EMAIL DELIVERABILITY GUIDE

Secrets for better Inbox Placement

Inhalt

Definitionen

Was ist Spam?

Spam (engl.; umgangssprachlich für UBE = Unsolicited Bulk Email) sind Massen-E-Mails bzw. Werbesendungen, die im Internet verbreitet werden. Diese landen unangefordert in Millionen von elektronischen Postfächern. Die meisten Spam-E-Mails haben einen kommerziellen Hintergrund und werden in folgende Typen unterteilt:

- kommerzieller E-Mail-Spam
- Kettenbriefe, Viruswarnungen, Hoaxes
- durch Viren versandte E-Mails
- Phishing-E-Mails

Zustellung (Zustellrate)

Die Zustellrate beschreibt den prozentualen Anteil der erfolgreich versendeten E-Mails (Empfang der Mail im Posteingang des Empfängers) an den insgesamt versendeten E-Mails. Bounces, das heißt unzustellbare Nachrichten, werden hier nicht mit einbezogen.
Die Zustellrate gibt somit unter anderem Auskunft über die Qualität der Verteilerliste. Um sie konstant auf einem hohen Niveau zu halten, bedarf es eines Bounce-Handlings, welches auch in der Global-Suppression-Lösung von Retarus implementiert ist. Nicht erreichbare E-Mail-Adressen werden hiermit automatisch aus einem Verteiler entfernt.

Reputation/Sender-Score

Scores werden als gleitender Durchschnitt über einen Zeitraum von 30 Tagen berechnet und repräsentieren die Rangordnung einer IP-Adresse gegenüber anderen IP-Adressen, ähnlich wie ein Prozentrang. Je näher der Score bei 0 liegt, desto schlechter ist er, und wenn er nahe an 100 liegt, scheint der Absender vieles richtiggemacht zu haben.

Beschwerden: Es wird der Quotient aus der Anzahl der Beschwerden und der Anzahl der empfangenen E-Mails berechnet. Berücksichtigt wird auch, wie viele Beschwerden die betreffende IP-Adresse im Vergleich zu anderen IPs erhält.

Volumen: Das Versandvolumen alleine ist kein Hinweis auf einen guten oder schlechten Ruf des Absenders. Es ist aber ein wichtiger Teil des allgemeinen Algorithmus. Zum Beispiel wird eine IP-Adresse, die 100 Nachrichten versendet und 99 Beschwerden erhält, als problematisch eingestuft. Dagegen wird eine IP-Adresse, die 100.000 Nachrichten versendet und 99 Beschwerden erhält, als gut bewertet. Das Volumen steht also immer in Abhängigkeit zu anderen Indexwerten.

Externe Reputation: Diese Zahl sagt aus, wie die IP-Adresse eines Absenders im Vergleich zu anderen auf einer Vielzahl von externen „Blacklists“ und „Whitelists” gelistet ist.

Unbekannte Kontakte
Das Verhältnis der Anzahl von unbekannten Kontakten einer IP-Adresse zu anderen Adressen wird direkt von einkommenden SMTP-Anmeldungen der beteiligten ISPs entnommen. Sie misst, wie oft eine IP-Adresse versucht, eine Nachricht an einen nicht existierenden Empfänger zu senden.

Zurückgewiesene Nachrichten
Hier wird gemessen, wie oft Nachrichten einen Soft- oder Hard-Bounce im Vergleich zu anderen IP-Adressen verursachen.

Angenommene Nachrichten
Diese Zahl repräsentiert, wie viele Nachrichten von den ISPs angenommen und an die Empfänger weitergeleitet werden. Die Zahl beinhaltet alle verschickten Nachrichten ohne die Anzahl der zurückgewiesenen.

