epsilon international™
Marketing As Usual. Not A Chance.™

# Leitfaden zu Blacklists und der Zustellbarkeit von E-Mails


**Dieser Leitfaden enthält Informationen zu Blacklists, Tipps, wie man diese vermeiden kann sowie Erläuterungen dazu, inwieweit das Email Deliverability Management von Epsilon International (EDM) Ihnen dabei helfen kann.**

**'Blacklist' (Schwarze Liste) ist eine allgemeine Bezeichnung für eine Auflistung von Domains, IP-Adressen oder URLs, die von bekannten Spammern genutzt werden. Diese Listen werden entweder intern gehostet oder sind im Internet verfügbar und sind eine sehr verbreitete Methode, um E-Mails von Absendern, die in ihnen aufgeführt sind, zu sperren.**

## Die verschiedenen Arten der Blacklist

### Blacklists für Domainnamen (RHSBL)

Auf Blacklists für Domainnamen werden Domainnamen aufgeführt, die mit bekannten Spammern in Zusammenhang stehen. Diese Listen werden manchmal RHSBLs (Right Hand Side Blacklist) genannt, da sie die rechte Seite der Absender-E-Mailadresse auflisten – den Domainnamen nach dem @.

Blacklists für Domainnamen sind nicht besonders wirkungsvoll, da die meisten Spammer entweder gefälschte „von"-Adressen oder Adressen aus beliebten Freemail-Domainnamen wie @gmail.com, @yahoo.com oder @hotmail.com verwenden. Außerdem glauben viele Experten für Spam-Bekämpfung, dass das Zurückverfolgen von Domains nur in begrenztem Maße wirkungsvoll sein kann, da professionelle Spammer dafür bekannt sind, ständig ihre Domains zu wechseln.

### Blacklists für IP-Adressen (DNSBL)

IP Blacklists für IP-Adressen identifizieren Adressen oder Adressbereiche, die mit bekannten Spammern oder ungenutzten IP-Adressen in Zusammenhang stehen. Die Technologie, mit der sie vorgehen, basiert auf dem Internet Domain Name System (DNS), daher nennt man diese Listen ganz allgemein DNSBLs (Domain Name System Blacklist).

Die meisten modernen Mailserver setzen die DNSBLs ein, die es den Administratoren des Mailservers ermöglichen, E-Mailadressen, die in einer spezifischen DNSBL enthalten sind, zu blocken und so die Anzahl der Spam-Mails einzudämmen. Außerdem werden DNSBLs oftmals als Bestandteil von Spam-Scoring-Systemen verwendet. Ist man auf einer DNSBL aufgeführt, die in einem Spam-Scoring-System erfasst ist, könnte sich die eigene Spam-Punktezahl (Spam-Score) erhöhen (die Kriterien für die Erhöhung variieren). Falls die Punktezahl durch zusätzlich durchgeführte Scoring Tests einen bestimmten Richtwert übersteigt, kann die E-Mail aussortiert oder in den Spamordner gefiltert werden.

## Die verschiedenen Arten der Blacklist (Fortsetzung)

Es gibt Dutzende von DNSBLs und jede einzelne hat andere Kriterien für die Aufnahme von IP-Adressen. Einige enthalten wegen ihrer strengen Kriterien und mangelnder Datenpflege auch seriöse Adressen, die in keiner Weise mit Spam in Zusammenhang stehen. Diese Listen werden von Providern, denen etwas daran liegt, dass seriöse Mails ankommen, nur sehr eingeschränkt eingesetzt. Andere DNSBLs sind etwas konservativer und versuchen, wirklich nur die unseriösen Spammer aufzuführen. Diese konservativen Blacklists werden zumeist von Providern und Mailservern eingesetzt.

### URI DNSBLs

URI (Uniform Resource Identifier) -DNSBLs führen Domains und IP-Adressen auf, die im Body der Spam-Mails auftauchen (in der Regel nicht in seriösen E-Mails), anstatt die Senderdomains oder IP-Adressen aufzuführen. Sie sind in der Regel sehr wirkungsvoll und werden von den meisten Spamfiltern eingesetzt.

