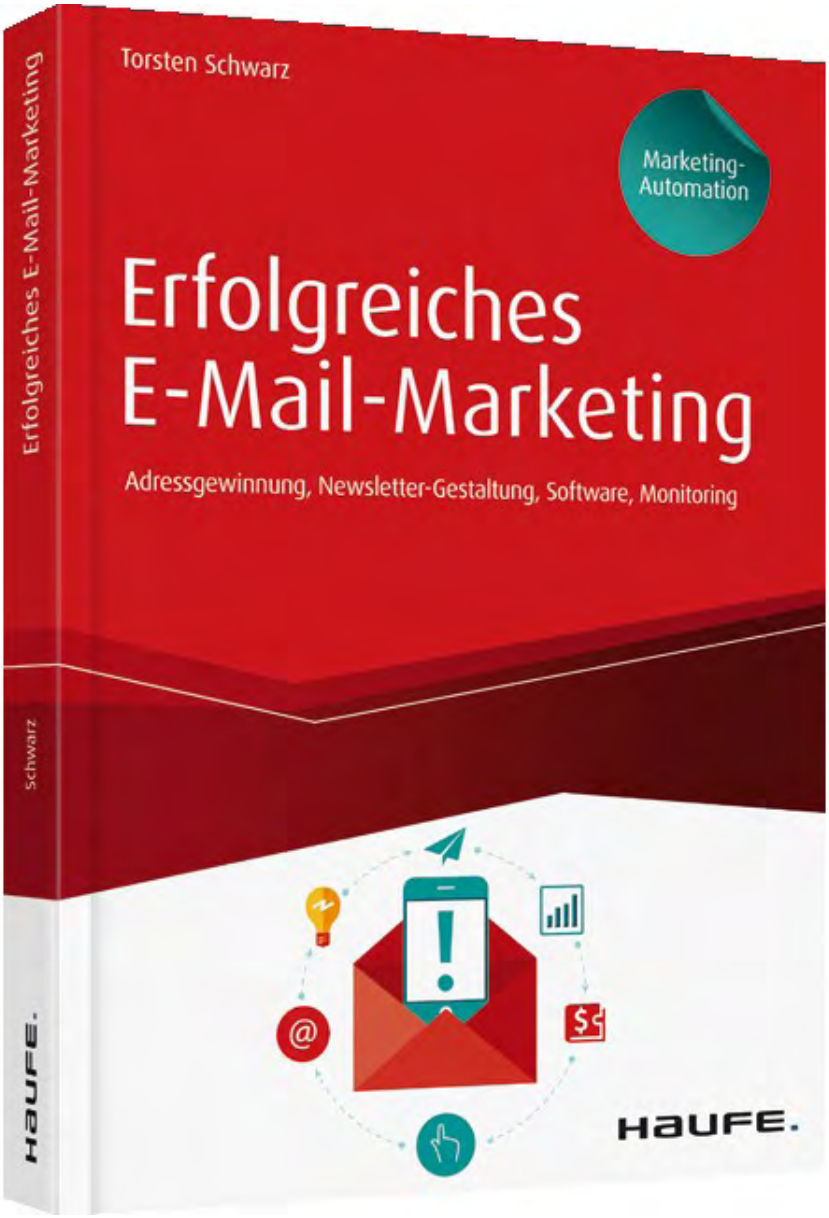
Kostenloser Download:

Die wichtigsten Kennzahlen im E-Mail-Marketing

Das PDF stammt aus dem Buch



12 Den E-Mail-Versand optimieren

12.1 Die wichtigsten Kennzahlen im E-Mail-Marketing

Verteilergröße (Versandmenge), Öffnungs- und Klickrate sowie Bounce- und Abmelderate sind die Standardwerte im E-Mail-Marketing. Leider liefern die Systeme oft ganz unterschiedliche Kennzahlen. Entweder werden Äpfel mit Birnen verglichen oder der Wert kann überhaupt nicht gemessen werden. Hier sind die häufigsten Fehlerquellen.