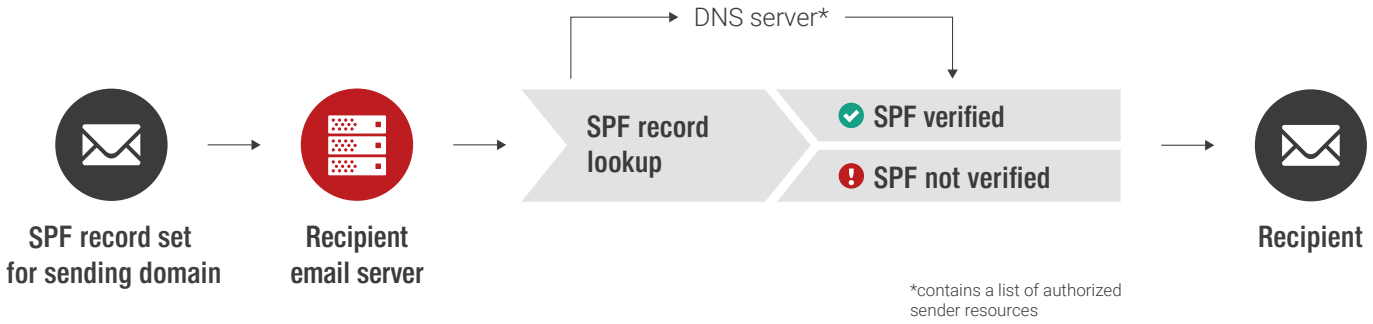
Verhältnis der angenommenen Nachrichten
Hierbei wird die Anzahl der angenommenen Nachrichten mit der aller versendeten Nachrichten verglichen. Dazu wird der Quotient aus Anzahl der verschickten Nachrichten und gelesenen Nachrichten gebildet.

Verhältnis der unbekannten Kontakte
Die Anzahl der unbekannten Kontakte oder ungültigen E-Mail-Adressen wird mit der Anzahl der verschickten Nachrichten verglichen.

SPF Record

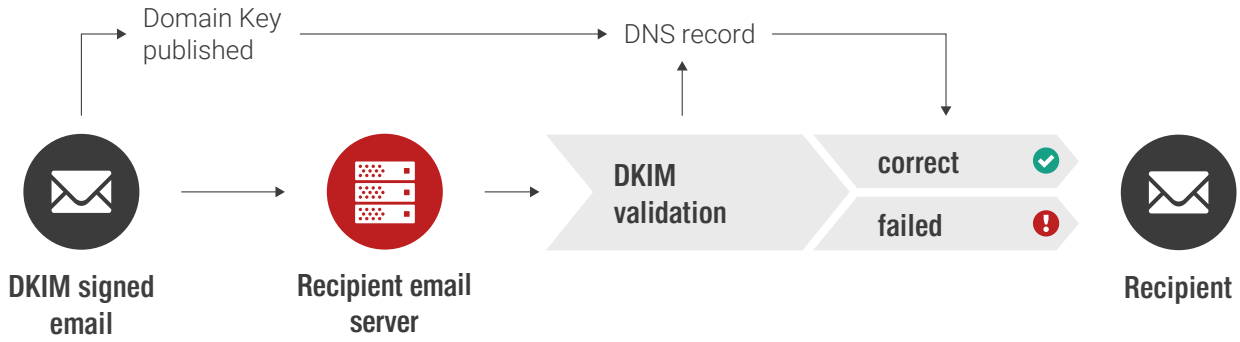
Das Sender Policy Framework (SPF; früher Sender Permitted From) ist ein Verfahren, welches das Fälschen von Absenderadressen einer E-Mail verhindern soll. Es entstand als Verfahren zur Abwehr von Spam. Bei SPF trägt der Inhaber einer Domain in das Domain Name System ein, welche Computer zum Versand von E-Mails für diese Domain berechtigt sind.

Der Administrator einer Domain hinterlegt in der DNS-Zone einen Resource Record vom Typ TXT (der SPF Resource Record wurde durch RFC 7208 obsolet). In diesen Resource Records sind die IP-Adressen derjenigen Mail Transfer Agents (MTA) enthalten, die für die Domain E-Mails versenden dürfen. Der Empfänger prüft anhand der in den Feldern „MAIL FROM“ und „HELO“ angegebenen Domain, ob der Absender zum Versand berechtigt ist. Für die angegebene Domain ruft der Empfänger die SPF-Information über das Domain Name System ab und vergleicht die IP-Adresse des sendenden MTAs mit den erlaubten Adressen. Stimmt die IP-Adresse überein, so ist der Absender authentisch, andernfalls kann die E-Mail verworfen werden.



