

Hoe je ervoor zorgt dat meer e-mails aankomen

GraphicMail White Paper 2011

GRAPHIC MAIL 
e-mail en sms marketing software

Inhoud

1. De uitdaging van het afleveren van e-mails	2
2. Afleveren of afleverbaarheid?	3
3. E-mails afgeleverd krijgen	3
4. Hoe komt mijn e-mail in de inbox	5
5. Filteren op basis van content	6
6. Filteren op basis van reputatie	7
7. Authenticiteit en domeingebaseerde reputatie	9
8. Hoe wordt zenderreputatie gedefinieerd?	10
9. Klachten spam metingen	11
10. Voorkom spamklachten	11
11. Hoe een ESP u kan helpen met het succesvol afleveren van meer e-mails	16

1. De uitdaging van het afleveren van e-mails

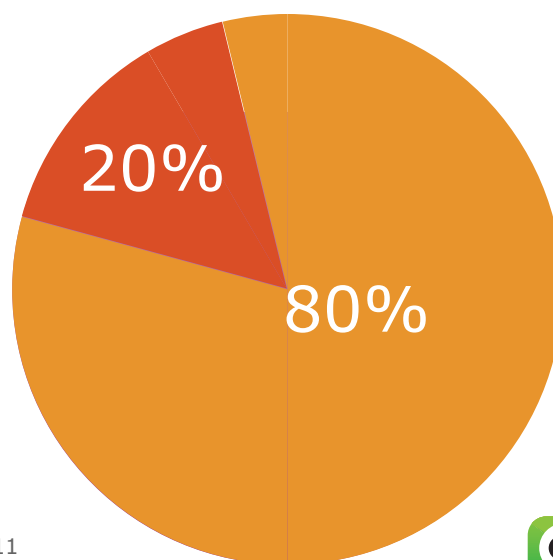
E-mail werkt eenvoudig. Zodra u op de button 'verzenden' hebt geklikt, vindt er een aardig staaltje technische magie plaats en wordt uw bericht succesvol afgeleverd in de inbox van de ontvanger.

Tenminste, dit is het idee dat wij van e-mail hebben. Jammer genoeg moet iedere e-mail behoorlijk wat obstakels overwinnen voordat het zijn uiteindelijke bestemming bereikt. Dat betekent ook dat niet alle e-mails hun eindbestemming halen. Zie het als goed nieuws, als u bedenkt dat 80% van alle verzonden e-mail spam betreft¹.

Het slechte nieuws eraan is dat het niet alleen spam betreft dat wordt tegengehouden door de obstakels. Ook opt-in e-mails (e-mails waar mensen om hebben gevraagd) sneuvelen af en toe.

Het meest recente rapport hierover, uitgevoerd door Return Path, toont aan dat 17.8% van alle legitieme e-mails die worden verzonden in Europa² hun eindbestemming (de inbox) niet bereikt, en dat geldt voor 19.9% in de Verenigde Staten en Canada³.

In dit white paper behandelen we de terminologie, technieken en tactieken die u nodig heeft om er zo zeker mogelijk van te zijn dat legitieme mailings aankomen.



1 Symantec (2011) State of Spam & Phishing: February 2011

2 Return Path (2010) European Email Deliverability Benchmark Report

3 Return Path (2010) Email Deliverability Benchmark Report

2. Afleveren of afleverbaarheid?

Er vinden een hoop (technische) controles plaats tijdens de reis die een e-mail aflegt van zender naar ontvanger, daarom kan het helpen uit te gaan van twee uitgangspunten.

1. Het afleveren van de e-mail: het proces waarbij de e-mail zich 'verplaatst' van de ene naar de andere organisatie. Er wordt gesproken van een succesvolle aflevering wanneer de e-mail niet wordt tegengehouden door de laatst genoemde.
2. De afleverbaarheid van de e-mail: dit verwijst naar de mogelijkheid de e-mail daadwerkelijk in de inbox van de ontvanger af te leveren.

