

# Die optimale Zustellbarkeit Ihrer E-Mails



# Summary

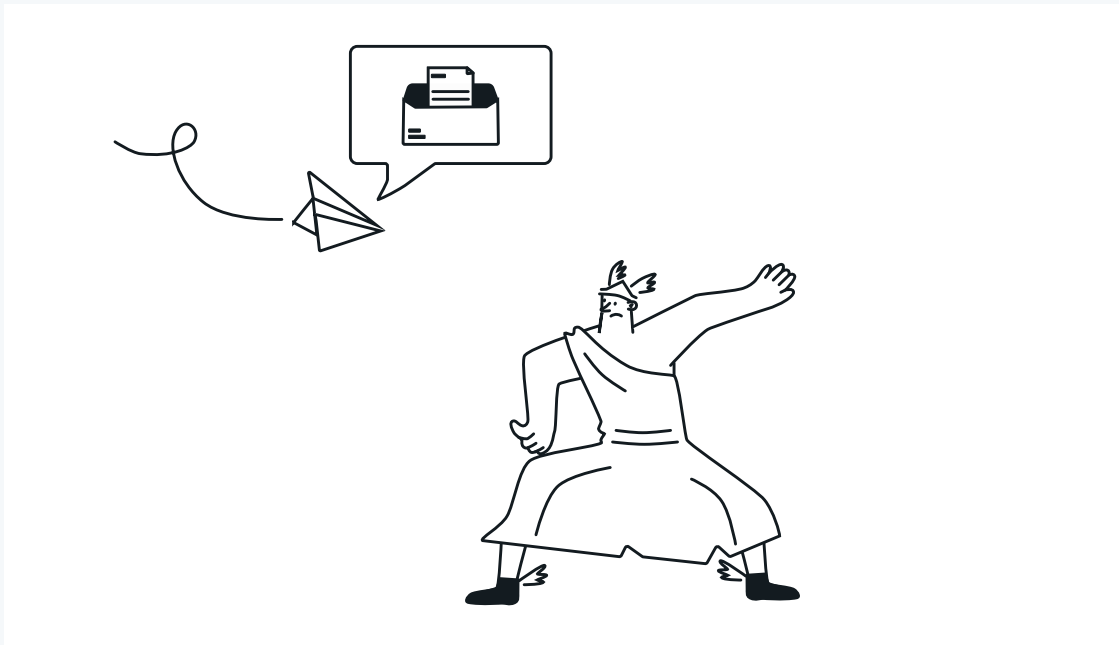
<b>Willkommen .....</b>	<b>3</b>
<b>1. Das Wichtigste zuerst: Was ist Zustellbarkeit? .....</b>	<b>4</b>
Definition der Zustellbarkeit .....	4
<b>2. Die Grundlage für eine optimale Zustellbarkeit.....</b>	<b>5</b>
Authentifizierung .....	5
<b>3. E-Mail Zustellung mit sicherer Geschwindigkeit.....</b>	<b>7</b>
Drosseln Sie Ihren Versand .....	7
Ist eine gemeinsame IP-Adresse für Sie geeignet? .....	7
Besitzen Sie eine dedizierte IP? .....	8
<b>4. Der Einfluss Ihrer Abonnenten auf Ihre Zustellbarkeit.....</b>	<b>10</b>
Stellen Sie ISPs und Ihre Empfänger zufrieden.....	10
Was haben Ihre Abonnenten zu erwarten? .....	11
<b>5. Maßnahmen zur Steigerung Ihrer Glaubwürdigkeit.....</b>	<b>12</b>
Nutzen Sie einen Domain-Namen mit aktiver Webseite.....	12
<b>6. Abschließende Gedanken für den weiteren Weg.....</b>	<b>13</b>
Zur rechtlichen Lage .....	13
Wie man die beliebtesten E-Mail Clients für sich gewinnt .....	14
<b>7. Die Umsetzung der Zustellbarkeit .....</b>	<b>15</b>
<b>8. Wie Mailjet Ihnen helfen kann .....</b>	<b>16</b>
Spezialisierte Customer Success Manager .....	16
Die besten Tools zur Verbesserung der Zustellbarkeit .....	16

# Willkommen

Derzeit landet jede siebte weltweit gesendete Nachricht nicht im Posteingang der E-Mail Empfänger. Diese Zahl kann je nach Branche, Land und Posteingang sehr unterschiedlich sein. E-Mail Marketer zählen die Zustellbarkeit als eine der wichtigsten Hürden für effektives Marketing auf. Von 2018 bis 2019 ist sie um über 12 % gestiegen, wobei 37 % der Marketer dies als Hauptanliegen bezeichneten.