1. Die Versandmenge – Dubletten dürfen nicht sein
Schon bei einer elementaren Zahl geraten manche Systeme ins Straucheln. Bei postalischen Mailings stellen Adressdubletten ein erhebliches Problem dar. Hier lebt der E-Mail-Marketer sorgenfrei. Der Grund: Anders als bei Postadressen gibt es bei E-Mails nur *eine* richtige Schreibweise – alles andere produziert Rückläufer (Bounces). Jedes professionelle E-Mail-Versandsystem entfernt automatisch doppelte E-Mail-Adressen. Falls Sie kein solches System verwenden, entfernen Sie die Dubletten manuell.

2. Die Bounce-Rate – Nicht jedes System arbeitet fehlerfrei
In der Praxis laufen bei der Rückläuferbearbeitung manchmal zwei Dinge falsch. Entweder das Bounce-Management funktioniert gar nicht, dann werden munter jedes Mal alle toten Adressen wieder angeschrieben. Nach einem Jahr schon kann so der halbe Verteiler aus toten Adressen bestehen. Es gibt aber auch das Gegenteil. Dann wird jede Rückläufermail als Bounce gewertet und fliegt aus dem Verteiler. Die meisten Rückläufer jedoch sind einfache Abwesenheitsnotizen und damit Softbounces. Softbounces werden weiter angeschrieben. Zwischen diesen beiden Extremen gibt es viel Raum für Optimierung. Die meisten professionellen Systeme beherrschen hier alle Tricks, um den Verteiler möglichst optimal zu pflegen.

3. Die Öffnungsrate liegt in Wahrheit meist höher
Um es vorweg zu sagen: Die Öffnungsrate kann nicht gemessen, sondern nur geschätzt werden. Das geschieht mit eingebauten Bildern, die beim Öffnen der E-Mail nachgeladen werden. Und genau das ist die Crux. Denn oft werden die Bilder nicht nachgeladen. Sei es die neue Outlook-Version oder der sicherheitsfanatische Webmaster, Bilder werden oft geblockt. Dafür zählen viele Systeme gleich mehrfach. Wenn von zwei Empfängern einer gar nicht und einer zweimal öffnet, entsteht eine Öffnungsrate von 100%. Im Zweifelsfall fragen Sie nach, ob auch wirklich die »Öffnungsrate unique« gemessen wurde. Das ist der Anteil der Empfänger, die vermeintlich geöffnet haben. In

Textmails kann die Öffnungsrate nicht gemessen werden. Dafür lässt sie sich jedoch anhand der Klickrate abschätzen. Und schon wieder schnappt die Falle der unterschiedlichen Erhebungsmethoden zu.

4. Die Klickrate – Unser bester Wert

Anders als die Öffnungsrate kann die Klickrate sehr genau gemessen werden. Aber auch hier liefern die Systeme unterschiedliche Werte: Besonders aussagekräftig ist die »Klickrate unique«. Dabei wird gemessen, wie viele der Empfänger tatsächlich etwas angeklickt haben. Manche Systeme messen jedoch jeden Klick. Wenn also jemand zwei unterschiedliche Links jeweils dreimal angeklickt hat, treiben diese sechs Klicks die Klickrate hoch, obwohl dahinter nur eine einzige Person steckt. Professionelle Systeme erfassen all diese Werte getrennt. Aber selbst wenn Sie nun mit der »Klickrate unique« als Erfolgskennzahl arbeiten, sollten Sie aufpassen. Vergleichen Sie sich nie mit anderen Unternehmen, denn es spielen zwei wichtige Faktoren eine Rolle: Wie alt ist Ihr Verteiler? Wer seit zehn Jahren E-Mails versendet, hat zwangsläufig eine niedrigere Klickrate als ein Unternehmen, das gerade einen neuen Verteiler aufgesetzt hat. Wie wichtig sind Sie für den Empfänger? Je höher die Relevanz Ihrer Inhalte für den Empfänger ist, desto höher auch die Klickrate. Das ist auch der Grund dafür, dass im B2B-Bereich die Klickraten meist höher sind als bei E-Mails, die sich an Verbraucher richten.