URI-DNSBLs wurden geschaffen, als ersichtlich wurde, dass Spamfilter selbst im engen Zeitfenster zwischen der ersten Nutzung einer IP-Adresse durch den Versender und deren Erfassung in größeren DNSBLs erhebliche Mengen an Spam-Mails durchgehen ließen. In vielen Fällen können Domainnamen und IP-Adressen (unter dem Sammelbegriff URIs bekannt) im Body der Nachrichten schon zuvor aussortierten Spam-Mails zugeordnet und die Mail damit als unseriöse Mail identifiziert werden. Wenn ein Spamfilter also alle URIs aus einer Nachricht herausfiltert und mit einer URI-DNSBL abgleicht, kann die Spam-Mail blockiert werden, auch wenn die Absender-IP-Adresse für diese Spam-Mail noch nicht auf einer entsprechenden DNSBL erfasst wurde.

## Gründe für die Erstellung von Blacklists

### Beschwerden von Empfängern

Spam-Beschwerden sind der wichtigste Grund dafür, dass die Zustellung von E-Mails durch Provider reguliert wird, die ihre User in erster Linie vor unwillkommenen E-Mails schützen wollen. Wenn eine Nachricht eine ausreichende Anzahl von Beschwerden hervorruft, wird sie vom Provider in den Spamordner geleitet, sie wird geblockt oder es werden anderweitige Maßnahmen getroffen, um die User zu schützen. In der Regel treffen Provider Maßnahmen gegen E-Mails, bei denen mehr als 1% aller Empfänger Beschwerde einlegen. Dies wird umso wahrscheinlicher, je neuer Domains sind und je weniger ihr Ruf gefestigt ist.

### Spam-Fallen

Spam-Fallen sind E-Mailadressen, die nicht zur Kommunikation verwendet, sondern eigens zur Identifikation von Spammern eingerichtet werden. Diese E-Mailadressen werden typischerweise nur an einem nicht-öffentlichen Ort bekannt gegeben, so dass sie bei der automatischen Datensammlung (wie sie von Spammern betrieben wird) aufgespürt werden können, aber kein Absender jemals dazu aufgefordert wird, an diese Adresse seriöse Mails zu senden. Dadurch kann jede E-Mail, die bei dieser Adresse eingeht, eindeutig als unerwünscht und damit als Spam eingestuft werden.

Der Einsatz von Spam-Fallen ist weit verbreitet bei Blacklists, den meisten großen Providern, vielen Spamfilter-Anbietern und Anti-Spam-Diensten (u.a. SpamCop, Passive Spam Block List (PSBL), Brightmail). Manche Unternehmen suchen in verschiedenen Fallen nach Treffern, manche verwenden zur Einstufung Spam-Fallen im Zusammenspiel mit anderen Kriterien, doch in der Regel ist es wahrscheinlich, dass man direkt oder indirekt auf einer Blacklist landet, wenn man in eine Spam-Falle geht (d.h. wenn man an sie eine Mail sendet).

## Sicherheit des sendenden Mailservers

Die meisten Blacklists verbieten E-Mails, die von ungesicherten Servern gesendet werden – d.h. Open-Relay-Server. Solche ungesicherten Server stehen Spammern zur Nutzung frei und sie können ihre Mails über Mailserver Dritter umleiten, um von den Resourcen der Open-Relay-Server zu profitieren, um eine Aufdeckung zu vermeiden und die Adressfälschung zu erleichtern. Sobald ein Mailserver, der den Mailverkehr Dritter zulässt, erkannt oder gemeldet wird, wird er auf einer oder mehreren Blacklists aufgeführt und andere Mailserver, die diese Listen einsetzen, blocken E-Mails von diesen Seiten.

