Waarom e-mail in spam belandt, en hoe je dat oplost

CRM & Email (FluentCRM) · https://autorespond.nl/docs/waarom-e-mail-in-spam-belandt/

Bijna elk bezorgprobleem op een nieuw platform komt neer op dezelfde drie oorzaken. In volgorde van hoe vaak ze de oorzaak zijn:

1. Je DNS-records kloppen niet

Drie records bepalen of een ontvangende mailserver gelooft dat jij het bent.

SPF geeft aan welke servers namens jouw domein mogen verzenden. Staat de verzendende infrastructuur er niet in, dan zien ontvangers mail die zegt van jouw domein te komen binnenkomen vanaf een plek die nergens vermeld staat.

DKIM ondertekent elk bericht cryptografisch, zodat de ontvanger kan vaststellen dat het bericht niet is gewijzigd en wel degelijk van een bevoegde afzender komt.

DMARC vertelt ontvangers wat ze moeten doen als SPF of DKIM faalt, en vraagt ze om terug te rapporteren. Begin met een beleid dat alleen meekijkt, lees de rapporten een paar weken en scherp het daarna aan.

Wij zetten alle drie voor je klaar. Wordt je DNS elders beheerd, dan sturen we je de exacte waarden. Gok hier niet naar: één verkeerd teken in een SPF-record faalt geruisloos.

2. Je hebt te veel, te snel verstuurd vanaf een nieuwe opzet

Verzendreputatie bouw je op in de tijd, per domein en per verzendende infrastructuur. Een domein dat nog nooit vanaf deze infrastructuur heeft verzonden, heeft geen geschiedenis, en plotseling tienduizend berichten ziet er precies zo uit als een gekaapt account.

Warm in plaats daarvan op. Eerste mailing naar je meest betrokken segment, een paar honderd adressen. Wacht een dag. Kijk naar het openpercentage. Verdubbel daarna. Binnen twee weken zit je op je volle volume, met een reputatie die dat draagt.

3. Je lijst is ouder dan je toestemming

Dit is de ongemakkelijke. Als een flink deel van je lijst in twee jaar niets heeft geopend, levert mailen naar die groep bounces, spamklachten en geen omzet op, en het drukt de bezorging voor de mensen die je mail wel willen.

Voordat je je eerste grote verzending doet, segmenteer je iedereen af die de laatste twaalf maanden niets heeft geopend. Stuur die groep één heractiveringsbericht. Wie niet reageert, mail je niet meer. Je verliest lijstgrootte en wint bezorging.

Je werk controleren

Stuur een test naar een adres bij een grote provider en bekijk de berichtkoppen. Je wilt daar SPF pass, DKIM pass en DMARC pass zien staan. Zegt een van de drie fail of none, los dat dan op voordat je iets echts verstuurt.

Vraag het ons, dan controleren we het samen met je. Het kost tien minuten en het is het enige waarvan je het zekerst wilt zijn.