5. Die Abmelderate – Zufriedenheit wird messbar

Die Abmelderate ist ebenfalls ein relativ präzise zu ermittelnder Wert. Auch hier jedoch sollte man sich vor Vergleichen mit anderen hüten, weil zu viele Faktoren eine Rolle spielen. Wie bequem ist die Abmeldung? Wer gehen will, geht. Bauen Sie also keine Hürden auf, sondern platzieren Sie das Wort »Abmelden« am besten nicht nur am Ende, sondern auch am Anfang einer E-Mail. Die Abmeldung sollte am besten ganz bequem mit einem einzigen Mausklick möglich sein, ohne noch einmal die Adresse eingeben zu müssen. Der Grund: Je einfacher das Abmelden, desto weniger Menschen drücken stattdessen den Spamknopf. Solche Beschwerden sind schlecht für Ihre Absenderreputation, die von den E-Mail-Providern sehr genau gemessen wird. Je besser Ihr Ruf, desto geringer das Risiko, von Spamfiltern blockiert zu werden. Weil inzwischen immer mehr Anbieter eine Abmeldung mit nur einem Klick ermöglichen, ändert sich das Nutzerverhalten. Empfänger erwarten, dass sie mit dem Anklicken des Abmelde-Buttons automatisch vom Verteiler gestrichen werden. Wenn jedoch noch ein weiterer Klick nötig ist, wird das häufig übersehen. Die Folge: Nutzer bleiben im Verteiler, obwohl sie raus wollten. Kommt die nächste E-Mail, sind sie verärgert und drücken den Spamknopf, weil sie glauben, dass die Abmeldung defekt sei.

6. Die effektive Klickrate ist sofort messbar
Versandmenge, Öffnungs- und Klickrate sowie Bounce- und Abmelderate sind die Standardwerte. Darüber hinaus gibt es eine Vielzahl von Werten, die man messen kann, aber nicht unbedingt muss. Praktisch ist vielleicht noch die effektive Klickrate (Click-to-Open-Rate). Das ist der Anteil der Öffner, die geklickt haben. Gegenüber der Klickrate hat der Wert den Vorteil, dass er sofort nach dem Versand schon eine grobe Orientierung darüber gibt, ob das Mailing voll in die Hose gegangen ist oder der Sekt kaltgestellt werden sollte. Der Grund ist einfach: Die Klickrate steigt auch noch am nächsten Tag, wenn diejenigen klicken, die gestern nicht da waren. Am Montag kommen noch einmal einige aus dem Urlaub und erst dann sind die Werte einigermaßen konstant. Dies gilt jedenfalls bei nicht täglich verschickten E-Mails. Daher ist die Klickrate ein Wert, der immer in Bezug zur Zeitspanne gesetzt werden muss, die seit dem Mailing vergangen ist. Aus dem Dilemma kommt man heraus, wenn man zwei solche zeitabhängigen Variablen durcheinander teilt, nämlich die Klick- durch die Öffnungsrate.

7. Lesedauer – einfach messbar, aber wenig aussagekräftig
Die Lesedauer lässt sich anhand der Differenz zwischen dem Öffnen und Klicken messen. Sobald jemand den Newsletter öffnet, registriert das Ihr Zählpixel, das die Öffnungsrate misst. Wenn dann jemand etwas anklickt, wird das von dem codierten Hyperlink erfasst, der alle Klicks auswertet. Die Zeit, die dazwischen vergangen ist, ist die Lesezeit der E-Mail. Ist es nun schlecht, wenn jemand schnell auf Ihren CTA-Button klickt? Oder ist es wirklich gut, wenn jemand ausgiebig Ihre interessante E-Mail liest, bevor er sich dann endlich zu einer Handlung (Klicken) entschließen kann? Es liegt an Ihnen, Ihre Ziele sinnvoll zu definieren.

8. Konversionsrate misst den Erfolg einer Kampagne
Die Stärke von E-Mail-Marketing ist es zweifellos, Menschen zu Handlungen zu bewegen. Das Medium macht es leicht, denn ein Mausklick ist nicht anstrengend. Die Konversionsrate misst beispielsweise den Anteil der Leser, die eine Umfrage auch bis zum Ende ausfüllen. Oder Käufer, die nicht nur etwas in den Warenkorb legen, sondern auch sofort bezahlen. Den Wert können Sie messen, wenn Sie E-Mails und die Website mit einem gemeinsamen Trackingsystem verbinden. Sobald jemand den Newsletter öffnet, registriert dies Ihr Zählpixel, das die Öffnungsrate misst. Wenn dann jemand etwas anklickt, registriert die Website den Besuch der Landingpage. Und diese wiederum misst, wie viele Menschen auch bis zum Check-out kommen.

