Wie ein Spamfilter funktioniert

Um die Qualität ihrer Mailings zu erhöhen, arbeiten Brands oft mit einem E-Mail Service Provider (ESP) zusammen, anstatt die E-Mails selbst zu versenden. Der ESP fordert den Brand auf, SPF, DKIM und andere Standards einzuführen. Aber warum ist das nötig? Sehen wir uns einmal an, wie ein typischer mehrstufiger Spamfilter heute funktioniert.

IP Filter

Die allererste Information, die ein potentieller Empfänger einer E-Mail erhält, ist die IP-Adresse des sendenden Servers, der versucht, eine Verbindung herzustellen. Wenn die IP-Adresse als Spamquelle bekannt ist, gibt der Empfänger höchstwahrscheinlich einen Fehlercode zurück, der die E-Mail nicht akzeptiert - oder schlimmer noch, er lehnt die Verbindung einfach ab.

Als Versender von E-Mails ist es äußerst wichtig, die IP-Reputation der sendenden E-Mail-Server zu überwachen. Brands, die sich auf die Dienste eines ESP verlassen, geben die Verantwortung dafür natürlich an den ESP ab.

Empfänger von E-Mails nutzen häufig Reputationsdaten von Dritten zusätzlich zu ihren eigenen, um bessere Ergebnisse zu erzielen. Dies können Blacklists sein, die IP-Adressen mit schlechtem Ruf enthalten, oder Whitelists wie die Certified Senders Alliance Whitelist, die IP-Adressen von zertifizierten Absendern enthält, die hohe Qualitätsstandards erfüllen und daher einen guten Ruf haben.

Authentifizierung

Selbst wenn ein Brand mit einem ESP arbeitet, müssen einige Einträge im DNS der Domain vorgenommen werden, damit Technologien wie SPF, DKIM und DMARC funktionieren. Warum ist das wichtig? Diese drei Technologien ermöglichen es dem Empfänger, den Sender zu authentifizieren. Einfach ausgedrückt, der Empfänger kann erkennen, ob eine eingehende E-Mail legitim ist und tatsächlich von der durch die Absenderadresse angegebenen Brand stammt. Empfänger können bösartige E-Mails mit gefälschten Absenderadressen identifizieren und herausfiltern.

Die Implementierung dieser Technologien führt nicht notwendigerweise direkt zu höheren Zustellraten für Brands, die E-Mails versenden, aber es ist wichtig, sich von allen Spammern da draußen zu unterscheiden und Vertrauen aufzubauen

Inhaltsanalyse

Bisher hat der Empfänger nur mit Informationen aus der Verbindung oder dem E-Mail-Header gearbeitet. Der nächste Schritt ist die Analyse des Inhalts der E-Mail. Dies kann bestimmte Wortfilter, das Verhältnis von Text zu Bild, Muster typischer schlechter oder guter E-Mails, die Reputation von in der E-Mail enthaltenen Links, Reputation von Anhängen, natürlich traditionelle Virenprüfung und vieles mehr beinhalten.

User Engagement und User Filter

Viele Empfänger prüfen auch, wie der Endbenutzer in der Vergangenheit auf ähnliche E-Mails reagiert hat. Wenn ein Benutzer in der Vergangenheit E-Mails zu einem bestimmten Thema nicht mochte, ist es sehr wahrscheinlich, dass es ihm jetzt auch nicht gefällt. Oder wenn die Mehrheit der Endbenutzer die E-Mails einer bestimmten Kampagne als Spam kennzeichnen, ist es wahrscheinlich, dass diese E-Mails auch für die anderen Benutzer im Spam-Ordner landen. Last but not least können Anwender individuelle Filterregeln einrichten. Im Hinblick auf User Engagement Filter ist es offensichtlich, dass technische Lösungen nicht ausreichen um zugestellt zu werden. Der Inhalt der E-Mails muss interessant und relevant sein.

Fazit

Spamfilter werden immer anspruchsvoller und komplexer. Der beste Weg, den Posteingang erfolgreich zu erreichen, ist nicht, diese Filter zu überlisten, sondern Best Practices zu befolgen und die bestmögliche E-Mail zu versenden. ESPs können einen großen Teil davon übernehmen, aber Brands müssen mit ihnen zusammenarbeiten, um fortschrittliche Technologien wie DMARC einzuführen. Die CSA-Zertifizierung stellt sicher, dass ein Absender diese Best Practices einhält und eine optimale Zustellung gewährleistet.

Weitere hilfreiche Dokumente, wie die "eco Richtlinie für zulässiges E-Mail-Marketing", können kostenlos heruntergeladen werden unter https://certified-senders.org/de/dokumente/

Authors: Technical Team of the Certified Senders Alliance