Wie effizient ist es daher für Ihren Erfolg, Zeit mit der Erstellung spannender Inhalte zu verbringen, wenn Ihre Nachrichten gar nicht bei Ihren Abonnenten ankommen? Erfahren Sie In diesem Guide Zustellbarkeit 101, wie Ihre E-Mails in den Posteingängen Ihrer E-Mail Empfänger landen und wie Sie es schaffen, die Bindung Ihrer Abonnenten als Herzstück Ihrer E-Mail Strategie beizubehalten.

Bleiben Sie gespannt! Wir haben Ihnen auf dem Weg wertvolle Informationen mitzugeben, bevor wir am Ziel angekommen sind.



<sup>1</sup> Return Path, Benchmark-Bericht zur Zustellbarkeit, (2018)

<sup>2</sup> Validity, The State of Email Marketing, (2019)



## TEIL 1

# Das Wichtigste zuerst: Was ist Zustellbarkeit?

### Definition der Zustellbarkeit

Viele Ereignisse spielen sich in den Sekunden zwischen dem Versenden Ihrer E-Mail und dem Erreichen der E-Mail im Posteingang des Empfängers ab. Tatsächlich kommt, wie bereits erwähnt, eine von sieben E-Mails gar nicht erst im Posteingang an. Sie landen im Spam-Ordner oder werden von ISPs wie Google Mail und Outlook vollständig blockiert. Eine wenig optimierte Zustellbarkeit ist daher einer der ausschlaggebenden Faktoren, die eine E-Mail am Erreichen Ihres Empfängers hindert.

**Schauen wir uns daher im nächsten Schritt an, wie diese Faktoren aussehen:**

- **Hard bounce:** Bei einem Ein Hard Bounce handelt es sich um das Ereignis, dass eine E-Mail an den Absender zurückgesendet wird, weil sie aus dauerhaften Gründen nicht zugestellt werden konnte. Entweder wurde die E-Mail Adresse falsch eingegeben oder eine gefälschte Adresse eingegeben, weil der Abonnent mehr am Vorteil der Anmeldung oder dem damit zusammenhängenden Angebot interessiert war als am tatsächlichen Erhalt Ihrer E-Mail. Deshalb ist es an dieser Stelle ratsam ein Double-Opt-In einzurichten, da dies mit einer Unterschrift vergleichbar ist. Wir werden später in diesem Leitfaden näher darauf eingehen.
- **Soft bounce:** Bei einem Soft Bounce wird Ihre E-Mail wegen temporären Zustellbarkeitsproblemen an den Absender zurückgesendet. Mögliche Gründe sind, dass der Posteingang des Empfängers voll, der Server down oder die Nachricht zu groß für den Posteingang des Empfängers ist.
- **Spamfilter:** Während die E-Mail durch den Server geleitet wird, finden zahlreiche Prüfungen statt – ISPs (Google Mail, Outlook, AOL) haben Filter eingerichtet, um die Posteingänge der Empfänger vor Spam- oder schädlichen E-Mails zu schützen.

Man sollte immer daran denken, dass die Zustellbarkeitsrate und die Zustellrate nicht das Gleiche sind. Diese beiden Werte klingen ähnlich, sollten aber nicht verwechselt werden. Die Zustellbarkeitsrate wird wie folgt berechnet:

**Zustellbarkeit:** Anzahl der E-Mails, die den Posteingang erreichen, geteilt durch die Anzahl der gesendeten E-Mails

Die Zustellrate enthält alle E-Mails, die vom ISP akzeptiert werden, darunter auch E-Mails, die im Spam-Ordner landen, aber nicht diejenigen, die blockiert werden. Sie können eine Zustellrate von 100 % haben, aber wenn Ihre Zustellbarkeitsrate nur bei 45 % liegt, entgeht Ihnen eine wichtige Gelegenheit, mit Ihren Kunden zu kommunizieren.



## TEIL 2

# Die Grundlage für eine optimale Zustellbarkeit

### Authentifizierung

Es ist sehr wichtig, bei den ISPs (z. B. Google Mail, Outlook usw.) einen guten ersten Eindruck zu hinterlassen, da hiermit angegeben wird, ob und wie Sie mit Ihren Abonnenten interagieren können. Doch denken Sie daran, dass diese das Gleiche wollen wie Sie: eine hervorragende Nutzungserfahrung ihrer Benutzer. Hier sehen Sie einige Schritte, mit denen Sie diese ISPs für sich gewinnen.