12.2 So erhöhen Sie die Zustellbarkeit

Trotz Einwilligung werden auch viele seriöse E-Mails von Spamfiltern blockiert. Professionelle E-Mail-Service-Provider (ESP) lassen daher ihre Mailserver von der Certified Senders Alliance (CSA) zertifizieren. Die CSA ist eine gemeinsame Initiative des Providerverbandes eco und des Direktmarketingverbandes DDV. Die Direktmarketer schließen mit den ESPs (E-Mail-Service-Provider) einen Vertrag, in dem sie zusichern, dass sie von allen Empfängern ein Opt-in haben. Die ESPs wiederum garantieren den Providern, dass E-Mails von Ihren Systemen ausschließlich an Empfänger mit nachweisbarer Einwilligung gehen. Dafür setzen die Provider diese ESPs auf eine Whitelist. Das heißt, dass deren E-Mails nicht vom Spamfilter geprüft werden. Allein mit einem CSA-zertifizierten Versender ist es aber nicht getan. Damit die eigenen E-Mails beim Empfänger und nicht im Spamfilter landen, ist Eigenarbeit gefordert. Die wichtigsten Kriterien werden hier kurz erläutert.

1. Keine Beschwerden provozieren
Man kann es nicht oft genug betonen: Auch wenn Sie juristisch wie technisch alles perfekt machen, gibt es trotzdem eine Schwachstelle. Wenn die Empfänger Ihre E-Mails als lästig empfinden, drücken sie den Spamknopf. Und wenn das mehr sind als bei anderen Versendern, dann haben Sie ein Zustellungsproblem. Der Anteil der Menschen, die sich trotz rechtlich korrekter Einwilligung beschweren, ist ein Kriterium für die automatisierte Spamerkennung.

2. Klare Einwilligung verhindert Beschwerden
Die Form der Einwilligung muss transparent sein. Sagen Sie dem Nutzer, was er in welcher Frequenz per E-Mail erhält. Werden die Empfänger beim Einholen der Einwilligung (Online-Anmeldung) auf ihr Widerspruchsrecht (Kündigungs- bzw. Abbestellmöglichkeit) hingewiesen? Werden die Empfänger beim Einholen der Einwilligung (Online-Anmeldung) auf die Verwendung ihrer Daten (Datenschutzerklärung) hingewiesen? Ist sichergestellt, dass sofort nach Einholen der Einwilligung eine Bestätigungsmail 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)? Wird es dem Empfänger leicht gemacht, nach Erhalt der Bestätigungsmail dem weiteren Bezug von E-Mails zu widersprechen? Standard ist ein anklickbarer Abmeldelink in der E-Mail. Die Abbestellung sollte aber auch möglich sein, indem die E-Mail einfach mit dem Vermerk »abbestellen« zurückgeschickt wird. 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 Website verlinkt wird, auf der dann die nochmalige Eingabe der E-Mail-Adresse erforderlich ist.

3. Einfache Abbestellung
Die bequeme Abbestellfunktion in jeder E-Mail verhindert Beschwerden. Enthält jede versandte E-Mail eine leicht auffindbare und bequem zu nutzende Abmeldemöglichkeit? Eine bequeme Abbestellung besteht aus einem Hyperlink, dessen Anklicken das Entfernen der E-Mail-Adresse bewirkt. Oft ist noch eine Sicherheitsabfrage vorgeschaltet, um versehentliches Abmelden auszuschließen. 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. Eine Abmeldung sollte auch dann möglich sein, wenn der Empfänger einfach die »Antworten«-Taste drückt und formlos um eine Kündigung seines Newsletter-Abonnements bittet.

4. Beschwerdemanagement
Ihr Unternehmen muss für Beschwerden per E-Mail erreichbar sein. 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. Je schneller Sie auf Beschwerden reagieren, desto geringer die Gefahr ernster Konsequenzen. 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. Die Reply-Adresse muss korrekt eingerichtet sein und darf keine Fehlermeldung produzieren. Die Reply-Adresse sollte über ein funktionierendes Bounce-Management verfügen, damit einzelne Beschwerden nicht in der Masse der Abwesenheitsmeldungen untergehen. Für Abmeldungen muss es einen zuverlässigen Prozess geben, damit die Abmeldung nicht verspätet oder überhaupt nicht realisiert wird. Wie lange dauert es, bis eine abgemeldete Adresse aus dem Verteiler gestrichen wird? 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.