DKIM

DomainKeys ist ein Identifikationsprotokoll zur Sicherstellung der Authentizität von E-Mail-Absendern. Es wurde konzipiert, um bei der Eindämmung unerwünschter E-Mails wie Spam oder Phishing zu helfen. DomainKeys basiert auf asymmetrischer Verschlüsselung. Die E-Mail wird mit einer digitalen Signatur versehen, die der empfangende Server anhand des öffentlichen Schlüssels verifizieren kann, der im Domain Name System (DNS) der Domäne verfügbar ist. Schlägt die Verifizierung fehl, hat der empfangende Mail Transfer Agent (MTA) oder das empfangende Anwendungsprogramm die Möglichkeit, die E-Mail zu verweigern oder auszusortieren.



Zusätzliche Definitionen in der E-Mail-Transactional-Welt

Inbox Placement Rate
Deliverability Rate, bereinigt um die Anzahl an E-Mails, die im Spam- oder Junk-Ordner gelandet sind

Softbounce
E-Mails, die an existierende Adressen versendet werden, aber temporär nicht zugestellt werden können

Hardbounce
E-Mails, die nicht dauerhaft zugestellt werden können

Öffnungsrate
Anzahl Öffnungen / Anzahl zugestellter E-Mails

Unique Click Rate
Anzahl Klicks in einer E-Mail, ohne Mehrfachklicks eines Users / Anzahl zugestellter E-Mails

Total Click Rate
Alle Klicks in einer E-Mail / Anzahl zugestellter E-Mails

Click to Open Rate
Unique Clickrate / Öffnungsrate

Conversion Rate
Anzahl gezielter Aktionen / Effektive Klickrate

Bounce Rate
Anzahl Bounces / Anzahl zugestellter E-Mails

Risiken und Gefahren

In einer aktuellen Studie stellt das E-Mail-Intelligence-Unternehmen Return Path fest, dass 20 Prozent der versendeten und gewollten E-Mails nicht bei den Empfängern ankommen. Nicht zugestellte E-Mails schaden Unternehmen in doppelter Hinsicht:

- Eine verringerte Reichweite von Marketing-Kampagnen ist mit Umsatzeinbußen verbunden. Das Umsatzpotenzial, das in Deutschland jährlich in Spam-Ordnern landet, wird auf etwa 3 Milliarden Euro geschätzt.
- Durch die versehentliche Spam-Klassifizierung entstehen nicht nur finanzielle Verluste. Auch die Reputation des Unternehmens bzw. der Marke wird in Mitleidenschaft gezogen, wenn die Versandadresse auf Blacklists erscheint und das Unternehmen als Absender von E-Mails negativ bewertet wird.

Ursachen für Spam-Klassifizierungen

Die Ursachen für eine Einstufung als Spammer können vielseitig sein, etwa Spam Traps, kalte IPs, die Gestaltung der E-Mails oder Reputations-Scores. Es ist verständlich, dass Anwender ihren E-Mail-Posteingang und ihren Rechner mit Sicherheitssoftware vor Angriffen aus dem Internet schützen wollen. Es empfiehlt sich, dieses Sicherheitsbedürfnis der Kunden bei der Planung von E-Mail-Marketing-Maßnahmen zu bedenken.