Het is belangrijk om te realiseren dat wanneer uw e-mail een "go" heeft om afgeleverd te worden, de e-mail nog steeds kan worden geblokkeerd en zijn eindbestemming (de inbox van de ontvanger) niet zal bereiken. De e-mail kan op voorhand worden verwijderd, of - al is hij afgeleverd aan het account - uit de inbox worden geweerd en direct in de spam, junk of een andere map worden geplaatst.

3. E-mails afgeleverd krijgen

Wanneer een e-mail niet geaccepteerd wordt door de ontvangende organisatie, is dat over het algemeen te wijten aan een technisch probleem. Bij dit type afgekeurde e-mails is het normaal een automatisch bericht te ontvangen - een bounce bericht - en bij de inhoud van zo'n bericht kunt u het best denken aan een equivalent bericht als 'return to sender'. Een bounce bericht vertelt de zender dat het verzendsysteem de e-mail niet kon afleveren en waarom dat is mislukt.

Waarom bounces belangrijk zijn

E-mailadressen met een permanent afleverprobleem moeten van een maillijst worden gehaald. Anders blijft u gebruik maken van bronnen om een e-mail te verzenden die toch niet kan worden afgeleverd.

Het verzenden van e-mail naar zogenoemde 'dode' adressen wordt door sommige systemen ook gebruikt om de verzender te identificeren als een 'slechte' verzender, maar daarover later meer.

Speciale gevallen: 'Blocked', bounces en 'beperking'

Sommige systemen zenden een bounce bericht wanneer de e-mail wordt aangemerkt als spam. De meeste bedrijven doen dit niet uit angst dat het de spammer te veel informatie geeft. De meeste spam wordt daarom eenvoudig verwijderd of geplaatst in de 'junk' map.

De term 'beperking' kunt u ook tegenkomen. Dit gebeurt wanneer een ontvangende organisatie het aantal e-mails dat binnenkomt wil beperken tot een bepaald aantal (over een periode of van een specifieke ontvanger). Deze term wordt ook gebruikt wanneer de organisatie die verzendt een limiet heeft opgesteld m.b.t. het maximaal aantal te verzenden e-mails. Over het algemeen heeft dit beleid alleen impact op hen die grote aantallen e-mails verzenden.

Overzicht actiepunten (om e-mail afgeleverd te krijgen)

- Bekijk alle bounce berichten om meer informatie in te winnen waarom een e-mail niet wordt afgeleverd.
- Houd het aantal bounce berichten laag door een ESP of software functionaliteit te gebruiken die bounce berichten nauwkeurig beoordeelt.
- Zorg ervoor dat e-mailadressen met een permanent afleverprobleem van de maillijst worden verwijderd.

4. Hoe komt mijn e-mail in de inbox

Ontvangende systemen zoals Internet Service Providers (grote webmail organisaties of breedband bedrijven) en zakelijke IT afdelingen willen niet alle e-mail naar de inbox toestaan, omdat de meeste e-mail spam lijkt te zijn. Daarom hebben deze bedrijven checkmomenten ingebouwd.

Dit wordt ook wel spam filtering genoemd, zodat deze bedrijven op grote schaal in staat zijn binnenkomende e-mails snel te categoriseren: houd tegen als spam, verwijder als spam, verzend naar inbox of plaats in andere map. Zelfs als uw e-mail met een positieve beoordeling is toegelaten door deze filter, kan het zijn dat de software die wordt gebruikt door de potentiële ontvanger van de e-mail de mail ook nog een keer beoordeelt voordat het bericht in de inbox wordt geplaatst.

Hoe kom ik erachter dat er een probleem is m.b.t. het afleveren van mijn e-mails?

Ontvangende organisaties geven over het algemeen geen informatie hoe zij binnenkomende e-mail categoriseren. De meeste marketeers baseren zich op andere bronnen die hen helpen met het identificeren van afleverproblemen.

