

Checkliste: 55 Tipps Spamfilter zu umgehen

1 Problematik

Weltweit sind 64 % aller E-Mails Spam. In Deutschland liegt der Anteil der unerwünschten E-Mail-Werbung bei 47%. Damit ihre Kunden weniger belästigt werden, richten Provider Spamfilter ein, welche einen Großteil unerwünschter Werbung blockieren. Aber wo gehobelt wird fallen Späne: auch angeforderte Newsletter verschwinden in den Klauen der Spamfilter.

In den USA werden 18,7% aller abonnierten Newsletter nicht ausgeliefert. In Deutschland filtern Provider derzeit 10-20% der angeforderten Newsletter zu Unrecht als vermeintliche Spam-Mails heraus. Dabei können Versender einiges dafür tun, damit ihrem Newsletter dieses Schicksal erspart bleibt.

2 Generell

Keine unangeforderten E-Mails versenden

Stellen Sie organisatorisch wie technisch sicher, dass niemand gegen seinen Willen E-Mails von Ihnen zugesandt bekommt? Ihre Sorgfalt beim Vermeiden unangeforderter E-Mails ist für Provider und Spamfilter ein wichtiger Indikator bei der Einschätzung, ob es sich um Spam handelt.

Keinen Anlass zu Beschwerden geben

Sind E-Mails von Ihnen erwartet, wird sich niemand beschweren. Beschwerden sind für Provider der zuverlässigste Indikator bei der Einschätzung, ob es sich um unerwünschte Werbung handelt.

Rückläufer aus dem Verteiler nehmen

Werden die Adressen regelmäßig angeschrieben und die Rückläufer (Bounces) aus dem Verteiler gelöscht, so haben Sie eine niedrige Rücklauferrate. Diese Rücklauferrate ist für Provider und Spamfilter ein wichtiger Indikator bei der Einschätzung, ob es sich um Spam handelt.

Vertrauenswürdiger Mailserver

Wenn über einen Mailserver nur seriöse E-Mails versandt werden, steigt dessen Reputation. Wird gespamt, landet der Mailserver auf schwarzen Listen. Verpflichtet sich der Mailserverbetreiber gegenüber den Providern, selbst gegen Spam vorzugehen, besteht die Chance, auf eine Whitelist zu kommen. Versenden Sie deshalb nur über vertrauenswürdige Mailserver, die eventuell in Whitelists stehen. Ein Zentralregister mit Punktekonto-Auskunft finden Sie unter <http://www.senderbase.org>

3 Versandtechnik

Mailserver sicher konfigurieren

Gibt es bei der Konfiguration des Mailservers eventuell Sicherheitslücken? Ist er gar ein "Open Relay", so dass Spammer darüber ihre E-Mails versenden können?

Sicheres Newsletteranmeldeformular

Gibt es Sicherheitslücken im Newsletteranmeldeformular, so dass man an das Versandsystem herankommt?

E-Mails konform RFC 2822

Produziert das Versandsystem Mails, die den technischen Normen (RFC 2822) und den Regeln für die Gestaltung professioneller E-Mails entsprechen?

Feste IP-Adresse

Wird die E-Mail von einer festen IP-Adresse aus versandt oder hat sich der Versender mit einer dynamischen Einwahlverbindung an das Internet angeschlossen?

Reverse DNS

Hat die IP-Adresse des versendenden Mailservers einen gültigen Domainnamen?

Korrektes Datum

Stellen Sie sicher, dass Ihr Versandsystem das Versanddatum mitliefert und dass dieses korrekt eingestellt ist.

Korrekte Absender- und Reply-Adresse

Sowohl die Absender- wie auch die Reply-Adresse müssen gültig sein. Wechseln Sie die Absenderadresse auch nicht ohne Not, das sie von Empfängern oft in ihre jeweiligen Adressbücher übernommen wird, um providerseitige Spamfilter zu umgehen.

4 Adressen

Nur Opt-In-Adressen mit Einwilligung

Enthält die Adressliste ausschließlich Adressen, von deren Empfängern nachweislich die explizite Einwilligung zum Empfang von E-Mails durch das versendende Unternehmen vorliegt?

