress för detta ändamål. Om du ändå vill publicera den - använd inte en klickbar länk till din e-post-adress. En elegant lösning är att enbart lägga ut den egna e-postadressen på sidan som en bild, vilket gör att e-postadressen inte blir maskinellt läsbar i koden för sidan. Den som besöker sidan i legitimt syfte ser däremot ingen skillnad, utan för ett mänskligt öga blir det fortfarande läsbart.

8. Svara aldrig på ett spam. Maila aldrig till en "remove"-adress. Vare sig "From" eller "To" eller "Reply-to" är att lita på... Genom att begära att ens e-post-adress ska tas bort från framtida utskickslistor bekräftar man att adressen existerar och blir läst. Den som får "remove"-önskemålet kan därför sälja din adress - till ett högre pris - som "verifierad" och resultatet av borttagsbegäran blir att du drabbas av mer spam än någonsin förr. Samma sak om du på annat sätt bekräftar att deras spam nått din e-adress, till exempel genom att klicka på länkar som finns med i meddelandet.

Här måste dock noteras att det idag tyvärr räcker med att öppna eller förhandsgranska ett modernt skräppostmeddelande för att din e-

postadress ska vara bekräftad. Modern skräppost bygger på html, och tillåter du att ditt e-postprogram laddar innehållet i brevet så är skadan skedd.

9. Handla aldrig av ett företag som marknadsför genom att spamma. Rösta inte på ett politiskt parti som spammar. Och tro inte på en Gud med anhängare som spammar. Gillar du inte sättet ett företag marknadsför sig på är det effektivaste sättet givetvis att tala om vad du tycker med hjälp av plånboken.

10. Spammotel är en tjänst för att registrera adresser som kan användas för prenumeration på mailinglistor och liknande. Börjar man få spam till en e-post-adress på Spammotel (<http://www.spammotel.com>), går det att spåra varifrån spammaren fått adressen och sedan avregistrera.

=====

Detta dokument får spridas, mångfaldigas och kopieras helt fritt förutsatt att detta sker i oförändrat skick och med angivande av versionsnummer och källa. Spridning i ändrat utförande är också tillåten. För det fall det handlar om användning i ändrat utförande måste dock alla ändringar tydligt markeras genom en inledande förklaring eller genom hyperlänk till originaldokumentet i det nya dokument.