Bijvoorbeeld:

1. Observeer of er ongebruikelijke dips in het aantal reacties voorkomen.
2. Observeer of er ongebruikelijke pieken voorkomen in het aantal spam block berichten.
3. Check het aantal reacties bij het domeinadres. Als niemand met een yahoo.com e-mail adres de e-mails opent of links in de e-mail aanklinkt, dan is de kans groot dat u een afleverprobleem hebt bij Yahoo! Mail.
4. Maak gebruik van een dienst die 'seed listing' aanbiedt. Een seed list is een lijst met e-mail adressen die kunnen worden opgenomen in de maillijst zodat iedere verzonden e-mail bekeken wordt bij een belangrijke ISP's en daadwerkelijk gecheckt kan worden of de ISP de e-mail aflevert in de inbox, in de junk map of dat de e-mail überhaupt niet aankomt. De ESP die u gebruikt kan deze service aanbieden, maar er zijn ook bedrijven die er volledig op zijn toegespitst zoals Email Reach, Delivery Watch en Return Path.

ISP's en e-mailsoftware gebruiken verschillende combinaties van publieke en interne filtertechnieken en producten voor de verwerking van e-mails, maar de twee dominante vormen van spam filtering zijn gebaseerd op content en reputatie.

5. Filteren op basis van content

Zoals de naam al suggereert, contentfilters beoordelen de content van een e-mail: code en structuur van de e-mail om te beoordelen of deze karakteristieken bevatten die wijzen op spam.

Een populaire spamfilter is Spam Assassin⁴. Dit programma test iedere binnenkomende e-mail op honderd verschillende unieke manieren waarvan velen zijn gericht op de content van de e-mail. Na iedere check wordt een aantal punten toegekend en het totaal aantal punten bepaalt de spam score. Als uit de score blijkt dat een e-mail een bepaalde hoeveelheid 'vervuiling' bevat wordt deze als spam aangemerkt met alle gevolgen van dien.

De testen die worden uitgevoerd door Spam Assassin zijn goed gedocumenteerd, hieronder een aantal voorbeelden van op content gebaseerde testen:

- E-mail bericht over een replica horloge
- Het onderwerp is in kapitalen
- Van: domein bevat een serie bestaande letters uit alleen medeklinkers
- HTML kleur van het lettertype is gelijk aan de achtergrond

Veel ISP's en anti-spam technologieën hebben hun aandacht op content filtering gereduceerd en besteden meer aandacht aan reputatie checks. Een van de belangrijke redenen hiervoor is dat spam testen vals positief waren, waarbij e-mails met een opt-in toch werden beoordeeld als spam omdat de content overeen kwam met de testpunten van de content check.

⁴ See <http://spamassassin.apache.org/tests.html>

Een aantal jaar geleden vermeden marketeers het woord 'gratis' in onderwerpregels te gebruiken, uit angst voor het stempel "spam" door contentfilters. Hoe dan ook, het risico ligt tegenwoordig veel lager: content die slechts op een aantal vlakken gelijkenissen toont met testpunten van een content check wordt niet meer beoordeeld als spam.

Overzicht actiepunten (contentfilters)

- Maak gebruik van een tool die test hoe de structuur en content door spamfilters wordt beoordeeld en onderneem actie op basis van feedback. ESP's zoals GraphicMail hebben dit type functionaliteiten in hun software ingebouwd. Standalones zijn ook verkrijgbaar via gespecialiseerde diensten zoals eerder genoemd.

6. Filteren op basis van reputatie

Een reputatiefilter kijkt niet zo zeer naar de inhoud van een e-mail, maar naar de herkomst van de e-mail. De belangrijkheid hiervan is snel gegroeid en de reputatie van de zender is voor webmail diensten als Hotmail, Gmail en Yahoo en andere ISP's op dit moment de meest belangrijke factor op basis waarvan een e-mail wordt beoordeeld.

Hoe wordt een zender geïdentificeerd?

De reputatie van de zender wordt geassocieerd met het netwerk connectiepunt van de e-mailbron: het zogenoemde IP adres waar vandaan de e-mail is verzonden. ESP's beheren bijvoorbeeld altijd een fors aantal IP adressen die zij gebruiken voor de verzendingen van hun klanten.