## Hohe Anzahl unbekannter Empfänger

Eine hohe Anzahl unbekannter Empfänger und Hard Bounces (Annahme der E-Mail wird verweigert) werden in der Regel mit Spammern assoziiert, die sich wenig um Datenbereinigung kümmern. So hat eine hohe Anzahl unbekannter Empfänger eine beträchtliche Auswirkung auf die Zustellbarkeit – Return Path berichtet, dass Absender mit 10% unbekannter Empfänger oder mehr davon ausgehen können, dass nur 44% ihrer Mails zugestellt werden.

## Erhöhte Spam-Scores

Die meisten E-Mailfilter verwenden einen „Spam-Score" um zu bestimmen, ob eine E-Mail Spam ist oder nicht. Bei der Vergabe der Scores werden in der Regel eine Menge von Faktoren in Betracht gezogen, z.B. Inhalt, Länge, Textanteil, Verwendung von Bildern, Anzahl der Empfänger, E-Mail-Header.

Falls der Score der Mail einen bestimmten Richtwert überschreitet, wird die Mail geblockt und landet im Spamordner. Die Höhe des Richtwerts wird bei der Konfiguration des Mailservers festgelegt. Standardmäßig stuft der Spamfilter Mails mit einem Score höher als 5 als Spam ein. Erhöhte Spam-Scores über einen bestimmten Zeitraum hinweg (dies variiert von Provider zu Provider) führen meistens nicht nur dazu, dass die E-Mails in Spamordnern abgelegt, sondern auch in Blacklists aufgenommen werden.

## Keine Links zum Abbestellen

Alle E-Mails müssen ihren Empfängern eine oder mehrere der folgenden Möglichkeiten zum Abbestellen anbieten:

- Einen URL-Link, über den man sich auf eine Website zum Abbestellen klicken kann
- Die Option zur Beantwortung der Mail mit dem Betreff „Abbestellen"
- Die Option, eine neue E-Mail unter Angabe des Benutzernamens zu versenden

## RFC-Richtlinien

Die RFC-Serie (Request for Comments) ist eine Sammlung von technischen und organisatorischen Dokumenten über das Internet, in denen ein Standard für E-Mailadressen festgelegt wird. Eine E-Mailadresse muss aus zwei Teilen bestehen – einem lokalen Teil und einem Domainnamen – mit einem „@"-Zeichen.

Der „lokale Teil" einer E-Mailadresse kann aus bis zu 64 Zeichen bestehen (Server werden jedoch aufgefordert, sich nicht selbst eine Grenze mit lediglich 64 Zeichen zu setzen) und der Domainname kann aus bis zu 255 Zeichen bestehen. Der lokale Teil der E-Mailadresse kann folgende ASCII-Zeichen enthalten:

- Groß- und Kleinbuchstaben
- C Das Zeichen . vorausgesetzt, es ist nicht das erste oder das letzte Zeichen und kommt nicht zweimal oder mehr in Folge vor
- Die Zeichen ! # $ % * / ? | ^ { } ` ~ & ' + - = _
- Ziffern 0 bis 9

epsilon international™
Marketing As Usual. Not A Chance.™

# So können Sie Blacklists umgehen

Zur Pflege des guten Rufs und zur Minderung des Risikos auf einer Blacklist zu landen, gibt es eine Reihe empfehlenswerter Maßnahmen.

## Verringern Sie Spam-Beschwerden

Die Kundenerwartungen sollten erfüllt werden, indem direkt auf der Anmeldeseite detaillierte Informationen über die Art und Häufigkeit der versendeten Mails zu finden sind. Diese Aussagen bezüglich Inhalt und Häufigkeit der Mails sollten zukünftig eingehalten werden, damit der Kunde weiterhin nur Mails im Rahmen der von ihm abonnierten Dienste erhält.

