

---

## Geef spam geen kans

---

Wat voor antispamsoftware heeft u nodig?

Dit white paper is een gids voor antispamsoftware en laat u zien welke antispamsoftware de beste voor u is en waarom.

---

## Inleiding

In dit white paper kunt u lezen wat u nodig heeft om spam op een effectieve manier te kunnen bestrijden.

Inleiding .....	2
De toename en de kosten van spam.....	2
Hoe kiest u de juiste antispamsoftware?.....	2
Hoe GFI MailEssentials spam bestrijdt .....	6
Over GFI.....	8

---

## De toename en de kosten van spam

Het Amerikaanse onderzoeksbureau The Radicati Group schat dat 52 procent van het huidige mondiale e-mailverkeer uit spam bestaat en voorspelt dat dit in 2007 gestegen zal zijn naar 70 procent. Volgens schattingen van de Europese Unie bestaat 50 procent van het e-mailverkeer uit spam.

Dit betekent dat werknemers een deel van hun werktijd moeten besteden aan spam. Dit leidt tot een afname van productiviteit (en een toename van frustratie!). De belangrijkste kostenpost van spam is productiviteitsverlies, vooral door het grote aantal spamberichten dat elke dag binnenkomt. Daarnaast wordt door spam uw bandbreedte verspild en heeft u andere opslag-, netwerk en infrastructuurkosten. Bovendien bestaat bij gehaaste pogingen om uw mailbox op te ruimen het gevaar dat een belangrijk bericht per ongeluk samen met de ongevraagde mailtjes in de virtuele prullenbak belandt.

Ferris Research heeft berekend dat als een werknemer 5 spamberichten per dag ontvangt en aan elk bericht 30 seconden besteedt, hij per jaar 15 uur aan spam verspilt. Vermenigvuldigd met het uurloon van iedere werknemer in uw bedrijf en dan heeft u een zeer conservatieve schatting van hoeveel spam uw bedrijf kost. Volgens The Radicati Group kostte spam IT-afdelingen ongeveer \$49 per mailbox in 2003. De verwachting is dat dit zal stijgen naar \$257 per mailbox in 2007.

Het is van het grootste belang een halt toe te roepen aan spam zodat u tijd, geld en bandbreedte kunt besparen. Allereerst moet u uw netwerkgebruikers duidelijk maken dat ze hun e-mailadres privé moeten houden (en dus geen berichten op message boards mogen plaatsen). Naast uw gezond verstand moet u echter ook antispamsoftware gebruiken.

---

## Hoe kiest u de juiste antispamsoftware?

Er zijn vele softwarepakketten op de markt die u kunnen helpen bij het bestrijden van spam. Niet al deze pakketten zijn echter voldoende effectief. Hieronder vindt u enkele aspecten die

belangrijk zijn bij het kiezen van antispamsoftware.

### **Via de server of niet?**

Het bestrijden van spam op cliëntniveau is veel tijdrovender dan op serverniveau. Als u kiest voor spambestrijding op cliëntniveau moet u op elk werkstation apart antispamsoftware installeren en bovendien regelmatig de antispamregels op ieder werkstation updaten. Bovendien is spam een belasting voor uw e-mailinfrastructuur doordat uw server volzit met nutteloze mailtjes die nog weggegooid moeten worden. Ook kost het uw gebruikers tijd, want zij moeten spam identificeren of hun regelsets updaten. En dat terwijl u juist tijd wilt besparen!

Bovendien beschikt cliëntgebaseerde antispamsoftware niet over de informatie en de middelen van servergebaseerde antispamsoftware – u kunt er bijvoorbeeld niet de verzendende server mee controleren. Om spam effectief te kunnen bestrijden hebt u een servergebaseerd antispamproduct nodig. Dit biedt u de volgende voordelen:

1. Het product wordt geïnstalleerd aan de gateway. Hierdoor hoeft u het niet op iedere computer apart te installeren.
2. Lagere licentiekosten.
3. Spam kan uw e-mailinfrastructuur niet eens binnenkomen. De opslagruimte komt dus niet vol spam te zitten.
4. Servergebaseerde antispamsoftware bevat meer informatie en kan meer doen om spam te detecteren.

