Mailculture®

Kultiviertes E-Mail-Marketing

So kommen Deine E-Mails sicher an.

Checkliste zur Zustellbarkeit im E-Mail-Marketing

Einleitung

Die E-Mail-Zustellbarkeit ist der zweite Schritt im E-Mail-Marketing-Trichter, direkt nach „Gesendet“ und bezieht sich auf den Prozentsatz der von Dir gesendeten E-Mails, die tatsächlich im Posteingang Deiner Zielgruppe ankommen.

Das heißt, wenn eine E-Mail-Kampagne nicht an Deine Abonnent*innen geliefert wird, kann diese E-Mail nicht geöffnet oder angeklickt werden, und es kann definitiv nicht funktionieren, sie in zahlende Kunden zu konvertieren.

In gewisser Weise ist die Zustellbarkeit also eine der wichtigsten Phasen Deiner E-Mail-Marketingkampagnen. Wenn Deine E-Mail-Zustellrate schlecht ist, erhalten Deine Abonnent*innen nicht einmal Deine E-Mails! Du solltest sie im Blick behalten und versuchen, sie zu verbessern, wenn sie nicht zufriedenstellend ist.

Aufgrund von steigendem Spam-Aufkommen reicht es zudem nicht mehr nur aus, sich vor Missbrauch zu schützen. Vielmehr musst Du als Versender*in selbst aktiv werden und Deine eigene Reputation stärken.

E-Mail-Betrug kostete die Opfer mehr als

$ 6 Milliarden

seit das FBI Ende 2013 damit begann, ihn aufzuspüren.*

Ein Litauer wurde beschuldigt, im Juli 2017 mehr als

$ 100 Mio.

bei separaten Angriffen auf Google und Facebook gestohlen zu haben.**

Aber Zustellbarkeit und Sicherheit sind keine Dinge des Zufalls oder des Glücks. In meiner Checkliste biete ich Dir 10 Schritte, um Deine E-Mail-Zustellbarkeit zu erhöhen und Deine Domain-Sicherheit zu optimieren.

Ich wünsche Dir viel Spaß beim Lesen!

Philipp Zöld
Inhaber
Mailculture

*FBI Internet Crime Complaint Center. '2017 Internet Crime Report'. May 2018.
**Reuters. 'Lithuanian court upholds extradition of man to U.S. in $100 million fraud case'. August 2017.

CHECKLISTE

Mailculture®
KULTIVIERTES E-MAIL-MARKETING

Zustellbarkeit im E-Mail-Marketing erhöhen

1 Separate Subdomain einrichten

- [ ] **Nutze je eine Domain für Deine Marketing- und geschäftlichen E-Mails.**

  Wenn du Deine Haupt-Domain auch für den werblichen Newsletter nutzt, kann sich eine mögliche Blockierung dieser E-Mails auch **negativ auf deine geschäftliche E-Mail-Kommunikation auswirken**.

2 Separate Subdomain authentifizieren

- [ ] **Authentifiziere Deine E-Mails mit den Standards SPF, DKIM und DMARC.**

  Somit teilst Du Deinem Mailbox Provider (GMX, WEB oder GMAIL) klar mit, dass die **E-Mails von Dir stammen** und legst zusätzlich fest, wie er E-Mails handhaben soll, die **angeblich** von Dir stammen.

3 Keine E-Mail-Adressen kaufen

- [ ] **Nimm nur Personen in deinen Verteiler auf, die sich freiwillig angemeldet haben.**

  Das verschafft Dir nicht nur **rechtliche Sicherheit**, sondern **schützt Dein Ansehen** bei den Internet Service Providern und **schafft Vertrauen** bei Deinen Kunden.

4 Verteileraufbau mit Double-Opt-in

- [ ] **Versende nur Werbung, wenn Du eine Einwilligung dafür erhalten hast.**

  Wenn es eine Kundenbeziehung zum Adressaten gibt, der ein bestimmtes Produkt bei Dir gekauft hat, sende ihm **nur Informationen zu einem gleichen oder ähnlichen Produkt** zu.