ISPs berücksichtigen zahlreiche Faktoren, wenn sie Ihre Absender-Reputation bestimmen. Die Authentifizierung ist nur einer davon. Doch sie ist der erste Schritt, um sicherzustellen, dass Sie auf dem richtigen Weg sind.

Sie können dazu etliche Authentifizierungsprotokolle nutzen:

#### SPF (Sender Policy Framework)

Haben wir nicht alle schon Spam-E-Mails bekommen, die E-Mails von Absendern mit guter Reputation erschreckend echt nachempfunden waren? Es ist überraschend unkompliziert, die „Von“-Adresse nachzuahmen, um betrügerische E-Mails zu versenden. Doch hier kommt SPF ins Spiel!

SPF ist eine der ältesten Formen der Authentifizierung und wurde vor über einem Jahrzehnt zusammen mit DKIM entwickelt. SPF stellt eine Möglichkeit für Domain-Besitzer dar, die Kontrolle über ihre eigene Domain-Reputation zu übernehmen, indem sie andere dazu autorisieren, E-Mails in ihrem Namen zu senden. Das macht automatisch jeden, der nicht in dieser Liste genehmigter Adressen steht, zum Spoofer, der **Täuschungsmethoden in Computernetzwerken zur Verschleierung der eigenen Identität nutzt**. Um mehr über die Einrichtung von SPF zu erfahren, lesen Sie bitte hier unseren nützlichen Leitfaden.

#### DKIM (DomainKeys Identified Mail)

Dies ist eine Methode der ISPs zur Überprüfung, dass es keine Phishing-Versuche gegeben hat.

Sie ermöglicht das Hinzufügen einer eindeutigen Signatur an Ihre E-Mail. Der Empfänger-Server kann die Domain-Signatur überprüfen, um zu bestätigen, dass die Nachricht wirklich von dort kommt, woher sie angibt zu kommen, und dass die Inhalte auf ihrem Weg nicht verändert wurden. Hier finden Sie einen Leitfaden zur Konfigurierung Ihres DKIM.



## **DMARC (Domain-based Message Authentication, Reporting and Conformance)**

Bei DMARC handelt es sich um eine zusätzliche Schutzmaßnahme gegen Domain-Spoofing. Falls SPF und DKIM je versagen, sagt DMARC der Empfänger-Domain, was zu tun ist: die Nachricht ablehnen oder in den Junk-Ordner umleiten.

Domain-Besitzer können die **Richtlinieneinstellung „p=“** nutzen, um Empfänger-Servern zu sagen, was mit E-Mails zu tun ist, die die DMARC-Validierung nicht bestehen.

2014 kündigten AOL und Yahoo eine Änderung ihrer DMARC-Richtlinien in p=reject an, um auf anhaltende Bedrohungen zu reagieren und Google nahm 2016 eine ähnliche Änderung mit Google Mail vor. E-Mails werden abgewiesen, wenn die Domains der „Von“-Adresse und des Absenders nicht übereinstimmen. ESPs können nicht länger Adressen nutzen, die mit @yahoo.com oder @aol.com enden, um E-Mails im Namen von Unternehmen erfolgreich zuzustellen.

## **WHOIS**

WHOIS listet alle Kontaktinformationen auf, die mit einem Domain-Namen zusammenhängen (d. h. den technischen Ansprechpartner, den Domain-Host sowie den vollständigen Namen, E-Mail Adresse, Anschrift und Telefonnummer jeder Referenz).

Die Umstellung des WHOIS auf Privat ist ein charakteristisches Merkmal von Spammern. Halten Sie also Abstand von Anbietern, die dies ermöglichen. Das ist eines der ersten Dinge, die Mailjet prüft, wenn ein Problem auftritt.

## **Forward und reverse DNS lookup**

Von Forward DNS Lookup spricht man, wenn ein Domain-Name verwendet wird, um eine IP-Adresse zu orten. Wenn Sie eine URL in Ihrem Browser eingeben, wird die Adresse an einen nahegelegenen Router übertragen, der daraufhin die IP-Adresse findet. Ein Reverse DNS Lookup ist der umgekehrte Prozess.

*Zu viele Abkürzungen? Haben Sie Schwierigkeiten mit der Einrichtung? Unser technisches Team ist rund um die Uhr für Sie da.*

ISPs und E-Mail Clients nutzen diese Prozesse häufig, um Ihre Identität zu überprüfen. Wenn Sie mit Mailjet E-Mails versenden, übernehmen wir diese gesamte Konfiguration für Sie.