### **Bayesiaanse filtertechniek**

Een paar jaar geleden gebruikten de meeste antispamproducten slechts een trefwoordenlijst om spam te identificeren. Een goede trefwoordenlijst kon de meeste spam wel opsporen. Tegenwoordig leidt een dergelijke methode echter tot te veel valse meldingen en moet er te veel handmatig geüpdated worden.

De experts zijn het er nu over eens dat het gebruik van een Bayesiaanse filter de beste manier is om spam te bestrijden. Een Bayesiaanse filter gebruikt een wiskundige benadering die is gebaseerd op bekende spam en ham (legitieme e-mail). Dit betekent een geweldig voordeel ten opzichte van ouderwetse antispamtechnologie die alleen naar trefwoorden zoekt of handtekeningen van bekende spam downloadt. U kunt meer lezen over Bayesiaans filteren in het white paper 'Waarom Bayesiaans filteren de meest effectieve antispamtechniek is' op <http://www.gfi.nl/whitepapers/why-bayesian-filtering.pdf>.

Kort gezegd heeft Bayesiaans filteren de volgende voordelen:

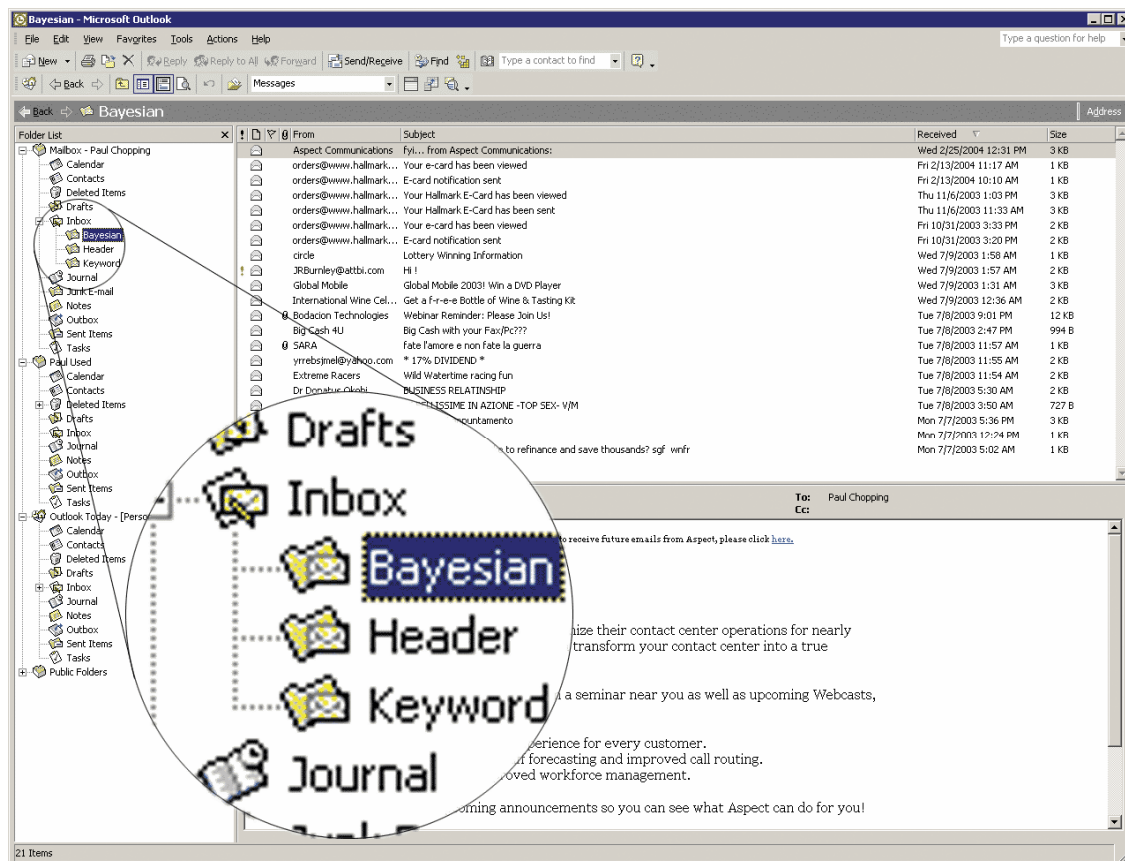
1. Kijkt naar het gehele spambericht en dus niet alleen naar trefwoorden of bekende spamhandtekeningen
2. Leert van uw verzonden mail (ham) en verkleint daardoor het aantal valse meldingen

3. Past zich aan door te leren over nieuwe spam en nieuwe legitieme mail
4. De dataset is uniek en daardoor onmogelijk te passeren.
5. Meertalig en internationaal.