BLACKLIST

Definition

- Verzeichnis von IP-Adressen und Domains, die durch den Versand unerwünschter E-Mails negativ aufgefallen sind
- E-Mails, die über diese IP versendet werden, werden abgefangen/blockiert
- Große E-Mail-Provider nutzen meist mehrere Blacklists

Vorteil

- Schutz der Anwender vor unerwünschter Kommunikation

Nachteile

- Gewollte E-Mails auf der Blacklist, z. B. wenn eine Blacklist eine ganze Domain sperrt, obwohl nur eine Subdomain Spam-Mails versendet
- Umsatzeinbußen und Imageschaden für den Absender – keine Zustellung mehr von Kampagnen, die über diese IP versendet werden
- Aufwändiges Delisting. Es ist möglich von einer Blacklist wieder gelöscht zu werden. Bei mehrfachen Vergehen landen Versender jedoch eventuell permanent auf der Blacklist
- Unlauteres Geschäftsmodell

GREYLIST

Definition

- Abweisung einer bisher unbekannten E-Mail- und/oder IP Adresse beim ersten Zustellversuch
- Zweiter, späterer Zustellversuch meist erfolgreich

Vorteile

- Effektive Spam-Bekämpfung: Viele Spammer geben beim ersten Zustellversuch auf, echte Mail Server führen in der Regel einen zweiten Zustellversuch aus
- Nach einer erfolgreichen E-Mail-Zustellung wird die Kombination von Sender, Empfänger und E-Mail-Server in die Whitelist eingetragen und Folge-Mails werden zugestellt
- Greylisting hat einen Einfluss auf die E-Mail-Qualität, es kommt also nicht zu einem automatischen Opt out

Nachteile

- Eine unerwünschte E-Mail kann durch Greylisting einige Minuten oder auch Stunden später eintreffen
- Einige Mail-Server-Programme generieren bereits nach dem ersten Versuch einen vorläufigen Zustellbericht an den Absender, der gegebenenfalls als fehlgeschlagene Zustellung interpretiert wird
- Beim Einsatz von IP-Tools könnten E-Mails gar nicht zugestellt werden

Leitfaden für eine gute Zustellbarkeit

Die Zustellbarkeit („Deliverability“) ist eine der wichtigsten Säulen im professionellen E-Mail-Marketing. Die Qualität der Systeme von Unternehmen, die E-Mail-Kampagnen versenden, ist wichtig, um Zustellbarkeitsraten hochhalten und ausbauen zu können.

Warm-Up unbekannter IPs

Die Reputation von IP-Adressen basiert größtenteils auf historischen Versandmustern und -volumen. Eine IP-Adresse, die über einen langen Zeitraum hinweg konsistente Mengen an E-Mails versendet, weist in der Regel eine hohe Zuverlässigkeit auf. Unternehmen, die dedizierte IP-Adressen verwenden, erhalten ihre Reputation als Absender aufrecht, indem sie konsistente und vorhersehbare Mengen an E-Mails versenden. Retarus empfiehlt hierzu folgendes zum Warm-Up einer dedizierten und bisher unbekannten IP zu beachten:

- Dauer des Warm-up-Prozesses: ca. 6-8 Wochen
- Anfangs ein geringes E-Mail-Volumen versenden:
  - » Max. 1.000 E-Mails an Tag 1
  - » Verdoppelung des Volumens auf Basis des Vortags
  - » Start mit gedrosselter Versandgeschwindigkeit
  - » Langsames Steigern von Volumen, Anzahl der Empfänger, Versandgeschwindigkeit
- Paralleler Start einer Bereinigung der Anwenderliste
- Alle verfügbaren IPs und Domains regelmäßig nutzen, so bleiben diese bekannt und werden als vertrauenswürdig betrachtet
- Keine plötzlichen und extremen Intensivierungen
- Gefahr von Blacklisting geringhalten (Vorsicht vor Spam Traps und Affiliate-Kampagnen)
- Während des Warm-Ups keine strategisch wichtigen, aber attraktive Kampagnen versenden
- Anfänglich Versand auf besonders aktive und interessierte Kunden konzentrieren

Zustellrate

Eine Anmeldung per Double-Opt-in-Verfahren erhöht die Qualität des Empfängerkreises. Denn es werden nur Empfänger angeschrieben, die sich selbst angemeldet haben und deren

E-Mail-Adresse auch tatsächlich existiert.