Sobald Sie alles eingerichtet und konfiguriert haben, sollten Sie mit der Überprüfung Ihrer Sendegeschwindigkeit fortfahren.



### TEIL 3

# E-Mail Zustellung mit sicherer Geschwindigkeit

Drosseln Sie Ihren Versand

Die meisten Leute tendieren zu dem Irrglauben, dass schnelles Handeln die beste Art ist, um sein Ziel schnell zu erreichen. Ob auf einer Autobahn oder beim Versenden von E-Mails, Verkehrspolizei und Rüttelschwellen können schwerwiegende Probleme verursachen. Doch wenn Sie zu schnell zu viele E-Mails senden, stoßen Sie auf Ihrer Reise auf Widerstand.

Die meisten ISPs überwachen für die Bestimmung der Reputation eines Absenders eine 30-tägige Sendehistorie. Wenn einem ISP eine Spitze oder eine Abweichung des Volumens auffällt, kann das verdächtig erscheinen und ISPs den Eindruck vermitteln, dass die IP des Benutzers gefährdet ist. Das kann dazu führen, dass die Absender-IP (oder -Domain) temporär geblockt (oder gedrosselt) wird, um die Endnutzer und ihre Posteingänge zu schützen.

Der Schlüssel zum Erfolg ist eine langsame und beständige Herangehensweise. Senden Sie Ihre E-Mails mit gleichbleibendem Volumen und konsistenter Häufigkeit. Wenn Sie gerade erst anfangen und Ihr Sendevolumen erhöhen möchten, fahren Sie Ihr Sendevolumen langsam hoch, um ISPs keine falschen Signale zu geben.

Ist eine gemeinsame IP-Adresse für Sie geeignet?

ISPs betrachten für gewöhnlich Ihre Aktivitäten der letzten 30 Tage vor Ihrem Versand. Falls Sie **unregelmäßig oder wenig versenden**, haben Sie möglicherweise keine Reputation, auch dann nicht, wenn sie schon längere Zeit E-Mails versenden. Dies bedeutet, dass Sie Ihre IP-Reputation jeden Monat von Grund auf neu aufbauen würden.

Glücklicherweise können Sie über eine gemeinsame IP auf andere zählen, um Ihre Reputation und Volumenhistorie gemeinsam aufrechtzuerhalten. Die Verantwortung liegt hierbei nicht bei Ihnen allein.

So werden Sie auch **Zeit und Geld sparen**. Mit einer gemeinsamen IP können Sie bei Bedarf größere Volumina ohne Aufwärmen versenden. Wenn Sie Ihre E-Mails saisonal und mit starken Schwankungen das gesamte Jahr über versenden, ist dies empfehlenswert. Außerdem ist diese Methode günstiger als eine dedizierte IP.

Bei Mailjet beobachten wir all unsere gemeinsamen Absender, um sicherzustellen, dass sie sich an die Best Practices der Zustellbarkeit und an die Richtlinien zum Versenden von E-Mails von Mailjet halten. Falls ein Problem auftritt, nutzen wir unsere Vertrauensbeziehungen mit ISPs, um das Problem so schnell wie möglich zu behandeln und zu beheben.





Es kann jedoch vorkommen, dass eine E-Mail, die von jemandem gesendet wird, der dieselbe gemeinsame IP-Adresse verwendet wie Sie, die Zustellbarkeit Ihrer Nachrichten beeinträchtigt. Falls Sie daher große Volumina versenden, empfehlen wir eine dedizierte IP (eine eindeutige IP-Adresse, die exklusiv einem einzelnen Hosting-Account zugewiesen ist).

Besitzen Sie eine dedizierte IP?

Mit einer dedizierten IP können Sie Ihre Reputation gegen andere Benutzer abschirmen. Das bedeutet:

Sie haben eine größere Verantwortung für und mehr Kontrolle über Ihre Reputation

Wir können die Ursache jedes beliebigen Problems einfacher und schneller feststellen

Versenden Sie mit jedem Versand über 10 000 E-Mails? Und versenden Sie regelmäßig gleichbleibende Volumina?

*Die dedizierte IP steht Ihnen mit unseren Plänen ab einem Sendevolumen von über 150 000 E-Mails pro Monat und mehr zur Verfügung.*

Das Aufwärmen Ihrer brandneuen IP

Falls Sie mit einer brandneuen IP beginnen, können ISPs auf keine Sendehistorie zurückgreifen. Bei Ihrem ersten Versand werden sie versuchen, Sie einzuordnen, indem sie die Qualität Ihrer E-Mails bewerten und beobachten, wie Empfänger auf Sie reagieren.