### **Een aangepast hamdatabestand voor de Bayesiaanse filter**

Het is uiterst belangrijk dat de Bayesiaanse filter een dataset gebruikt die speciaal voor uw bedrijf is gemaakt: de hamdata MOETEN uit uw verzonden mail komen (op deze manier past de Bayesiaanse filter zich aan aan uw bedrijf). Sommige antispamsoftware maakt gebruik van een algemeen hamdatabestand dat bij het product wordt geleverd. Een voorbeeld hiervan is de Outlook spamfilter of de Exchange Server Internet Message filter. Hoewel een dergelijke filter meteen vanaf het begin werkt zijn er twee belangrijke nadelen:

1. Het hamdatabestand is openbaar en kan dus worden gekraakt door professionele spammers en zo worden omzeild. Als uw databestand uniek is, heeft het geen zin om het te kraken. Er zijn bijvoorbeeld hacks beschikbaar waarmee de Microsoft Outlook 2003 spamfilter gepasseerd kan worden.
2. Ten tweede is het hamdatabestand een algemeen bestand. Omdat het niet is toegespitst op uw bedrijf kan het nooit even effectief zijn als een aangepast bestand. U zult een merkbaar hoger aantal valse meldingen krijgen. Een bank gebruikt bijvoorbeeld vaak het woord "hypotheek" en zou dus een groot aantal valse meldingen krijgen als er een algemeen hamdatabestand gebruikt zou worden.



Het beoordelen van spam is heel eenvoudig dankzij een subfolder in de mailbox van de gebruiker

### Automatisch bijgewerkt spamdatafile voor de Bayesiaanse filter

Het spamdatafile van de Bayesiaanse filter moet steeds door de antispamsoftware worden bijgewerkt met de nieuwste spam. Hierdoor bent u ervan verzekerd dat de Bayesiaanse filter op de hoogte is van de nieuwste trucs en dus een hoge detectiegraad bereikt (let op: het bijwerken vindt plaats na afloop van de leerperiode van twee weken). Kies een antispamproduct dat deze data voor u verzamelt en u deze updates automatisch laat downloaden!

### Een efficiënte methode voor het beoordelen van spam

Het is onvermijdelijk dat u valse meldingen zult krijgen: e-mails die ten onrechte als spam worden aangemerkt. Met goede antispamsoftware kunnen gebruikers gemakkelijk en snel mail beoordelen die als spam is aangemerkt.

Het is het beste als antispamsoftware over een optie beschikt waarmee als spam aangemerkte mail naar de junkmailfolders van de individuele gebruikers wordt gestuurd. Dit bespaart de netwerkbeheerder veel gedoe en tijd. Bovendien moet de software de spam sorteren in verschillende mappen afhankelijk van waardoor het als spam is aangemerkt. Zo kunnen

gebruikers hun spam gemakkelijk beoordelen. Met sommige antispamproducten moeten gebruikers op een webgebaseerd systeem inloggen en ieder mailtje afzonderlijk bekijken – in de praktijk is dit hinderlijk voor de gebruiker en wordt deze optie dus nauwelijks gebruikt.

### **Flexibele whitelists kunnen het aantal valse meldingen verkleinen**

Antispamsoftware moet over een efficiënte manier beschikken om automatisch uitgebreide whitelists op te stellen. Alle legitieme zakenpartners moeten op een whitelist komen te staan zodat hun mail nooit als spam kan worden aangemerkt. Goede antispamsoftware moet de mogelijkheid bieden dergelijke whitelists automatisch te creëren en bij te werken.