Zertifizierte Server und Reputationsdienste
Der einfachste Weg, Spammails zu erkennen, ist die Identifikation ihrer Herkunft. Wer heute Massenmails verschicken will, muss vorher den Internet Service Providern (ISP) klarmachen, dass diese E-Mails seriös sind. Die ISP nutzen als Erkennungsmerkmal die IP-Adresse des Mailservers. Entweder, Sie nehmen nun selbst zu jedem ISP Kontakt auf oder Sie lassen Dienstleister dies tun. Die Dienstleister sind E-Mail-Service Provider (ESP), die sich auf den Massenversand von E-Mails spezialisiert haben. Es gibt aber auch Anbieter wie Returnpath, die nicht selbst versenden, sondern sich nur auf das Reputationsmanagement ihrer Kunden konzentrieren.

Versender, die in der Certified Senders Alliance (CSA) sind

Die meisten deutschen Unternehmen arbeiten mit ESPs zusammen, deren Mailserver von der CSA zertifiziert sind. Sie schließen einen Vertrag mit dem ESP ab, in dem Sie sich verpflichten, nur an E-Mail-Adressen mit nachweisbarer Einwilligung zu versenden. Wenn es viele Beschwerden gibt, meldet sich die CSA beim ESP. Dieser wird von Ihnen dann eine Erklärung verlangen. Die CSA garantiert den ISPs damit, dass keine Spammails verschickt werden. Die CSA betreibt eine Whitelist zertifizierter Versender, deren E-Mails am Spamfilter vorbei direkt in die Mailboxen zugestellt werden.

Absender-Authentifizierung durch Reverse-DNS Lookup

Die IP-Adresse in einer E-Mail ist fälschungssicher, denn irgendwoher muss die E-Mail ja kommen. Meist nutzen Sie mit anderen Kunden des ESP eine gemeinsame IP-Adresse. Sie können aber auch eine eigene IP-Adresse nur für Ihr Unternehmen erhalten. Dann können Sie sich Ihre eigene Reputation erarbeiten. In jedem Fall sollte von außen offenkundig sein, zu wem die Adresse gehört. Dazu dient der Reverse DNS Lookup (rDNS). Der dabei ermittelte Domainname muss exakt mit der Domain übereinstimmen, die der versendende Mailserver im SMTP-Dialog (E-Mail-Versand) im HELO-Kommando (Begrüßungsdialog der Server) übermittelt.

SPF verhindert den Missbrauch Ihrer Absenderdomain

Sender Policy Framework (SPF) ist ein Verfahren, mit dem das Fälschen der Absenderadresse einer E-Mail verhindert wird. Im SPF trägt der Inhaber einer Domain in das System ein, welche Computer zum Versand von E-Mails für diese Domain berechtigt sind. Hier tragen Sie die genaue Domain vom Versandserver Ihres E-Mail-Versenders (ESP) bei Ihrem Hosting- oder Domaindienstleister im DNS-Eintrag ein. Es reicht also nicht die Hauptdomain (versender.de), sondern es muss der konkrete Versandserver sein (mail3.versender.de). Zu den bekanntesten Unterstützern von SPF gehören GMX, Microsoft (Hotmail und Outlook.com), Arcor, AOL, Gmail, Yahoo und Web.de.

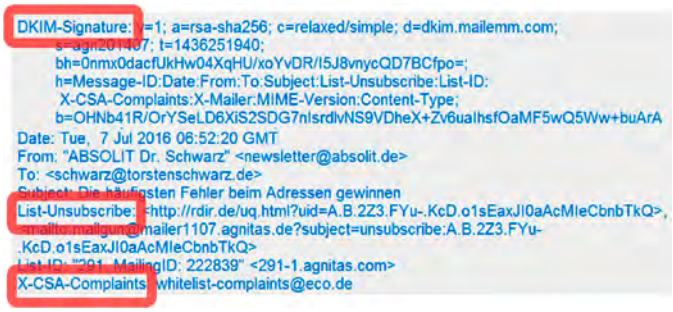


Abb. 12.1: Header einer E-Mail mit den Seriositätsmerkmalen DKIM, List-unsubscribe und CSA-Complaints [Screenshot]