Um Ihr Sendeverhalten dahingehend zu optimieren, empfiehlt es sich Ihre IP aufzuwärmen. Erhöhen Sie Ihr Sendevolumen gleichmäßig und stufenweise. Eine plötzliche Spitze beim Versandvolumen wirkt verdächtig, also gewinnen Sie das Rennen eher mit einer langsamen und gleichmäßigen Herangehensweise.

Wie bereits erwähnt, ist die Aufwärmphase für Benutzer, die E-Mails von einer gemeinsamen IP senden, nicht erforderlich.

Trennen Ihrer Transaktions- und Marketing E-Mails

Ein weiterer zu berücksichtigender Punkt für Versender mit großem Sendevolumen ist die Trennung Ihrer Transaktions- und Marketing E-Mails, um etwaige Probleme bei der Zustellbarkeit besser erkennen und behandeln zu können.

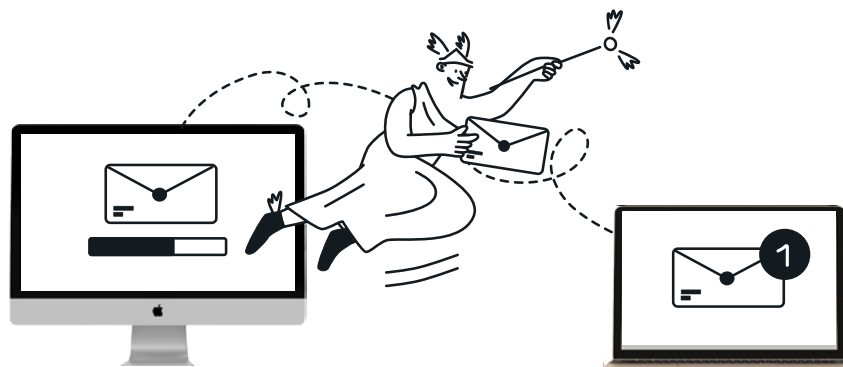




Marketing E-Mails werden mit höherer Wahrscheinlichkeit als Spam markiert oder abbestellt. Der Grund dafür ist, dass Marketing E-Mails in großen Mengen an viele Kontakte gleichzeitig gesendet werden, häufig ohne direkte Ansprache oder Personalisierung der Kunden. Transaktions-E-Mails hingegen sind persönliche Mitteilungen, die an einen bestimmten Empfänger gesendet werden, normalerweise, nachdem eine bestimmte Aktion ausgeführt wurde (z. B. ein Zurücksetzen des Passwortes, ein Kauf...). Daher ist es wichtig, Ihre Transaktions-E-Mails getrennt zu versenden, um sicherzustellen, dass sich Ihre Reputation unter diesen E-Mails nicht verschlechtert.

*Mit Mailjet können Sie Nebenkonten erstellen, um Ihren E-Mail Versand ganz einfach aufzuteilen.*

Sind Sie immer noch unsicher, was Sie brauchen? Das Mailjet Team hilft Ihnen, eine Lösung zu finden, die am besten zu Ihrem Sendeverhalten passt. Setzen Sie sich mit unserem Kundensupport in Verbindung, wenn Sie mehr erfahren möchten.



## TEIL 4

# Der Einfluss Ihrer Abonnenten auf Ihre Zustellbarkeit

### **Stellen Sie ISPs und Ihre Empfänger zufrieden**

„Der Kunde ist König“, wie es so schön heißt. Wenn Sie Ihren Kunden an die erste Stelle setzen und es sich zur Priorität machen, transparent zu sein und Versprechen zu halten, stellen Sie sicher, dass Ihre Abonnenten Ihnen treu bleiben.

Authentizität und qualitativ hochwertige Inhalte sind der Schlüssel im zunehmend wettbewerbsorientierten digitalen Raum. ISPs sorgen für die Benutzerfreundlichkeit des Posteingangs, indem sie verfolgen, an welcher Art von Inhalten Ihre Benutzer interessiert sind und welche sie nicht so gern mögen (Spam). Deshalb landen E-Mails von beliebten Absendern öfter im Posteingang und E-Mails von unbeliebten Absendern häufig im Spam-Ordner. Sie können das Interesse Ihrer Kontakte messen, indem Sie sich Ihre Öffnungs- und Klickraten ansehen.