---

## **Hoe GFI MailEssentials spam bestrijdt**

GFI MailEssentials bestrijdt spam op de volgende manieren:

1. Spam wordt aangepakt op serverniveau – GFI MailEssentials wordt geïnstalleerd op uw Exchange 2000/2003-server of voor uw mailserver (als u Exchange 5.5 of een andere mailserver gebruikt). Spam wordt gedetecteerd VOORDAT het uw mailserver bereikt. Op deze manier wordt uw e-mailinfrastructuur niet door spam belast en hoeft u de detectieregels alleen op de GFI MailEssentials-machine bij te te werken. Whitelists (domeinen en e-mailadressen waarvan u altijd mail wilt ontvangen) en blacklists (domeinen en e-mailadressen waarvan u geen mail wilt ontvangen) kunnen op serverniveau worden gebruikt.
2. De inhoud van uw mail wordt geanalyseerd door middel van een Bayesiaanse filter. Hierbij worden hamdata gebruikt die specifiek zijn voor uw bedrijf. De spamdata worden automatisch bijgewerkt door middel van downloads van de GFI website. Kijk voor meer informatie over de Bayesiaanse filtertechniek op <http://www.gfi.nl/nl/whitepapers/why-bayesian-filtering.pdf>.
3. Een kleiner aantal valse meldingen dankzij een automatische whitelist – GFI MailEssentials bevat een automatische tool voor whitelistbeheer waarvoor patent is aangevraagd. Dankzij deze unieke techniek worden al uw zakenpartners automatisch aan uw whitelist toegevoegd, zonder dat u daarvoor iets hoeft te doen. Hun mail gaat niet door de spamfilter en het aantal valse meldingen wordt zo beduidend kleiner.
4. Flexibele behandeling van spam – Als een spambericht wordt aangetroffen kan het worden doorgestuurd naar een subfolder in de mailbox van de gebruiker. Als gebruikers in deze folder een legitiem bericht vinden (bijvoorbeeld een nieuwsbrief die ze willen ontvangen) dan kunnen ze de afzender toevoegen aan de whitelist.
5. GFI MailEssentials biedt de mogelijkheid om op trefwoord te controleren zodat netwerkbeheerders hun antispamfilters verder kunnen optimaliseren.

6. Voor een nog betere bescherming beschikt GFI MailEssentials niet alleen over de Bayesiaanse filtertechniek maar ook over verscheidene **andere spamdetectietechnieken**, zoals intelligente mailheaderanalyse en het gebruik van zowel unieke als openbare blacklists (zoals ORDB en SpamHaus).

---

## Over GFI

GFI is een toonaangevende ontwikkelaar van software voor netwerkbeveiliging, inhoudsbeveiliging en messaging. Dankzij bekroonde technologie, een agressieve prijsstrategie en een sterke focus op MKB-bedrijven helpt GFI bedrijven over de hele wereld om maximale continuïteit en productiviteit te bewerkstelligen. GFI is opgericht in 1992 en heeft kantoren in Malta, Londen, Raleigh, Hong Kong, Adelaide en Hamburg die wereldwijd meer dan 200.000 installaties ondersteunen. GFI is een kanaalgericht bedrijf met meer dan 10.000 partners over de hele wereld. GFI is ook een Microsoft Gold Certified Partner. Meer informatie over GFI is te vinden op <http://www.gfi.nl>.

© 2007 GFI Software Ltd. Alle rechten voorbehouden. De informatie in dit document geeft het standpunt van GFI weer betreffende de besproken onderwerpen op de datum van publicatie. Aangezien GFI moet reageren op veranderende marktomstandigheden, moet dit document niet als een toezegging van GFI worden geïnterpreteerd. Na de publicatiedatum kan de correctheid van de informatie niet worden gegarandeerd. Dit white paper dient puur ter informatie. GFI GEEFT IN DIT DOCUMENT GEEN ENKELE GARANTIE, EXPLICIET NOCH IMPLICIET. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor en de bijbehorende logo's zijn ofwel geregistreerde handelsmerken of handelsmerken van GFI Software Ltd. in de Verenigde Staten en/of andere landen. Alle product- en bedrijfsnamen in dit persbericht zijn mogelijk handelsmerken van hun respectievelijke eigenaren.