DKIM stellt Authentizität her
DomainKeys Identified Mail (DKIM) ist ein Identifikationsprotokoll zur Sicherstellung der Authentizität von E-Mail-Absendern. Es wurde entwickelt, um den Zugang von unerwünschten E-Mails wie Spam oder Phishing einzudämmen. Neben SPF ist es das meistgenutzte Verfahren zur Sender-Authentifizierung. Im Gegensatz zu SPF funktioniert die Authentifizierung über ein kryptografisches Verfahren. Dazu wird in den Header der versendeten E-Mail ein Hashwert als DKIM-Signatur eingefügt. Der empfangende Mailserver vergleicht diesen Wert mit einem öffentlich hinterlegten Schlüssel.

DMARC verbindet SPF und DKIM
Domain-based Message Authentication, Reporting and Conformance (DMARC) ist eine Spezifikation, die entwickelt wurde, um Missbrauch von E-Mails zu reduzieren. Dabei definieren und hinterlegen Sie Regeln, wie im Fall von Missbrauch Ihrer Domain durch Spammer mit solchen E-Mails zu verfahren ist.

List-Unsubscribe vermeidet Beschwerden
Je bequemer die Abmeldung ist, desto weniger Beschwerden gibt es. Wenn im Header der E-Mail ein sogenannter List-Unsubscribe-Link enthalten ist, macht dies das Abmelden für viele leichter. Der Grund: Manche ISPs, wie zum Beispiel Google (Gmail), lesen den List-Unsubscribe-Link automatisch aus und nutzen ihn für Abmeldelinks oder Abmelde-Buttons im Webmail-Interface.

CSA-Complaints kanalisiert Beschwerden
Wenn im Header einer E-Mail ein X-CSA-Complaints-Hinweis steht, kann dies eine einfache Beschwerdemöglichkeit für E-Mail-Empfänger bedeuten. Damit verringert sich die Chance, dass jemand, der sich beschweren will, einfach auf den Spam-Knopf drückt und die Reputation des Empfängers leidet. Damit kann sich der Empfänger eines CSA-zertifizierten Absenders mit seiner Beschwerde direkt an die CSA und damit an den Verband der deutschen Internetwirtschaft e.V. (eco) wenden.

12.3 Spamfilter umgehen – 7 wirkungsvolle Tricks

Über 90% der weltweit verschickten E-Mails sind Spam. Spamfilter schützen die Inhaber von E-Mail-Adressen vor solchen unerwünschten Nachrichten. Von 100 gesendeten Nachrichten sortieren E-Mail-Anbieter derzeit 80 als offensichtliche Werbemails aus. Von den 20 verbleibenden sind immer noch 15 unerwünscht. Davon betroffen sind jedoch auch seriöse Newsletter. Nur 80% der angeforderten Newsletter werden korrekt ausgeliefert. Der Grund: Die Spamfilter klassifizieren jede Serienmail pauschal als Werbemüll. Dabei gibt es

ein paar einfache Wege, den Spamfiltern klarzumachen, dass es sich um einen explizit bestellten Newsletter handelt.

1. Zertifizierte Versandserver
Der einfachste Weg, seriöse Serienmails zu erkennen, ist die IP-Adresse des Versandservers. Steht dieser auf der Liste der registrierten und zertifizierten Versender legaler Massenmails, muss die Mail nicht von dem relativ unscharf arbeitenden Spamfilter geprüft werden. Newsletter von zertifizierten Versendern werden am Spamfilter vorbei direkt ausgeliefert. Da die Zertifizierung jedoch aufwendig ist, arbeiten die meisten Unternehmen über die zertifizierten Server von Dienstleistern. Auf https://certified-senders.eu/participants finden Sie eine Liste der von der Certified Senders Alliance CSA zertifizierten Unternehmen.

2. Keine Beschwerden
Der zweitbeste Weg, Spam zu identifizieren, ist der Anteil der Beschwerden. Die großen E-Mail-Anbieter haben einen Knopf, über den Spambeschwerden direkt an den Anbieter gehen. Normale E-Mail-Verteiler produzieren nur ganz wenige Beschwerden. Wenn jedoch zum Beispiel Ihre Abmeldefunktion zu umständlich oder schwer auffindbar ist, kommt es zu Beschwerden. Der Grund: Statt den Newsletter direkt abzubestellen, wird stattdessen der Spamknopf gedrückt.