Gedeeld/uniek IP adres

Een uniek IP adres is er een die exclusief wordt gebruikt door een enkele verzender. De reputatie is volledig gebaseerd op uw eigen e-mail en verzendpraktijken. Een gedeeld IP adres wordt ook door andere verzenders gebruikt. Uw reputatie wordt beïnvloedt door uw eigen verzendingen, maar ook door die van andere verzenders. Het lijkt op basis van deze informatie logisch dan altijd te kiezen voor het gebruik van een uniek IP adres (of dit bij uw ESP aan te vragen), maar dat zorgt ook voor problemen:

1. Het is verplicht een significant aantal e-mails te verzenden om een reputatie op te kunnen bouwen. IP adressen die maar weinig verzendingen verrichten, worden door ISP's over het algemeen als negatief beoordeeld.
2. Nieuwe IP adressen moeten met zorg worden behandeld waarbij de volumes die worden verzonden, geleidelijk worden opgebouwd. Dit zogenoemde 'warming up' proces vraagt om professionele begeleiding.

Daarom zijn kleinere zenders van e-mails vaak beter af als zij verzenden via een gedeeld IP adres via een ESP. Zij zijn experts in het managen van deze adressen om ervoor te zorgen dat het IP adres zijn goede reputatie behoudt. De betere ESP's erkennen goede verzenders door hen allen via hetzelfde 'high reputation' IP adres te laten verzenden. Zo wordt het risico voorkomen dat goede verzenders per ongeluk worden geassocieerd met een 'rotte appel' die voor reputatieschade kan zorgen.

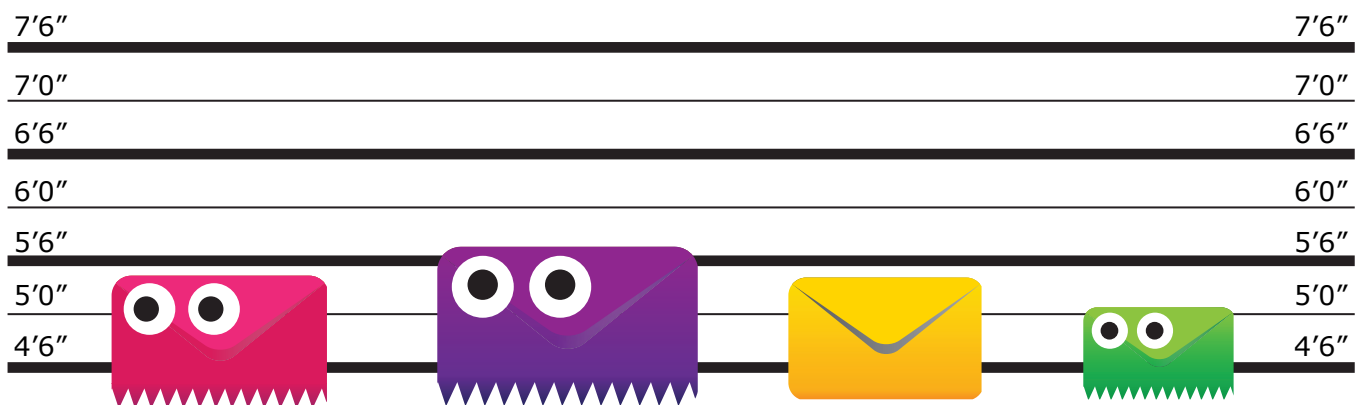
7. Authenticiteit en domeingebaseerde reputatie

Eigenlijk zou het beter zijn als ISP's e-mails filteren op basis van de 'echte' zender, zoals de domeinnaam die bij de e-mail hoort i.p.v. het IP adres te checken dat wordt gebruikt. Het geeft legitieme zenders de kans hun eigen reputatie op te bouwen en met deze certificatie gebruik te maken van verschillende verzendsystemen.