5 Eine einfache Abmeldung ermöglichen (Single-Opt-out)

- [ ] **Integriere einen gut sichtbaren Abmeldelink in den Newsletter.**

  Laut DSGVO muss in jedem Newsletter ein **Abmeldelink** platziert werden, der **gültig** und **funktionsfähig** ist. Die Abmeldung muss auch **ohne Anmeldung auf einer Website möglich** sein.

CHECKLISTE

Mailculture®
KULTIVIERTES E-MAIL-MARKETING

Zustellbarkeit im E-Mail-Marketing erhöhen

6 Werbung nur mit Einwilligungen (Double-Opt-in)

- [ ] **Versende nur Werbung, wenn Du eine Einwilligungserklärung besitzt.**

  Wenn es eine Kundenbeziehung zum Adressaten zu einem bestimmten Produkt gibt, senden Sie ihm **nur Informationen zu einem gleichen oder ähnlichen Produkt** zu.

7 Die Verteilerliste(n) sauberhalten

- [ ] **Nutze einen Listenhygienedienst zur Überprüfung von E-Mail-Adressen.**

  Indem du **regelmäßig prüfst**, ob die E-Mail-Adressen zu aktiven Personen gehören, kannst du diejenigen Adressen identifizieren, die Deinem Ruf möglicherweise schaden könnten.

8 Die schwarzen Listen im Blick behalten

- [ ] **Nutze ein Blacklist-Suchtool, um potenzielle Probleme zu erkennen.**

  Das Suchtool testet eine IP-Adresse eines Mailservers gegen über 100 E-Mail-Blacklisten. Wenn Dein Mailserver auf einer schwarzen Liste steht, werden einige Deiner E-Mails evt. nicht zugestellt.

9 Spam-Wörter und Zeichen vermeiden

- [ ] **Vermeide Wörter und Zeichen, die Spamfilter alarmieren könnten.**

  SPAM-Filter reagieren besonders auf die Kategorien „Kostet nix“, „Sparen“, „Kaufen“, „Schnell sein“ und „Ganz sicher“.

10 Richtige Versandfrequenz finden und stets einhalten

- [ ] **Halte die Zeitabstände zwischen den Mailings nicht zu kurz.**

  So vermeidest Du, dass Du die Leser*innen belästigst und am Ende mit einer Abmeldung bestraft wirst. Beispiel: **Halte den** 14-tägigen **Versandrhythmus ein**, wenn Du diesen versprochen hast.

GLOSSAR

ZUSTELLUNG

ZUSTELLRATE

Die Zustellrate gibt prozentual an, wie viele E-Mails aus einem System oder von einem Server tatsächlich in das adressierte Postfach zugestellt werden. Eine hohe Zustellrate ist die Grundlage für erfolgreiches E-Mail Marketing und sollte im besten Fall immer über 95 Prozent liegen.

WHITELIST

E-Mail-Anbieter greifen in der Regel auf öffentliche Whitelists (Positivlisten) zurück. Die bekanntesten Anbieter hierfür sind die Certified Senders Alliance (CSA), Return Path und TrustedDialog. Um in eine öffentliche Whitelist eingetragen zu werden, muss der Versender seine Authentizität sowie Best-Practice-Beispiele nachweisen.

BLOCKLIST

Die Newsletter Blocklist (ehemals Blacklist) ist eine Sammlung von IP-Adressen und Domains, denen Spam unterstellt wird. Newsletter, die von einer dieser IP-Adressen oder Domains versendet werden, werden vom E-Mail Provider nicht angenommen und somit an Empfänger:innen nicht zugestellt.