Aktuell gepflegte Adressliste

Ist die Adressliste gepflegt? Enthält sie weniger als ein Prozent Bounces (Rückläufer)? Hohe Bouncerate sind ein sicherer Indikator für Spam-Adressen.

Adressen werden regelmäßig angeschrieben

Werden die Adressen regelmäßig (mindestens viermal jährlich) angeschrieben? Beschwerden können auch daher resultieren, dass Empfänger schlichtweg vergessen haben, dass sie sich in einen Verteiler eingetragen haben.

5 Einwilligung

Hinweis auf Widerspruchsrecht bei Einwilligung

Werden die Empfänger beim Einholen der Einwilligung (Online-Anmeldung) auf ihr Widerspruchsrecht (Kündigungs- bzw. Abbestellmöglichkeit) hingewiesen?

Datenschutzhinweis bei Einwilligung

Werden die Empfänger beim Einholen der Einwilligung (Online-Anmeldung) auf die Verwendung ihrer Daten (Datenschutzerklärung) hingewiesen?

Sofortige Bestätigungs-E-Mail nach Einwilligung

Ist sichergestellt, dass sofort nach Einholen der Einwilligung eine Bestätigungs-E-Mail gesendet wird, in der entweder eine weitere Bestätigung gefordert wird (Double Opt-In) oder in der zumindest eine bequeme Widerspruchsmöglichkeit (Abmeldung) besteht (Confirmed Opt-In)?

Confirmed-Opt-In: bequeme Abbestellfunktion in der Bestätigungs-E-Mail

Wird es dem Empfänger leicht gemacht, nach Erhalt der Bestätigungs-E-Mail dem weiteren Bezug von E-Mails zu widersprechen? Standard ist ein anklickbarer Abmeldelink in der E-Mail. Besonders bequem ist es für Nutzer, wenn Sie auf allen Kanälen (Hyperlink, formlose Antwort-Mail, Telefon, Fax) formlos abbestellen können. Umständlicher ist es, wenn erst auf eine Webseite verlinkt wird, auf der dann die nochmalige Eingabe der E-Mail-Adresse erforderlich ist.

6 Abbestellung

Bequeme Abbestellfunktion in jeder E-Mail

Enthält jede versandte E-Mail eine leicht auffindbare und bequem zu nutzende Abmeldemöglichkeit?

Abbestellung bequem mit weniger als zwei Mausklicks

Eine bequeme Abbestellung besteht aus einem Hyperlink, dessen Anklicken das Streichen der E-Mail-Adresse bewirkt. Oft ist noch eine Sicherheitsabfrage vorgeschaltet, um versehentliches Abmelden auszuschließen.

Abbestellung funktioniert auch bei weitergeleiteten E-Mails

Manche Nutzer lassen sich ihre E-Mails an eine andere Adresse weiterleiten. In diesem Fall muss bei einer Abmeldung die ursprünglich registrierte E-Mail-Adresse automatisch erkannt und gelöscht werden.

Abmeldung auch mit formloser E-Mail

Eine Abmeldung sollte auch dann möglich sein, wenn der Empfänger einfach die "Antworten"-Taste drückt und formlos um eine Kündigung seines Newsletterabonnements bittet.

7 Beschwerden

Unternehmen für Beschwerden per eMail erreichbar

Durch gute Erreichbarkeit per E-Mail lassen sich viele Probleme schnell aus dem Weg räumen. Nicht erreichbar zu sein ist eine typische Eigenschaft von Spammern.

Schnelle Reaktion auf Beschwerden

Je schneller Sie auf Beschwerden reagieren, desto geringer die Gefahr ernster Konsequenzen.

Jede E-Mail enthält alle Impressumsangaben

Die wichtigsten Kontaktdaten wie E-Mail, Telefon und Postadresse sollten in jeder E-Mail sein. Ebenso ein Hyperlink auf das komplette Impressum auf der Website.

Funktionierende Reply-Adresse

Die Reply-Adresse muss korrekt eingerichtet sein und darf keine Fehlermeldung produzieren.