Als onderdeel van een bredere beweging voor meer accountability in het e-mail ecosysteem willen ISP's en andere aanbieders e-mail authenticiteit implementeren: op basis van een aantal normen bevestigen ontvangers van e-mail de ware identiteit van de verzender. De rol van authenticiteit en op domeingebaseerde reputatie groeit, dus het is een aanrader ervoor te zorgen dat uw verzonden e-mails het authenticiteit proces ondersteunen. Dit proces kijkt naar de domeinnaam en de informatie die gepaard gaat met de verzonden e-mail.

Overzicht actiepunten (e-mail authenticiteit)

- Overleg met uw technische medewerkers dat u de twee belangrijkste normen van authenticiteit ondersteunt: SPF/Sender ID en Domeinsleutels/DKIM.
- Als u gebruikt maakt van een ESP, is het de bedoeling dat zij uitgaande e-mails voor u checken op authenticiteit en u helpen bij het doorvoeren van aanpassingen in uw domeinarchief als dat nodig is.



Identificeer de echte spam?

8. Hoe wordt zender-reputatie gedefinieerd?

Zoals u waarschijnlijk al verwacht: organisaties markeren, wegen en selecteren verzendingen op verschillende manieren, maar over het algemeen trekken zij allemaal een conclusie op basis van de volgende uitgangspunten:

- Gebruikersinteractie met uw berichten
- Schone lijst (bounce management en spam traps)
- Blacklisting
- Infrastructuur en patronen verzendingen

Reputatiefactor: gebruikersinteractie n.a.v. uw e-mail

ISP's en andere aanbieders bekijken hoe gebruikers reageren op e-mails die eerder zijn afgeleverd van dezelfde zender. Positieve interactie draagt bij aan een 'goede' zenderreputatie voor toekomstige e-mails van die zender en negatieve interactie geeft het tegenovergestelde effect. De meest belangrijke interactie is of ontvangers e-mails markeren als spam door dit (over het algemeen) aan te geven via de spam button in het e-mail programma dat zij gebruiken. Wanneer het aantal e-mails dat als spam is gemarkeerd een maximum overschrijdt, zullen ISP's het aantal toekomstige e-mails van deze verzender in de toekomst beperkt toelaten of de aflevering ervan volledig blokkeren. Deze blokkades kunnen tijdelijk zijn, het kan ook zijn dat ISP's de verzender verzoeken herstelmaatregelen door te voeren voordat hun e-mailverkeer permanent wordt geblokkeerd.



9. Klachten spam metingen

De belangrijkste ISP's bieden een feedback loop (FBL) aan. Een FBL is een bericht aangeleverd door ISP's aan de verzender waarin wordt aangegeven welke e-mail-adressen op de maillijst de ontvangen e-mail als spam hebben gemarkeerd. Het is in het belang van de verzender dat hij voorkomt dat deze e-mailadressen in de toekomst nog e-mails ontvangen en daarnaast direct aanpassingen doorvoeren om te voorkomen dat hun e-mail in het vervolg ook door anderen als spam wordt gemarkeerd.

Overzicht actiepunten (klachten spam metingen)

- Schrijft u zich in bij alle FBL's van belangrijke ISP's⁵ en vergelijk klachten met verschillende verzonden campagnes om problemen goed te kunnen identificeren.
- Veel ESP's zijn al aangesloten bij de relevante FBL's en monitoren en verwerken klachten automatisch namens u.

10. Voorkom spamklachten

Het is belangrijk inzichtelijk te krijgen waarom mensen legitieme e-mails als spam markeren. Op basis van onderstaande informatie kunt u het aantal spam markeringen zo laag mogelijk houden:

1. Toestemming

De klassieke definitie van spam is ongevraagde bulk e-mail: e-mail waar de ontvanger nooit om heeft gevraagd. Hoe dan ook, zelfs wanneer mensen zich hebben ingeschreven voor een e-mail, kunnen zij de e-mail als spam markeren als:

- de inhoud van de e-mail niet aan hun verwachtingen voldoet. Voorbeeld: als u uw inschrijvers een nieuwsbrief zendt van een zusterorganisatie.
- de ontvanger is vergeten dat hij zich had ingeschreven voor het ontvangen van uw e-mail.