Auf der Anmeldeseite sollte für den Kunden ebenfalls die Möglichkeit bestehen, über die Nachrichten, die er erhält, zu bestimmen. Auswahlmöglichkeiten hinsichtlich des Formats der Nachricht, der Häufigkeit der Zustellung und Produkt- und Themenkategorien, ermöglicht es dem Kunden, die E-Mails auf seinen Geschmack zuzuschneiden, was den Erhalt der Mails für den Kunden wesentlich attraktiver macht und die Wahrscheinlichkeit zukünftiger Beschwerden verringert.

Bitten Sie den Kunden um Feedback. Wenn Sie Ihren Kunden kennen lernen und diese Informationen zu Verbesserung ihrer Kommunikation aufwenden, können Sie sowohl die Beschwerden verringern als auch den Inhalt so personalisieren, dass der Kunde dies auch zu schätzen weiß. Wenn Sie den Kunden darum bitten, Ihre Unternehmensadresse im „Von"-Feld in seinem Adressbuch abzuspeichern, werden Sie insgesamt seltener Opfer von Spamfiltern und erhöhen somit erheblich die Wahrscheinlichkeit, im Posteingang zu landen.

Außerdem sollte auch die Option zum Abbestellen klar ersichtlich und leicht durchzuführen sein sowie einer regelmäßigen Kontrolle unterzogen werden. Falls sich jemand über den von Ihnen vorgegebenen Weg abmeldet und dies nicht gelingt, wird die nächste Mail von Ihnen an diese Person höchstwahrscheinlich als Spam verzeichnet.

## Opt-In-Strategie

Eine Opt-In/Opt-Out-Strategie in Kombination mit ständiger Datenbereinigung in Ihren Verteilerlisten sind die wirkungsvollsten Wege, um eine hohe Zustellungswahrscheinlichkeit zu gewährleisten. Die enge Zusammenarbeit mit Anbietern von Adresssammlungen ist von hoher Bedeutung, wenn es darum geht, deren Opt-In-Strategie sowie die Qualität der Verteilerlisten zu ermitteln.

Es sollten Maßnahmen zur Datenbereinigung eingeführt werden, die Folgendes beinhalten:

- Nachweis des Opt-In
- Datum, an dem die E-Mailadresse aufgelistet wurde (Alter der Verteilerliste)
- Datum, an dem die Liste zuletzt versandt wurde

Dies ist besonders wichtig, da bei Adresssammlungen, die länger nicht verwendet wurden:

- die Adressen in Spam-Fallen umgewandelt worden sein können oder
- die Personen evt. Interesse an ihrem Abonnement verloren haben und die Mail als Spam melden

Außerdem sorgt eine effiziente Datenbereinigung dafür, dass Ihre Verteilerliste nicht voller ungültiger E-Mailadressen ist, die wiederum den Zuwachs an Hard Bounces in Kampagnen fördern und dazu beitragen, dass Ihr Spam-Score bei Providern und Spamfiltern steigt.

### Überprüfen Sie inaktive Abonnenten

Inaktive Abonnenten (jene, die ihre Mails über einen bestimmten Zeitraum hinweg nicht öffnen) können auf inaktive Accounts umgestellt werden und werden immer häufiger von Providern als Spam-Fallen genutzt.

Diese ist eine besonders präsente Bedrohung hinsichtlich erworbener oder erneut aktivierter Adressen; eine E-Mailadresse, bei der die Mails über drei Kampagnen hinweg nicht geöffnet oder beantwortet werden, sollte gut überwacht und evt. von der Liste genommen werden, um das Risiko zu mindern, in Spam-Fallen zu landen.

Umgekehrt ist es bei inaktiven E-Mailadressen, deren Inhaber sich für die Zusendung Ihrer Werbe-Mails entschieden haben, unwahrscheinlicher, dass diese kurzfristig in Spam-Fallen umgewandelt werden und in der Regel sollten diese nach 12 Monaten Inaktivität von der Verteilerliste genommen werden.