Um ISPs und Ihre Kunden für sich zu gewinnen, sollten Sie Ihren Kunden hochwertige Inhalte anbieten. Seien Sie von Anfang an ehrlich – halten Sie die Versprechen, die Sie bei der Anmeldung geben, und halten Sie die Benutzer auf emotionaler Ebene beschäftigt. Hier erfahren Sie mehr dazu.

Stellen Sie sicher, dass Sie Ihre E-Mails segmentieren und eine intelligente Personalisierung anwenden und so sicherstellen, dass Ihre Inhalte künftig bei Ihren Empfängern Anklang finden. Vergessen Sie auch nicht, Ihre Kontaktliste regelmäßig zu reinigen, um inaktive Kontakte und ungültige E-Mail Adressen zu entfernen, die Ihre Zustellbarkeit beeinträchtigen könnten.

*Teilen Sie Ihren Abonnenten und Benutzern mit, was sie zu erwarten haben.*



## **Was haben Ihre Abonnenten zu erwarten?**

**Holen Sie das ausdrückliche Einverständnis Ihres Abonnenten ein, seine persönlichen Daten in sämtlicher E-Mail Kommunikation zu nutzen.**

Klarheit bei der Anmeldung bedeutet, dass Sie letztendlich eine sauberere Liste an Kontakten haben. Sie sollten Ihren Kunden genau sagen, für was sie sich anmelden und auf welche Art ihre Informationen verwendet werden. Das schafft Vertrauen und sorgt für höhere Öffnungs- und Klickraten und geringere Abmeldungs- und Beschwerderaten, sobald die Abonnenten anfangen, Ihre E-Mails zu erhalten.

Um auf das Thema des Double-Opt-In zurückzukommen, das wir vor ein paar Seiten in diesem Leitfaden erwähnt haben: Wenn Sie einem Benutzer gleich nach seiner Anmeldung eine Bestätigungs-E-Mail mit einem Bestätigungs-Link senden, können Sie damit sicherstellen, dass die angegebene E-Mail Adresse korrekt und aktiv ist und dass sich der Benutzer auf Ihre Inhalte freut.

**Bestärken Sie Ihren Abonnenten. Der Benutzer hat ein Recht auf Vergessenwerden.**

Stellen Sie klar, dass der Kunde sich jederzeit abmelden und Sie auch bitten kann, jegliche persönlichen Datenaufzeichnungen über ihn vollständig zu löschen. Antworten Sie auf diese Anfragen und entfernen Sie den Kunden umgehend aus Ihrer Liste.

Mit politischen Reformen (wie der DSGVO) ist es noch wichtiger geworden, sicherzustellen, dass Benutzer mehr Einfluss darauf haben, was mit ihren Daten geschieht, damit Ihre Abonnenten ihre E-Mail Einstellungen einfach verwalten und mit ihren persönlichen Daten arbeiten können.



## TEIL 5

# Maßnahmen zur Steigerung Ihrer Glaubwürdigkeit

### **Nutzen Sie einen Domain-Namen mit aktiver Webseite**

Durch den absichtlichen oder versehentlichen Gebrauch eines Domain-Namens, der zu einer nicht funktionierenden Webseite führt, wird Ihre Glaubwürdigkeit und die des ISPs geschmälert. Das ist etwas, was die Absender vieler Spam- oder Phishing E-Mails tun. Es beeinträchtigt die Legitimität Ihrer Nachricht (und Ihre Absender-Reputation), wodurch wiederum die Verifizierung durch die Server Ihrer Kontakte schwieriger wird.

#### **Vergewissern Sie sich, dass Ihr Domain-Name:**

- Erkennbar ist und mit Ihrer beworbenen Marke übereinstimmt. Wenn Sie beispielsweise E-Mails im Namen einer E-Commerce Seite für Hundehalter versenden, sollten Sie nicht die Absender-Domain „katzenandiemacht.de“ nutzen.
- Mit einer Webseite verbunden ist, die von Suchmaschinen gecrawlt werden kann.
- Mindestens eine Seite mit Infos über Ihr Unternehmen, eine Datenschutzrichtlinie und detaillierte Kontaktinformationen des Unternehmens enthält, entweder über ein Kontaktformular oder durch die Angabe der E-Mail Adresse, Anschrift und/oder Telefonnummer auf der Webseite.