Um die Zustellrate weiter zu erhöhen, kann bei der Newsletter-Anmeldung dazu aufgefordert werden, den Absender zum persönlichen Adressbuch bzw. zur persönlichen Whitelist hinzuzufügen. Denn oftmals werden auch erwünschte E-Mails und Newsletter im Postfach des Abonnenten als Spam gekennzeichnet (false positives). Die Mitgliedschaft des Versenders in der Certified Senders Alliance (CSA), einer zentralen Whitelist-Datenbank, welche zusätzliche Sicherheitsmechanismen fordert, kann sich ebenfalls positiv auf die Zustellrate auswirken.

Reputation

Erkenntnis ist stets der erste Schritt zur Besserung. Da es einige Zeit dauert, um einen schlechten Sender Score zu verbessern, sollten Absender ihre Reputation vom ersten Versand an kennen. Es gibt mehrere Aspekte im E-Mail-Marketing, die Unternehmen überprüfen und bei Bedarf anpassen können, damit sich der Sender Score verbessern kann. Die folgenden Baustellen haben den größten Einfluss auf die Zustellbarkeit von E-Mails:

Unregelmäßiges Sendevolumen
Ein Versand gleichmäßiger E-Mail-Volumina ist für die Reputation maßgebend – Peaks oder ähnliches können die Reputation negativ beeinflussen.

Häufigkeit der versendeten Nachrichten
Auch Aussendungen gleichmäßig zu versenden, wirkt sich auf die Reputation positiv aus. Dabei spielt es keine Rolle, ob Unternehmen E-Mailings täglich, jeden zweiten Tag oder jede Woche versenden. Dies richtet sich nach den Erfordernissen des Marketings. Es sollte lediglich sichergestellt sein, dass nach einem festen Zeitplan versandt wird. Wenn E-Mail-Marketing gut aufgebaut und stabilisiert ist, lässt sich mithilfe von Tests die optimale Frequenz für die jeweilige Zielgruppe ermitteln.

Auf einer Blacklist stehen
Es gibt etwa 50 bekannte Blacklists, die festhalten, welche IPs Spammer sind. Retarus hat die größten und bekanntesten Blacklist-Betreiber in das aktive Monitoring des Customer Services aufgenommen und überwacht diese. Sollten Anwender von Retarus Transactional Email trotz Warm-Up und weiteren reputationssteigernden Maßnahmen in eine dieser Blacklists eingetragen worden sein, unterstützt der Retarus-eigene Customer Service beim Delisting und recherchiert die Ursachen eines Eintrags. Mit den Ergebnissen können die Anwender von Transactional Email ihre E-Mail-Marketing-Methoden verbessern.

Spam Traps
Eine solche Falle ist eine E-Mail-Adresse, die zwar einmal gültig war, es aber mittlerweile nicht mehr ist und Absendern deshalb als Hard Bounce angezeigt wird. Wenn jedoch ein Mail-Server registriert, dass ein Absender regelmäßig an eine ungültige Adresse Nachrichten versendet, kann diese E-Mail-Adresse zur Spam-Falle werden. Das bedeutet, dass Absender nicht länger eine Hard-Bounce-Benachrichtigung erhalten, sondern dass entsprechende Nachricht angenommen und jeweilige Absender als Spammer gekennzeichnet werden. Es empfiehlt sich, Hard Bounces im Blick zu behalten und Verteiler regelmäßig zu pflegen.

Spam-Berichte
Empfänger, die einen Absender für einen Spam-

mer halten, können diesen in Spam-Berichten melden. Das schadet dem Ruf der Absender. Deshalb sollten diese regelmäßig überprüfen, wie hoch ihre Spam-Quote ist. Anhaltspunkt: Wenn eine Nachricht pro 1.000 als Spam markiert wird, gibt es keinen Anlass zur Sorge.