⁵ See http://wiki.wordtothewise.com/ISP_Summary_Information for a list

Overzicht actiepunten (voorkom problemen m.b.t. toestemming)

- Verzend alleen e-mail aan mensen die er expliciet om hebben gevraagd.
- Koop geen e-mailadressen, omdat deze mensen geen e-mail van u verwachten.
- Wacht niet te lang met het verzenden van de eerste e-mail na inschrijving (2-4 weken) en zorg ervoor dat nieuwe inschrijvers altijd een welkomst e-mail ontvangen.
- Zorg voor heldere en duidelijke inschrijfformulieren en leg in de welkomst e-mail uit wat voor e-mails de inschrijver kan verwachten.
- Denk erover na om in de e-mail footer aan te geven wanneer ontvangers zich voor uw nieuwsbrief hebben ingeschreven.
- Een gezonde periode tussen iedere verzending is 3 a 4 weken.
- Zorg ervoor dat de e-mail (ook de 'Van'- en onderwerpregel) op een heldere en duidelijke manier de identiteit van de e-mail en de verzender communiceren.

2. Irritaties

Mensen kunnen e-mails ook als spam markeren als zij niet meer geïnteresseerd zijn in de inhoud van de e-mail of omdat ze vinden dat ze van deze zender te vaak e-mail ontvangen.

Overzicht actiepunten (voorkom irritaties)

- Monitor spamklachten en het response als u ervoor kiest het aantal verzendingen te verhogen.
- Blijf continue werken aan de relevantie en waarde van uw e-mails op pijl te houden en/of te verbeteren.
- Identificeer inschrijvers die (langere tijd) geen response hebben gegeven en overweeg een campagne die speciaal is gericht aan deze doelgroep om hun interesse terug te winnen.

3. Luie uitschrijvers

Sommige mensen die webmail gebruiken, klikken liever op de button 'spam' dan dat ze de moeite nemen zich uit te schrijven. Beide acties hebben hetzelfde gevolg: geen e-mails meer van deze zender in de inbox.

Overzicht actiepunten (voorkom luie uitschrijvers)

- Zorg voor een duidelijke uitschrijflink in de footer van uw e-mail en zorg ervoor dat het uitschrijfproces helder en efficiënt is. Monitor reacties op uw e-mail of er uitschrijfverzoeken bij zitten.
- Als u zich bij voorbaat zorgen maakt over eventuele klachten m.b.t. spam, overweeg dan de uitschrijflink op een nog prominentere plek te plaatsen, bijvoorbeeld in de header van uw e-mail.

Reputatiefactor: 'schone' maillijst

ISP's en andere aanbieders verwachten van hun verzenders dat zij hun maillijsten 'schoon' houden: vrij van niet-bestaande of niet functionerende e-mailadressen. Ook op basis hiervan worden 'goede' en 'slechte' zenders bepaald of zelfs benoemd tot 'spammers', waarbij de laatste groep over het algemeen geen enkele moeite doet hun maillijst 'schoon' te houden. Hoe hoger het aantal e-mails dat wordt verzonden aan 'dode' e-mailadressen, hoe slechter dat is voor de reputatie van de verzender.

Sommige ISP's houden e-mailadressen die niet meer werken (bijvoorbeeld van een gesloten account) bij en na een tijdje wordt dit e-mailadres vervangen voor een spam trap. Een spam trap is een e-mailadres waarbij alle e-mails die aan dit adres worden verzonden, direct wordt gemarkeerd als spam. Een 'goede' verzender heeft 'dode' e-mailadressen allang van zijn maillijst verwijderd voordat een ISP er een spam trap van maakt.

Overzicht actiepunten ('schone' maillijst)

- Opnieuw, zend alleen e-mails naar mensen die er specifiek om hebben gevraagd.
- Opnieuw, koop geen e-mailadressen: het betreft vaak 'dode' adressen en/of spam traps.
- Verwijder altijd adressen die niet langer e-mails van u accepteren, of maak gebruik van een ESP die dit automatisch voor u doorvoert.