### **Konfigurieren Sie abuse@- und postmaster@-E-Mail Adressen**

Die abuse@- und postmaster@-Adressen werden für den Empfang von Kundenbeschwerden bzw. Verarbeitungsfehlern verwendet. Sind diese Adressen nicht für Ihre Absender-Domains konfiguriert, führen diese Probleme zu Fehlern bei ISPs. Daran erkennen E-Mail Kunden, dass Sie diese Nachrichten nicht überwachen.

Achtung: Wenn unsere Adresse abuse@mailjet.com kontaktiert wird, wird unser Team benachrichtigt und Ihre Praktiken werden daraufhin möglicherweise genau untersucht. Beachten Sie auch, dass diese Adressen für bestimmte Whitelisting-Verfahren benötigt werden. Wenn Sie also möchten, dass Ihre Reputation einwandfrei ist, sollten Sie sie schnell konfigurieren.

### **Machen Sie sich bei Ihren Abonnenten beliebt**

Benutzer fügen Absender, denen sie vertrauen, zu ihren Kontakten hinzu. Laden Sie Ihren Abonnenten ein, Sie zu seinem Adressbuch hinzuzufügen. Das zeigt Spamfiltern, dass Ihre Empfänger tatsächlich von Ihnen hören wollen. Unten sehen Sie ein Beispiel von Foursquare. Im unteren Teil jeder E-Mail fügen sie eine Zeile ein, die Abonnenten einen Link bereitstellt, mit dem sie Foursquare einfach zu Ihrem Adressbuch hinzufügen können, sodass die E-Mails nicht im Nirgendwo hängenbleiben.



## TEIL 6

# Abschließende Gedanken für den weiteren Weg

### Zur rechtlichen Lage

Die globalen Anti-Spam-Gesetze ändern sich ständig. Es ist wichtig, auf dem neuesten Stand zu bleiben, um Ihren E-Mails nicht Unrecht zu tun.

Senden Sie nach oder aus:

- **Der EU?** Stellen Sie sicher, dass Sie die Anforderungen der DSGVO erfüllen, wenn es um das Versenden und das Listenmanagement geht.
- **USA oder Canada?** Sie sollten in Bezug auf die Richtlinien CAN-SPAM bzw. CASL auf dem neuesten Stand bleiben. Vergewissern Sie sich auch, dass Sie die lokalen Datenschutzgesetze kennen, die in den verschiedenen Bundesstaaten gelten, wie z.B. den California Consumer Privacy Act (CCPA).
- **Großbritannien?** Die Richtlinie für Datenschutz und elektronische Kommunikation (EG-Richtlinie) verbietet das Senden automatisierter Marketing-Mitteilungen an Abonnenten ohne deren vorheriges Einverständnis. Es gibt allerdings „Soft-Opt-In“-Ausnahmen, bei denen das Einverständnis impliziert wird. Sie können sich hier darüber informieren.

Anti-Spam Gesetze mögen sich von Land zu Land unterscheiden, doch wir konnten sie zu ein paar universellen, umsetzbaren Schlussfolgerungen zusammenfassen:

**Nutzen Sie eine Double-Opt-In Option für Ihre erste Kampagne, um sofort an das Einverständnis der Benutzer zu gelangen.** Möglicherweise hat ein Benutzer bei der Anmeldung die falsche Adresse angegeben oder sich sogar mit schädlichen Absichten angemeldet. Vergewissern Sie sich, dass Ihre Kunden sich auf Ihre Inhalte freuen, und stellen Sie sicher, dass Sie an keine inaktiven Konten versenden.

**Binden Sie einen eindeutigen Link zur Abmeldung ein.** Ihr Absendername und der Link zur Abmeldung sollten in jeder E-Mail klar erkennbar sein – nicht nur aus rechtlichen Gründen, sondern auch, um die Rechte Ihrer Abonnenten zu würdigen (und um Ihre Absender-Reputation und den Ruf Ihres Unternehmens makellos zu halten!)

Sie haben sich also authentifiziert, die richtige IP gefunden und wissen, wie Sie Ihre Absender-Reputation rechtmäßig hoch halten.

Achtung: Es gibt einen weiteren Faktor, der Ihre Zustellbarkeit beeinflussen kann: eine fehlende Anpassung Ihrer E-Mails an die Anforderungen einzelner ISPs.



## Wie man die beliebtesten E-Mail Clients für sich gewinnt

**Heutzutage ist die wichtigste Metrik, die alle E-Mail Clients für die Platzierung im Posteingang berücksichtigen, das Benutzerengagement (Öffnungen, Klicks...).** Alle Webmail-Anbieter haben ihre Eigenarten. Möglicherweise sollten Sie Ihre Taktik ein bisschen an ihre unterschiedlichen Voraussetzungen anpassen.