### E Erfolgreiche E-Mail-Strategien

Die Befolgung des Leitfadens für E-Mail-Strategien von DMA trägt sehr wahrscheinlich zur Verbesserung der Zustellbarkeit und in der Regel zur erfolgreicheren E-Mailkampagnen bei. Die wichtigsten Empfehlungen hinsichtlich Zustellbarkeit sind u.a.:

- Permission – Der Schlüssel zur Zustellbarkeit
- Opt-In/Opt-Out-Strategien
- Datenbereinigung in den Verteilerlisten
- Kommunikation mit Internetprovidern

## Wie Epsilon International helfen kann

Das Epsilon Deliverability Management (EDM) überwacht und bewertet permanent den Ruf des Kunden, um sicherzustellen, dass die Zustellbarkeit seiner E-Mails optimiert wird. Unten sehen Sie eine Auflistung aller Maßnahmen, die durchgeführt werden, um die Zustellbarkeit zu fördern und einen guten Ruf zu pflegen.

### Überwachung von IP-Adressen

Epsilon International überwacht all seine IP-Adressen (Adresspools and Einzeladressen) hinsichtlich Spam-Beschwerden. Die IPs sind bei SpamCop gelistet, die das EDM mit stündlichen Berichten versorgen.

Ebenso wird der Ruf einer E-Mailadresse mithilfe des Sender Score Reputation Tool überwacht. Der Ruf wird gemessen an einer Skala bis 100, dabei stuft Epsilon jedes Ergebnis unter 70 als gefährlich ein. Untersuchungen von Return Path (ihre Q2 2008 Benchmark-Studie) haben gezeigt, dass Server mit einem Sender Score von 72 im Durchschnitt Zustellraten von 87% verzeichnen. Die durchschnittliche Ruf für die Absender-IPs von Epsilon International liegt bei 85-90.

Das hohe Ansehen von Epsilon International führt zu guten Resultaten bei der Zustellung der E-Mails seiner Kunden. Untersuchungen von DREAMmail zeigen, dass seit dem 17.09.2008 E-Mails in EDM-Kampagnen (insgesamt 11 101 448 E-Mails) mit einer Wahrscheinlichkeit von 96% erfolgreich zugestellt wurden. Das ist 8% höher als der Branchendurchschnitt von 88% für Werbe-Mails, so berichtet Return Path.

## Bounce-Analyse

Bei allen Kampagnen wird die Häufigkeit von Hard Bounces streng überwacht. Das EDM erhält eine Meldung, wenn bei einer Kampagne die Häufigkeit der Hard Bounces bei über 15% liegt, so dass eine Untersuchung und gegebenenfalls eine Problembehandlung stattfinden kann.

## Überprüfen von Blacklists

Alle IP-Adressen, die von Epsilon International betrieben werden, werden rund um die Uhr überprüft und mit über 200 Blacklists abgeglichen. Das EDM erhält innerhalb weniger Stunden eine Benachrichtigung, falls eine IP-Adresse auf einer Blacklist erscheint.

## Überwachen des Verhaltens von Providern

Epsilon hat eine Reihe von E-Mailadressen geschaffen, die einzig und allein dem Zweck dienen, die Zustellung von Nachrichten zu analysieren. Jedes Mal, wenn eine Nachricht von DREAMmail versandt wird, werden der Posteingang und der Spamordner jeder E-Mailadresse überwacht, um herauszufinden wie die Provider die Nachricht behandeln. Berichte zu den Zustellkriterien bei diesen Test-Verteilerlisten ist sowohl über DREAMmail selbst (über Delivery Monitoring in der Reports-Schnittstelle) als auch über DREAMmail Delivery Assurance (DDA) verfügbar, ein externes DREAMmail-Tool, das von Epsilons Partnerunternehmen Return Path betrieben wird.

Das DDA überwacht 55 weltweite Provider und ermöglicht so einen kompakten Überblick über die kurz- und langfristige Entwicklung einer Kampagne. Das Mailbox Monitor Tool verwendet eine Technologie, die auf dem Einsatz von Testadressen beruht, bei denen der Status aller E-Mails (im Posteingang, im Spamordner oder auch bei Verlust einer Mail) verfolgt wird. DDA verfügt außerdem über ein Blacklist Alert Tool sowie ein Campaign Preview (Spam Filter Monitor) Tool, mit dem E-Mails anhand eines Spam Assassin Score beobachtet und angepasst werden können.