SPF

Das Protokoll SPF (Sender Policy Framework) ist dafür verantwortlich, dass deine Absenderdomain bei einem authentischen Server liegt und dieser für den Versand verifiziert ist. Der SPF-Datensatz ist ein „Dokument“, das den Namen des einzigen autorisierten „virtuellen Postboten“ enthält – nennen wir ihn Rüdiger – der für die Zustellung deiner E-Mail an den Empfänger verantwortlich ist. Auf diese Weise akzeptiert der Empfänger deine Nachricht.

DKIM

Mithilfe von DKIM (DomainKey Message Identifier) übernimmst du die Verantwortung für Nachrichten und kannst garantieren, dass der Inhalt authentisch ist und nicht geändert wurde. Jeder, der versucht, die E-Mail während des Transports zu manipulieren, muss das Siegel brechen, um dies zu tun und ist daher für den E-Mail-Empfänger unweigerlich erkennbar.

DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) vereint die anderen beiden Protokolle und ist der "Hund" vor dem Empfänger-Briefkasten. Dieser kennt deine Unternehmensregeln und weiß dank seines guten Geruchssinns, ob der Postbote (Versender) und seine Post (E-Mail) betrügerisch sind. Er fängt an zu bellen, um den Empfänger auf die bevorstehende Betrugsgefahr aufmerksam zu machen.

SPAM

Unter Spam (engl. für „Abfall“ oder „Plunder“) versteht man den Versand unerwünschter E-Mails. Als unerwünscht gilt eine E-Mail dann, wenn diese dem Empfänger ohne seine ausdrückliche oder zumindest mutmaßliche Einwilligung zugestellt wird.

SOFT BOUNCE

Soft Bounces sind vorübergehende Fehler wie beispielsweise ein volles E-Mail-Postfach. Der Mailserver versucht, die E-Mail zu einem späteren Zeitpunkt erneut zuzustellen. Scheitert dies nach mehreren Versuchen, dann wird der Soft Bounce meist zu einem Hardbounce hochgestuft.

HARD BOUNCE

Hard Bounces sind dauerhafte Fehler wie beispielsweise eine nicht mehr existierende E-Mail-Adresse. Du solltest sie regelmäßig aus deiner Verteilerliste entfernen. Die meisten E-Mail-Marketingsysteme entfernen die nicht funktionierende E-Mail-Adresse automatisch aus dem E-Mail-Verteiler. Werden gebouncte Adressen zu oft angeschrieben, kann der Versender schnell als Spammer eingestuft werden. Außerdem werden unnötige Versandkosten gespart.

INFORMATIONSQUELLEN

Inxmail E-Mail-Marketing-Glossar. https://www.inxmail.de/wissen/glossar.de
Sendinblue: https://de.sendinblue.com/glossar/
proofpoint: Whitepaper Stopping Email Fraud

Über Mailculture

Hi, mein Name ist Philipp Zöld.

Ich bin Inhaber von Mailculture und trainiere, berate und begleite Tech-Start-ups und IT-Dienstleister beim Aufbau Ihres E-Mail-Marketings.

Zusammen mit meinem Netzwerk aus Experten für Copywriting und Design konstruiere ich leidenschaftlich gern Geschichten um Produkte und Dienstleistungen herum, sodass Du langfristig Neukunden gewinnst und Deine Bestandskunden bindest.

Kostenlose IT-Sicherheitsprüfung für Deine Domain

Prüfe online, ob die wichtigsten Sicherheits-mechanismen des IT-Grundschutzes bei Deiner Domain wirksam implementiert sind.

Zum Domain Check

Fragen und Anregungen

Du hast Fragen zum Inhalt der Checkliste oder möchtest mir Anregungen mit auf den Weg geben? Dann schicke mir einfach eine E-Mail!

E-Mail senden

Lass uns Dein E-Mail-Marketing kultivieren.

Mailculture
Heinrich-Mann-Str. 15, 19053 Schwerin
+49(0)385 59389564
hi@mailculture.de
mailculture.de