Reply-Adresse in Mailings reagiert schnell auf Beschwerden

Die Reply-Adresse sollte über ein funktionierendes Bounce-Management verfügen, damit einzelne Beschwerden nicht in der Masse der Abwesenheitsmeldungen untergehen.

Abgemeldete Adressen sicher aus dem Verteiler streichen

Für Abmeldungen muss es einen zuverlässigen Prozess geben, damit nicht verspätet oder gar überhaupt nicht die Abmeldung realisiert wird. Wie lange dauert es, bis eine abgemeldete Adresse aus dem Verteiler gestrichen wird?

Interne Blacklist

Eine der technisch wichtigsten Forderungen ist eine interne Blacklist, die sicher gewährleistet, dass die darin genannten Adressen niemals auch nur eine einzige E-Mail erhalten. Ist erst einmal eine Unterlassungserklärung unterschrieben, hat der Adressat als Empfänger der Vertragsstrafe ein finanzielles Interesse doch noch eine E-Mail zu erhalten.

8 Gestaltung generell

SpamAssassin-Test

Der einfachste Weg, die eigene E-Mail auf mögliche Spam-Klassifikation zu prüfen, ist der Spam-Assassin-Test. Unter <http://www.lyris.com/contentchecker/> können Sie Ihre Mail testen.

Reizworte in Betreff und Body

Betreffzeilen mit drei Ausrufungszeichen und GROSSBUCHSTABEN sollten Sie vermeiden. Generell sollte auf mehrfache Sonderzeichen verzichtet werden. Bei manchen Filtern kann schon "Gewinnspiel" kritisch sein. Im Hauptteil der E-Mail sind Sie freier, auch hier sollte jedoch auf Super-Super-Schnäppchen oder Viagra verzichtet werden.

Seriöse Absender-Adresse

Absender wie John523467@yahoo.com werden häufiger von Spammern verwendet, als sauber geschriebene Namen wie newsletter@firma.de oder hans.maier@firma.de.

Einfacher HTML-Code

Je einfacher der HTML-Code aufgebaut ist, desto geringer die Gefahr, dass E-Mails defekt ankommen. Gängige HTML-Editoren wie Dreamweaver oder Frontpage sind nicht geeignet, HTML-Code für E-Mails zu erstellen.

Kein Anhang

Auf Anhänge sollte in Serien-E-Mails nach Möglichkeit verzichtet werden. Ausnahme: PDF-Dokumente.

9 Gestaltung bei Eigenversand

Nicht wie Spam aussehen

Je ähnlicher Ihre E-Mail einer typischen Spam-E-Mail ist, desto wahrscheinlicher ist es, dass sie als solche klassifiziert wird. Wenn Sie in Whitelists stehen, gelten diese Gestaltungsregeln nur teilweise. Wenn Sie jedoch von einem eigenen System aus versenden, sollten Sie die folgenden Regeln beherzigen.

Name in die "To"-Zeile

Der komplette Name des Adressaten in der "To"-Zeile sowie in der Anrede ist für manche Filterprogramme ein Kriterium, dass es sich NICHT um Spam handelt. Spam-Versender kennen diese Daten meist nicht.

Betreff ohne Personalisierung

Verzichten Sie auf die responsesteigernde Personalisierung der Betreffzeile, die für einige Spamfilter ein Kriterium sind, DASS es sich um Spam handelt. Spammer "personalisieren" ihre Mails oft durch Einfügen der E-Mail-Adresse in den Betreff.

Betreff ohne Reizworte

Verzichten Sie auf responsesteigernde Begriffe wie kostenlos oder Gewinnspiel in der Betreffzeile. Die Liste der "Unworte" wird ständig länger. Alles was werblich wirkt ist Spamverdächtig. Auch im Textteil der Mail sollten Sie auf werbliche Begriffe wie "Geld-zurück-Garantie" verzichten.

Betreff ohne viele Zahlen

Verzichten Sie auf Zeilen mit vielen Ziffern, Kundennummern oder IDs.

Wenig HTML-Code

Versuchen Sie den Anteil von HTML-Code gegenüber dem reinen Text gering zu halten. Verzichten Sie auf JavaScript und auf Tabellen. Verwenden Sie einen einfachen Editor. Frontpage ist nicht geeignet, Newsletter zu entwerfen.