3. Absender ins Adressbuch eintragen
Der sicherste Weg, die Zustellung zu garantieren, ist ein Eintrag ins eigene Adressbuch. Daher sollten Sie Ihre Nutzer schon in der Begrüßungsmail nach der Registrierung auffordern, die Absenderadresse Ihres Newsletters ins Adressbuch zu übernehmen.

4. Vorher einen Spamtest machen
Vor dem Versand sollten Sie einen Spamcheck durchführen. Dabei wird die E-Mail an eine definierte Adresse gesendet, die dann einen automatisierten Test durchführt. Im Anschluss erhalten Sie eine Übersicht über Verbesserungsmöglichkeiten. So können zum Beispiel große Überschriften und knallige Farben dazu führen, dass Spamverdacht geweckt wird. Fast alle E-Mail-Dienstleister bieten einen solchen Test an.

5. Betreff nicht zu werblich formulieren
Die Betreffzeile gehört neben Absender und Textkörper zu den wichtigsten Bereichen. Zwar arbeiten die wenigsten Spamfilter heute nur noch mit Schlüsselworten, trotzdem sollten Sie auf Begriffe wie »Viagra« im Betreff besser verzichten. Generell haben langfristig die weniger marktschreierischen Texte die besseren Öffnungsraten.

6. Gepflegte Liste
Wer mit einem mangelhaften Bounce-Filter arbeitet, hat schlechte Karten. Rückläufer sind für Provider ein wichtiger Indikator für Spamlisten. Entfernen Sie also ungültige Adressen möglichst schnell aus Ihrem Verteiler.

7. Sauberes HTML
Ein letztes Spamkriterium ist schlechtes HTML. E-Mail-Marketing hat in Bezug auf HTML einige Besonderheiten und selbst seriöse Versender verzweifeln da oft. Erst recht die Spammer: Spammails sind meist recht schnell erstellt und entsprechend strotzen sie nicht nur vor Rechtschreib-, sondern auch Programmierfehlern. Diese werden von Spamfiltern erkannt und dienen der Indizierung. Auch sollten Sie in URLs auf IP-Adressen verzichten und in den Links stattdessen immer den Domainnamen nennen.

Schlüsselworte, auf die ein Junk-Filter reagiert
Die folgende Liste enthält typische Schlüsselwörter, auf die zum Beispiel der Junk-E-Mail-Filter von Microsoft reagiert:

- Die ersten acht Zeichen in der Absenderzeile der E-Mail sind Ziffern.
- Betreff mit »Werbung«
- Textkörper mit »Geld zurück«
- Textkörper mit »Karten akzeptiert«
- Textkörper mit »Anweisungen zum Entfernen«
- Textkörper mit »Extraeinkommen«
- Betreff mit »!« *und* Betreff mit »$«
- Betreff mit »!« *und* Betreff mit »kostenlos«
- Textkörper mit ».000« *und* Textkörper mit »!!« *und* Textkörper mit »$«
- Textkörper mit »Lieber Freund«
- Textkörper mit »kostenlos?«
- Textkörper mit »kostenlos!«
- Textkörper mit »Garantie« *und* Textkörper mit »Zufriedenheit« *oder* Textkörper mit »absolut«
- Textkörper mit »Weitere Informationen« *und* Textkörper mit »besuchen« *und* Textkörper mit »$«
- Textkörper mit »WERBEAKTION«
- Textkörper mit »einmalige Mail«
- Betreff mit »$$«
- Textkörper mit »bestellen Sie heute«
- Textkörper mit »bestellen Sie jetzt!«
- Textkörper mit »Geld-zurück-Garantie«
- Textkörper mit »100% zufrieden«
- Die Adresszeile der E-Mail enthält einen der folgenden Ausdrücke: »Freund@« *oder* »öffentlich@« *oder* »Erfolg@«

- Die Absenderzeile der E-Mail enthält einen der folgenden Ausdrücke: »Vertrieb@«, »Erfolg.«, »Erfolg@«, »mail@«, »@öffentlich«, »@savvy«, »Profit@«, »hallo@«
- Textkörper mit »mlm«
- Textkörper mit »@mlm«
- Textkörper mit »////////////////«
- Textkörper mit »per Scheck oder Überweisung«