**Gmail kategorisiert gerne.** E-Mails entwickeln sich immer mehr zu einer kundenorientierten Erfahrung. Kürzlich führte Gmail Registerkarten im Posteingang ein, die Nachrichten in Kategorien wie Allgemein, Soziale Netzwerke und Werbung einordnen. Der Algorithmus für diese Einordnung basiert auf dem Feedback von Benutzern. Unterstützen Sie Gmail und trennen Sie Ihre Transaktions- und Marketingnachrichten. Damit wird ebenfalls sichergestellt, dass Ihre Nachricht richtig ankommt.

**Hotmail, Outlook und Yahoo halten es gerne einfach.** Hotmail und Outlook empfehlen, Ihre E-Mails nicht über zu viele IP-Adressen zu verteilen, um Ihr Volumen gering zu halten. Yahoo hat es gerne so simpel wie möglich. Fügen Sie keine HTML-Formulare, JavaScript oder eingebettete Objekte wie Flash oder ActiveX ein.



TEIL 7

# Die Umsetzung der Zustellbarkeit

Setzen Sie diese Tipps noch heute um und sorgen Sie dafür, dass Ihre E-Mails nicht im Spam-Ordner landen.

Das Mailjet Team ist stolz darauf, dass Zustellbarkeit eine unserer wichtigsten Stärken ist. Wir arbeiten eng mit ISPs und E-Mail Clients zusammen, um Sie dabei zu unterstützen, mehr Zeit mit der Bereitstellung spannender Inhalte aufzuwenden.





## TEIL 8

# Wie Mailjet Ihnen helfen kann

### Spezialisierte Customer Success Manager

Es spielt keine Rolle, ob Sie das Interesse der Kunden wecken, den Umsatz steigern oder eine höhere Zustellbarkeitsrate erzielen möchten. Unser Expertenteam verhilft Ihnen zum Erfolg. Dank maßgeschneiderter Onboarding-, Schulungs- und Beratungsdienste können Ihre Teams Mailjet optimal nutzen und von umsetzbaren Strategien zum Aufbau einer effizienten E-Mail Kampagne profitieren.

### Die besten Tools zur Verbesserung der Zustellbarkeit

Bei Mailjet bieten wir Funktionen wie E-Mail Bestätigungen und Inbox Preview, damit Benutzer die Kontrolle über ihre Zustellbarkeit übernehmen. Mailjet verwendet außerdem branchenführende Zustellungstools wie 250ok und SendForensics, um Ihnen einen klaren Plan zu erstellen, Ihre Absender-Reputation zu optimieren. Wir nutzen diese Tools außerdem dafür, um einen gemeinsamen IP-Pool zu erstellen, um so die Zustellbarkeit all unserer Kunden zu verbessern.

- Um mehr über unsere Zustelloptionen für Unternehmen zu erfahren, [vereinbaren Sie jetzt einen Termin mit einem unserer Zustellbarkeitsexperten](#).
- Möchten Sie sich für eine optimale Zustellbarkeit unserer gemeinsamen IP-Adresse anschließen? [Jetzt kostenlos anmelden!](#)
- In unserem [Blog](#) finden Sie weitere Tipps und [abonnieren Sie unsere Newsletter](#)-Liste, um sicherzustellen, dass Sie Neuigkeiten nicht verpassen.
- Haben Sie Fragen zum Gelesenen oder brauchen Sie Hilfe, um alles einzurichten? Zögern Sie nicht, unseren [Kundensupport](#) zu kontaktieren. Wir freuen uns darauf, Ihnen zu helfen!





Pathwire befähigt 100.000 zahlende Kunden auf der ganzen Welt, komplexe Kommunikationsprobleme zu lösen. Mit seiner leistungsstarken E-Mail-API und intuitiven E-Mail-Marketing-Lösungen liefert Pathwire jährlich mehr als 250 Milliarden E-Mails für Unternehmen wie DHL, Wikipedia, Toast, Lyft und Microsoft aus.

Das Unternehmen bietet eine zuverlässige, Cloud-native Infrastruktur, lokale Expertise und intelligente Lösungen, die auf maschinellem Lernen basieren, damit Unternehmen ihre Kunden leichter erreichen und vernetzte Erlebnisse schaffen können. Pathwire hat weltweit Niederlassungen, unter anderem in Großbritannien, Spanien, Frankreich, Deutschland und den USA.

Weitere Informationen finden Sie unter [www.pathwire.com/de](http://www.pathwire.com/de).