Qualität der User-Liste

Die Anmelde- und Abmelde-Funktion ist bei einem kundenfreundlichen, seriösen E-Mail-Versand inzwischen selbstverständlich. Ein Grund dafür sind rechtliche Rahmenbedingungen für den Versand elektronischer Post, denen dadurch entsprochen wird. Der Newsletter-Versand ist nur dann legal, wenn der Empfänger seine Einwilligung erteilt hat. Teilnehmer einer Whitelist müssen diese Zustimmung mit Quelle und Zeitstempel nachweisen.

Eine ebenso wichtige Rolle spielt die Unsubscribe-Funktion, den jeder Newsletter enthalten muss. Ein Kunde, der das Abonnement schnell und zwanglos kündigen kann, wird die Sendung nicht als Spam melden. Das ist wichtig, da sonst eine negative Reputation oder gar der Eintrag auf einer Blacklist droht. Wenn sich ein Kunde aus dem Verteiler abmeldet, sollte seine Adresse möglichst sofort aus dem Verteiler entfernt werden und darf keinesfalls ein weiteres Mal angeschrieben werden.

Nutzung von Anhängen

ISPs prüfen sehr häufig auf typische File Types, von denen ein hohes Gefahrenpotential ausgeht. Hierzu zählen insbesondere ausführbare Dateien (exe) oder Skripte.

.ade	.js	.msh	.ps1xml
.adp	.jse	.msh1	.ps2
.app	.ksh	.msh2	.ps2xml
.asp	.lib	.mshxml	.psc1
.bas	.lnk	.msh1xml	.psc2
.bat	.mad	.msh2xml	.tmp
.cer	.maf	.msi	.url
.chm	.mag	.msp	.vb
.cmd	.mam	.mst	.vbe
.com	.maq	.ops	.vbs
.cpl	.mar	.pcd	.vps
.crt	.mas	.pif	.vsmacros
.csh	.mat	.plg	.vss
.der	.mau	.prf	.vst
.exe	.mav	.prg	.vsw
.fxp	.maw	.reg	.vxd
.gadget	.mda	.scf	.ws
.hlp	.mdb	.scr	.wsc
.hta	.mde	.sct	.wsf
.inf	.mdt	.shb	.wsh
.ins	.mdw	.shs	.xnk
.isp	.mdz	.sys	
.its	.msc	.ps1	

Rollenbasierende Absender-Adressen

Rollenbasierende Adressen sind in der Regel Firmenadressen, die nicht von einer Person, sondern von einem Job definiert und oft von mehreren Personen verwaltet oder letztendlich nicht genutzt werden. Einige dieser Adressarten sind mit hohen Bounce-Raten und Spam-Beschwerden verbunden. Deshalb werden sie von Retarus auf Wunsch blockiert. Rollenbasierende E-Mail-Adressen können auch nicht zur Anmeldung für ein Konto verwendet werden.

abuse@	list@	spam@
admin@	noc@	support@
billing@	no-reply@	sysadmin@
compliance@	noreply@	tech@
devnull@	null@	undisclosed-recipients@
dns@	phish@	unsubscribe@
ftp@	phishing@	usenet@
hostmaster@	postmaster@	uucp@
inoc@	privacy@	webmaster@
ispfeedback@	registrar@	www@
ispsupport@	root@	
list-request@	security@	

Strategie und Priorisierung von Kampagnen

Um die Reputation nicht zu gefährden, trägt auch die richtige Strategie und Priorisierung der Kampagnen ihren Teil bei. Der Schlüssel um Ihre Reputation nicht zu gefährden heißt:

Frequenzen definieren
Zeitpunkt und Frequenz des Versands einer Kampagne haben einen entscheidenden Einfluss darauf, wie die Empfänger die Nachricht einstufen. Eine Flut von einzelnen Benachrichtigungen innerhalb weniger Stunden führt mit großer Wahrscheinlichkeit zur Ablehnung seitens des Empfängers. Schlägt das Feedback auf den ISP durch, hat das einen negativen Einfluss auf die Reputation zur Folge.

