Februari 2024: Gmail en Yahoo update

Deployteq - Suzanne Martens - 2024-01-11 - Reacties (0) - Deliverability

Gmail en Yahoo scherpen eisen verder aan voor verzenders van e-mail

Vanaf februari 2024 moeten marketeers hun verzonden e-mails laten voldoen aan een nieuwe set regels. Zo moeten e-mails voorzien zijn van e-mailauthenticatie die voldoet aan de verscherpte eisen van Gmail en Yahoo. Ook moet er een eenvoudigere manier zijn om je uit te schrijven van de e-mails en komt er een maximaal aantal ‘spam’ e-mails dat je kunt afleveren bij een e-mailadres. Met deze aanpassingen zorgen Gmail en Yahoo ervoor dat het aantal spamberichten in de inbox verder verlaagd wordt.

Spam gaat verder dan pogingen van hackers en scammers om je creditcardgegevens of je inloggegevens te los te weken. Het gaat ook om e-mails waar de ontvangende partij geen behoefte aan heeft of zich niet voor heeft aangemeld. Een goed schone verzendlijst was al belangrijk, maar met het oog op deze ontwikkeling nóg belangrijker.

Wat verandert er precies ?

Rond februari 2024 zullen bulkverzenders zich moeten houden aan de volgende eisen:

Eenvoudig uitschrijven

Een eenvoudig uitschrijfproces helpt bij het optimaliseren van de gebruikerservaring. Ontvangers moeten zich straks met één klik kunnen afmelden voor commerciële e-mails.

Als e-mailmarketeer betekent dit dat je zult moeten standaardiseren en wellicht ook automatiseren. Verwerk je uitschrijvingen nog handmatig? Dan is het verstandig om eens te gaan kijken of je dit proces kunt automatiseren.

Lagere spamratio’s

Als tweede aanscherping stelt de update van Gmail en Yahoo dat er een strikter beleid komt voor het aantal verzonden e-mails per dag aan een specifiek e-mailadres. Er worden al veel tools ingezet om ongewenste berichten uit de inbox van de ontvanger weren, maar om deze bescherming te optimaliseren heeft Gmail een zogeheten ‘spamdrempel’ ingesteld, waar afzenders onder moeten blijven. Deze spamdrempel betreft 0,3%.

E-mailauthenticatie

Misschien wel de belangrijkste ontwikkeling in dit verhaal is dat Gmail en Yahoo strenger gaan worden op de beveiligingsmaatregelen die je als verzender treft. Een sterke e-mailauthenticatie wordt nog crucialer om te waarborgen dat e-mails daadwerkelijk in de inbox van de ontvanger terecht komen en dus niet in de map met ongewenste e-mails. SPF, DKIM en DMARC worden per februari 2024 vereist wanneer je een bulkverzender bent (meer dan 5000 e-mails per dag).

In het kort: wat houden SPF, DKIM en DMARC ook alweer in?

De meeste e-mailsmarketeers onder ons zullen deze termen wel bekend in de oren klinken. Deze drie termen zijn al sinds jaar-en-dag de standaarden voor e-mailbeveiliging, maar de kracht van herhaling zorgt er vandaag de dag nog steeds voor dat we informatie langer onthouden. Dus, even een opfriscursus.

SPF, oftewel Sender Policy Framework, is een tekstregel die je kunt toevoegen in de instellingen van je domeinnaam en helpt de echtheid van ontvangen e-mails vast te stellen. Dus, als iemand namens jouw domeinnaam een e-mail stuurt, maar die afzender niet in jouw SPF-record staat, komt de mail niet in de inbox van de ontvanger terecht.

De afkorting **DKIM** staat voor Domain Keys Identified Mail. Met DKIM wordt er een soort digitale handtekening ingesteld, waarin staat dat de e-mail van jou afkomstig is.

DMARC staat voor Domain-based Message Authentication, Reporting and Conformance. DMARC is eigenlijk een vervolg op bovengenoemde stappen. Als een e-mail binnenkomt, wordt gekeken of alle controles door SPF en DKIM overeenkomen. Mocht dit niet het geval zijn, wordt de e-mail niet doorgestuurd naar de inbox van de ontvanger. Een mooie feature van DMARC is de rapportagefunctie. Je krijgt een bericht wanneer een e-mail niet door alle controles is heen gekomen en zo weet je dus meteen of je slachtoffer bent geworden van phishing of spoofing.

Extra tips

Voor sommigen is dit misschien heel logisch, maar het belang van een ‘schone’ database is enorm. Door met een e-maillijst met actieve mailadressen te werken voorkom je een hoop onnodige bounces bij de verzending. Filter je e-maillijst op typfouten, bounces en bijvoorbeeld langdurige activiteit. Zo voorkom je een negatief effect op je deliverability.

Een andere tip is het personaliseren van je e-mails. E-mailclients en spamfilters waarderen personalisatie, omdat het aantoont dat de e-mail afkomstig is van een legitieme bron én relevant is voor de ontvanger. Zo heeft jouw verzonden e-mail dus minder kans om als spam gemarkeerd te worden.

Hulp nodig?

Bij Deployteq maken wij standaard gebruik van een eenvoudig en geautomatiseerd afmeldproces in onze mailings en campages. Deze functionaliteit wordt aan iedere verzonden e-mail toegevoegd. Om onder de drempelwaarde van de afgegeven spamdrempel te blijven is het van belang om een schone verzendlijst te hebben, een gezonde verzendfrequentie aan te houden en e-mails zoveel mogelijk gepersonaliseerd te verzenden. Uiteraard kan Deployteq ook assisteren in het toevoegen van de vereiste e-mailauthenticatie.

Denk je nu, wat een ingewikkeld verhaal? Wij helpen je graag bij het instellen, aanpassen of optimaliseren van bovenstaande punten. Neem contact op via support@deployteq.com

Instellingen e-mail validatie

Wanneer e-mailauthenticatie met DKIM op jullie domein niet goed ingeregeld staat toont Deployteq hiervoor een foutmelding. In dat geval is het van belang dat er informatie wordt toegevoegd in het DNS van het domein om ondertekening met DKIM te kunnen faciliteren. In onze handleiding vind je de benodigde DNS instellingen.