Reputatiefactor: Blacklisting

Een blacklist is een lijst met 'slechte' zenders van wie e-mails automatisch geblokkeerd kunnen worden. Een blacklist kan ook domeinnamen bevatten die vaak worden gebruikt in spam, hierdoor is het mogelijk ook een bericht dat een domein bevat die op de blacklist staat vermeldt, automatisch te blokkeren. ISP's beheren hun eigen interne blacklists en/of maken gebruik van lijsten die worden uitgegeven door derde partijen. Een verzender komt op zo'n lijst terecht als er excessief veel spamklachten zijn geweest of doordat een andere indicator aangeeft dat er een slechte zender reputatie bestaat, zoals bijvoorbeeld het veelvuldig e-mailen naar spam trap adressen. Het kan van tijdelijke aard zijn dat een zender op een blacklist staat vermeld indien de zender de vereiste herstelwerkzaamheden doorvoert. Een verzender die op een blacklist staat vermeld, raden we aan contact op te nemen met de eigenaar van de blacklist voor overleg.

Overzicht actiepunten (blacklisting)

- Alle tactieken die in dit document worden toegelicht om uw reputatie te verbeteren, zorgen ervoor dat u niet op een blacklist wordt geplaatst.
- Monitor publieke blacklists door uw eigen ESP's functionaliteiten te gebruiken, diensten af te nemen van partijen die voor een juiste afleverbaarheid van uw e-mailings zorgen of maak gebruik van standalone blacklist checkers zoals MXToolBox. Wanneer u onverhoopt toch op een blacklist terecht komt: volg de gegeven instructies zodat u van de lijst kan worden verwijderd.

Reputatiefactor: infrastructuur en patronen voor verzendingen

Deze factor heeft betrekking op technische aspecten van het verzendproces zoals de configuratie of de connectie en de informatie die wordt meegezonden met een e-mail. Al deze zaken moeten binnen de normen vallen m.b.t. veiligheid en transparantie die zijn opgesteld voor het verzendproces. Een regelmatige, constante verzending van e-mails zonder specifieke en ongewone pieken draagt ook bij aan een goede reputatie.

Overzicht actiepunten (infrastructuur en patronen voor verzendingen)

- Overleg met een 'aflever' specialist om ervoor te zorgen dat uw systeem en verzendpatronen in lijn zijn met de ISP voorwaarden.
- Als alternatief: maak gebruik van de diensten van een professionele ESP die al beschikt over de juiste infrastructuur en een goed volume management.

11. Hoe een ESP u kan helpen met het succesvol afleveren van meer e-mails

Er wordt een hoop jargon gebruikt in de wereld van het afleveren van e-mails en er bestaan behoorlijk wat (potentiële) valkuilen voordat een e-mail de inbox heeft bereikt van zijn ontvanger. Hoe dan ook, afleverbaarheid is niet de grootste uitdaging wanneer u alle voorzorgsmaatregelen treft en tips volgt die staan omschreven in dit document. Afleverbaarheid wordt beïnvloed door wat u verzendt en hoe u het verzendt.

We kunnen ons goed voorstellen dat u het prettiger vindt deze uitdaging aan te gaan in samenwerking met een professionele ESP. Deze helpt u bij het in goede orde afleveren van uw e-mails, via o.a.:

- Een automatisch bounce management systeem om uw maillijst 'schoon' te houden.
- Ingebouwde spamtesten en andere functionaliteiten die de aflevering en optimalisatie van de aflevering monitoren.
- Geoptimaliseerde gedeelde IP adressen om een 'higher sender' reputatie te kunnen bewerkstelligen voor klanten die geen grote verzendingen verrichten.
- Ondersteuning bij e-mail authenticiteit.
- Ingebouwde feedback loops (FBL) en automatische klachtenverwerking.
- Professionele infrastructures voor verzendingen die voldoen aan de vereiste normen.
- Experts die het e-mailmarketing jargon volledig eigen zijn, de vaak ingewikkelde en wisselende spelregels van de belangrijke ISP's begrijpen en op het hoogste niveau oplossingen kunnen bedenken voor problemen m.b.t. afleverbaarheid.