Priorisierung / Gruppen gezielt ansprechen
Es empfiehlt sich, wichtige Aussendungen nicht zeitgleich mit weniger wichtigen Kampagnen zu versenden. Durch das erhöhte Versandvolumen steigt das Risiko, die Reputation negativ zu beeinflussen. Dadurch sinkt die Zustellungsrate der wichtigen Kampagnen und das gesetzte Ziel der Kampagne wird nicht erreicht.

Differenzierte Ausgangskanäle nutzen und klare Trennung
Über separate Versandstränge lassen sich hohe Zustellraten für Kampagnen erhalten. Kampagnen sollten nicht über die Haupt-Domain ausgesandt werden, sondern über entsprechende Sub-Domains. Noch besser ist es, dedizierte IP-Adressen (Dedicated IP) zu nutzen.

Gestaltung von E-Mails

In der Kopf- und Betreffzeile von E-Mails darf weder der Absender noch der kommerzielle Charakter der Nachricht verschleiert oder verheimlicht werden. Ein Verschleiern oder Verheimlichen liegt dann vor, wenn die Kopf- und Betreffzeile absichtlich so gestaltet sind, dass der Empfänger vor Einsichtnahme in den Inhalt der Kommunika-

tion keine oder irreführende Informationen über die tatsächliche Identität des Absenders oder den kommerziellen Charakter der Nachricht erhält. Jede versendete E-Mail muss ein den geltenden rechtlichen Anforderungen entsprechendes, leicht erkennbares Impressum enthalten.

BETREFFZEILE

- Eine E-Mail sollte stets einen Betreff haben
- Kurz, aber aussagekräftig
- Auf Großbuchstaben und Sonderzeichen verzichten
- Bestimmte Begrifflichkeiten meiden (zum Beispiel SEX, GRATIS!€; LEIHE)
- Zusammenhang zwischen Betreff und Inhalt sicherstellen
- Wortwiederholungen meiden

Tipps für optimale E-Mail-Gestaltung

Relevanz für die Empfänger deutlich machen
Konzentrieren Sie sich auf ein spezielles Thema und legen Sie dieses deutlich dar.

Above-the-Fold-Space nutzen
Positionieren Sie die wichtigsten Bausteine in der E-Mail ganz oben, sodass sie direkt auffallen.

Passende Handlungsaufforderungen einfügen
Machen Sie dem Leser deutlich, was er tun soll und was er für sein Handeln bekommt.

Bilder mit Dateinamen versehen
Kennzeichnen Sie Bilder mit einem entsprechenden Dateinamen, damit der Leser den Inhalt versteht, sollte das Bild nicht geladen werden.

Spam-Begriffe vermeiden
Benutzen Sie keine Begriffe, die mit Geld oder Gewinn zu tun haben, damit Ihr Newsletter im Posteingang landet und nicht als Spam gewertet wird.

Social Media Shares ermöglichen
Fügen Sie eine Funktion zum Teilen ein, damit der Leser die Möglichkeit hat, den Newsletter zu publizieren.

Personalisiert schreiben
Der Empfänger fühlt sich sofort angesprochen, wenn er seinen Namen liest. Fügen Sie daher in der Anrede den Namen des Empfängers ein.

Für den Versand von E-Mails mit Werbeinhalten gilt zudem:
Der Auftraggeber einer Werbesendung muss klar erkennbar sein. In jeder E-Mail ist der Empfänger gesondert auf die Möglichkeit hinzuweisen, die erteilte Einwilligung in die Zusendung von E-Mails jederzeit zu widerrufen. Der Widerruf / das Abbestellen von E-Mails (Opt-Out / Unsubscribe) muss dem Empfänger grundsätzlich ohne Weiteres, das heißt ohne die Eingabe von Zugangsdaten (zum Beispiel Login und Passwort) möglich sein.

Verfasser: Peter Schnäp, Technical Product Manager Transactional Email. Erstellt am 05.06.2018

Wie Sie Retarus Transactional Email bei der Deliverability unterstützt, erklären wir Ihnen gerne in einem persönlichen Gespräch:
www.retarus.de/contact