Das EDM von Epsilon International überwacht täglich die Ergebnisse des DDA. Jede Nachricht, bei der mehr als 5% aller E-Mails verloren gehen, wird untersucht, genauso wie jede Nachricht bei der die Zustellwahrscheinlichkeit in den Posteingang bei unter 90% liegt. Die Verwendung von X-Headern (angepasste Header, durch den Anwendungen kommunizieren können) ist ein gängiges Verfahren, um die Ursachen solcher Probleme zu orten. Je nach Problemlage werden dann die Provider kontaktiert (siehe unten).

## Zusammenarbeit mit Providern

Epsilon International pflegt sehr enge Beziehungen zu Providern:

- Alle Epsilon-IPs sind von den großen Providern freigegeben (einschließlich Hotmail, AOL, Yahoo).
- Epsilon legt großen Wert auf Feedback von großen Providern, das es ermöglicht, die wichtigsten Kriterien für die Zustellung sowie Spam-Beschwerden zu überwachen. Das EDM gibt wöchentlich Informationen über Spam-Beschwerden an das Account Management weiter.
- Epsilon erfüllt alle Anforderungen hinsichtlich der von einzelnen Providern gestatteten Anzahl an Verbindungen oder Nachrichten.
- Epsilon EDM-Vertreter nehmen gemeinsam mit Providern und Vertreibern von Anti-Spam-Programmen an internationalen Konferenzen Teil, wo die Themen Best practice and Delivery erörtert werden und können soden Neuentwicklungen bei Providern, in der Politik und bei den Branchenstandards folgen und ihnen effektiv Rechnung tragen.

## Zusammenarbeit mit Providern (Fortsetzung)

- Wenn nötig, kommuniziert das EDM mit Providern, Blacklists und Vertreibern von Anti-Spam-Programmen, um Probleme bei der E-Mail-Zustellung in den Griff zu bekommen.

## Ablauf für Problembehandlung

Epsilon International hat einen allgemeinen Ablauf für Kundenanfragen hinsichtlich der Problembehandlung bei der Zustellung von E-Mails entwickelt.

Falls der Kunde ein Problem bei der Zustellung entdeckt:

- Der Kunde erstellt ein Ticket über die Support Helpline, das Email Ticketing System oder das Account Management.
- Das Epsilon Support Team wird dann eine erste Prüfung der Anfrage vornehmen und falls möglich, das Problem beheben.
- Wo eine Problembehebung auf Supportebene nicht möglich ist, wird das Problem an das Email Delivery Management (EDM) weitergegeben.
- Nach einer ersten Prüfung des Problems tritt das EDM mit dem Kunden in Kontakt – bezieht sich dabei auf die Ticketnummer – und gibt die Ursache des Problems sowie die einzelnen Schritte zu seiner Behebung von Kundenseite (falls erforderlich) oder durch Epsilon bekannt.

Falls Epsilon ein Problem bei der Zustellung entdeckt:

- Das Epsilon Support Team wird dann eine erste Prüfung des Problems vornehmen und falls möglich, das Problem beheben – der Kunde wird dann per Ticket über die erfolgreiche Problembehandlung informiert.
- Wo eine Problembehebung auf Supportebene nicht möglich ist, wird das Problem an das Email Delivery Management (EDM) weitergegeben.
- Nach einer ersten Prüfung des Problems tritt das EDM mit dem Kunden in Kontakt – bezieht sich dabei auf die Ticketnummer – und gibt die Ursache des Problems sowie die einzelnen Schritte zu seiner Behebung von Kundenseite (falls erforderlich) oder durch Epsilon bekannt.

Prinzenallee 7
40549 Düsseldorf
Deutschland
+ 49 (0) 211 5239 1134
info_de@epsilon.com