Multipart statt HTML-Format

Versenden Sie HTML-Mails immer im Multipart-Format und nie als reine HTML-Mails.

Große Überschriften

Verzichten Sie auf große, farbige Überschriften und vermeiden Sie Farben.

Farben vermeiden

Verzichten Sie auf farbige Schrift. Rot grün und Blau sollten Sie meiden. Grau Gelb, Cyan oder Magenta sind absolut tabu. Der Hintergrund sollte am besten weiß sein.

Wenig Bilder

Je weniger Bilder, desto besser. Große Bilder und ein hoher Anteil von Bildern gegenüber Text sind zu vermeiden.

Links mit Domainnamen

Hyperlinks in Ihrer E-Mail sollten immer auf existierende Domainnamen verweisen und nicht auf IP-Adressen. Auch sollte der Link nicht in JavaScript versteckt sein.

Weitere Tricks

Eine Reihe von Spamfilterregeln gehen hart an die Grenzen seriösen E-Mail-Marketings. So ahnden es manche Spamfilter, wenn Sie beschreiben wie die Adresse gewonnen wurde. Genau dies ist jedoch eine Forderung seriösen E-Mail-Marketings. Gleiches gilt für den Abmeldelink, der bequem mit einem Mausklick abmeldet. Eine Abmeldung wird sogar vom Gesetzgeber verlangt. Auch das User-Tracking, bei dem gemessen wird, welche Themen bei welchen Zielgruppen am besten ankommen, kann für Spamverdacht sorgen.

10 Dienstleister

Freistellungserklärung des Dienstleisters

Wie sieht der Vertrag zwischen versendendem Unternehmen und E-Mail-Dienstleister aus? Wenn Sie ohne Vertragsstrafe spammen können, können andere Kunden dieses Anbieters das auch . Sie sind dann eventuell in schlechter Gesellschaft.

Ausschluss zweifelhafter Adressen

Verpflichtet sich das versendende Unternehmen gegenüber dem E-Mail-Dienstleister dazu, nur an Adressen zu versenden, von deren Empfängern nachweislich die explizite Einwilligung zum Empfang von E-Mails durch das versendende Unternehmen vorliegt?

ISP-Relations

Zu welchen Internet-Service-Providern (ISP) unterhält der Dienstleister welche Beziehung? Kennt er die jeweiligen Spamfilter-Verantwortlichen? Bestehen nur Beziehungen zu Anbietern öffentlicher E-Mail-Adressen (GMX, Web.de, T-Online, AOL) oder auch zu Internet-Providern, die Firmen-Mailserver an ihr Backbone-Netz anschließen.

Whitelist

Bei welchen ISPs ist der Dienstleister auf der Whitelist (Allow List)? Manche Provider haben mehr als eine Whitelist - z.B. AOL mit seiner enhanced Whitelist.

Monitoring Postfach

Bei welchen Providern überwacht der Dienstleister mit eigenen Postfächern kontinuierlich die Auslieferung von Serien-E-Mails?

Monitoring Öffnungsrate

Überwacht der Dienstleister kontinuierlich die Öffnungsraten bei den unterschiedlichen Providern?

Monitoring Rückläufer

Überwacht der Dienstleister kontinuierlich die Rückläufer (Bounces) bei den unterschiedlichen Providern? Kann zwischen normalen Hard- und Softbounces sowie blockierten E-Mails unterschieden werden?

Reporting

Erhält der Kunde für jedes Mailing eine nach Providern gestaffelte Übersicht über die Auslieferung des Mailings im Vergleich zu den insgesamt vom Dienstleister an diesen Provider ausgelieferten Mails?

Monitoring Blacklist

Überwacht der Dienstleister kontinuierlich relevante Blacklists? Welche Blacklists werden wie oft geprüft?

Zweitversand blockierter E-Mails

Besteht die Möglichkeit, blockierte E-Mails noch einmal auszuliefern?

Providerspezifische HTML-Versionen

Manche Provider filtern aus HTML-Mail Bilder oder Hyperlinks. Die ersten Dienstleister beginnen nun E-Mails providerspezifisch anzupassen.