Filter für nicht jugendfreien Inhalt

- Betreff mit »xxx«
- Betreff mit »über 18«
- Betreff mit »über 21«
- Betreff mit »Erwachsene«
- Betreff mit »Nur für Erwachsene«
- Betreff mit »ab 18«
- Betreff mit »18+«
- Textkörper mit »über 18«
- Textkörper mit »über 21«
- Textkörper mit »müssen 18 sein«
- Textkörper mit »Nur für Erwachsene«
- Textkörper mit »Web für Erwachsene«
- Textkörper mit »müssen 21 sein«
- Textkörper mit »Erwachsene«
- Textkörper mit »18+«
- Betreff mit »erotisch«
- Betreff mit »Erwachsene«
- Betreff mit »Sex«
- Textkörper mit »xxx«
- Textkörper mit »xxx!«
- Betreff mit »kostenlos« *und* Betreff mit »erwachsen«
- Betreff mit »kostenlos« *und* Betreff mit »Sex«

Checkliste für seriöse E-Mails

Damit E-Mails geöffnet und angeklickt werden, müssen sie als seriös wahrgenommen werden. Unseriöse E-Mails laufen Gefahr, von den Nutzern als Spam markiert zu werden, obwohl eine Einwilligung vorliegt. Jede solche Beschwerde geht zulasten der Reputation des Absenders und erhöht damit das Risiko, von Spamfiltern blockiert zu werden. Versender von Serienmails an mehrere tausend Empfänger sollten die Seriosität ihrer Nachricht durch folgende Maßnahmen sicherstellen:

Checkliste: So sichern Sie die Seriosität Ihrer Nachricht

1.	Garantieren Sie, dass der Absender authentisch ist.	In einem SPF-Eintrag (Sender Policy Framework) wird klar definiert, welche Mailserver berechtigt sind, E-Mails im Namen des Unternehmens zu versenden. Domainmissbrauch wird damit verhindert.
2.	Verhindern Sie, dass E-Mails gefälscht werden.	DKIM (Domain Keys Identified Mail) wirkt wie eine digitale Signatur. E-Mails von gefälschten Absendern können damit eindeutig erkannt werden.
3.	Nennen Sie das Absender-Unternehmen klar.	Serienmails sollten im Absenderfeld immer den Unternehmensnamen nennen. Wenn dort Privatnamen stehen sollen, dann sollte mindestens dahinter der Firmenname gesetzt werden: Martin Müller – Lufthansa.
4.	Geben Sie das vollständige Impressum an (kein Link).	Das vollständige Impressum sollte in der E-Mail enthalten sein. Das ist ein offensichtlicher Unterschied zu Spammails, die keine klare Anbieterkennzeichnung enthalten.
5.	Nennen Sie die E-Mail-Adresse des Adressaten.	Um bei Weiterleitungen Missverständnisse zu vermeiden, sollte die ursprüngliche Adresse, an die eine E-Mail geschickt wurde, genannt werden.
6.	Geben Sie nähere Informationen zur Einwilligung.	Wenn möglich, sollten in der E-Mail Informationen zu Datum und Form der Einwilligung geliefert werden. Beispiel: »Sie haben uns am 10.10.2016 auf der Seite www.eco.de/onlinemarketing die Einwilligung erteilt …«
7.	Bestätigen Sie Einwilligungen sofort.	Versenden Sie bei einer Einwilligung sofort eine Bestätigung, in der noch einmal der Text der Einwilligung wiederholt wird. Damit wird der Inhalt der Einwilligung dem Empfänger zugänglich gemacht. Um die Identität des Empfängers zu überprüfen, muss die Einwilligungsmail ein zweites Mal bestätigt werden (Double-Opt-in).
8.	DOI-Mails dürfen keine Werbung enthalten.	Die Double-Opt-in-Mail, mit der die Identität des Empfängers geprüft wird, darf keine Werbung enthalten.
9.	Richten Sie in jeder E-Mail einen Abbestell-Link ein.	Jede E-Mail sollte einen Link enthalten, über den sich Empfänger bequem und ohne Hürden per Mausklick abmelden können.