

## Hilfe! Ich habe eine Spamtrap getroffen!

### Was ist eine Spamtrap und wofür ist sie gut?

Eine Spamtrap ist eine E-Mail-Adresse, die nicht von einer tatsächlichen Person verwendet wird. Ihr Zweck ist es, E-Mail-Absender zu finden, die unerwünschte E-Mails versenden. Spamtraps werden normalerweise verwendet, um Spamfilter zu verbessern, indem sie IP-Adressen identifizieren und blockieren, die E-Mails an eine Spamtrap senden. Es gibt zwei verschiedene Arten von Spamtraps:

- pristine spamtrap:

Die E-Mail Adresse einer pristine spamtrap wurde noch nie zuvor von jemandem verwendet. Sie wurde ausschließlich zum Zweck des "Einfangens" von Spam erstellt. Jede E-Mail, die an eine pristine Spamtrap gesendet wird, kann nie angefordert worden sein. Die einzige Ausnahme könnte sein, dass jemand bei der Anmeldung zu einem Newsletter seine eigene E-Mail-Adresse falsch geschrieben und versehentlich genau die Adresse einer Spamtrap eingegeben hat. Um dies zu verhindern, verwenden die meisten Spamtrap-Betreiber keine "Tippfehler"-Domains für ihre Traps. (z.B. outlok.com)

- recycled spamtrap:

Im Gegensatz zu pristine Spamtraps war die Adresse einer recycled Spamtrap zuvor im Besitz einer echten Person. Dies kann die Domain eines Unternehmens sein, welches den Betrieb eingestellt hat, oder einzelne E-Mail-Adressen von Freemail-Nutzern, die ihr Konto gelöscht und die Adresse freigegeben haben. Je nach Mailbox-Anbieter reagiert eine von einem ehemaligen Kunden freigegebene E-Mail-Adresse mindestens 6 bis 12 Monate lang mit einem Hardbounce, bevor sie in eine Spamtrap umgewandelt wird.

### Wer betreibt Spamtraps?

Grundsätzlich kann jeder eine Spamtrap betreiben. Sie werden jedoch in der Regel von Postmastern größerer Unternehmen oder Freemail-Anbietern betrieben, um ihre Spamfilter zu verbessern und natürlich von Blacklist-Anbietern. Viele Blacklists sind auf Spamtraps angewiesen. Wenn mehrere E-Mails (in seltenen Fällen sogar nur eine) von derselben IP auf eine Spamtrap treffen, wird die IP der Blacklist hinzugefügt.

## Wie vermeidet man das Treffen von Spamtraps?

Spamtraps in Ihren E-Mail-Listen sind eine schlechte Sache. Wie geraten die überhaupt dort hin? Die Hauptgründe dafür sind:

- Adresssammler: Einige Spamtrap-Betreiber veröffentlichen die Adressen auf einfachen Websites, Foren usw., um sie so genannter Harvester-Software auszusetzen. Während die Nutzung dieser Programme selbst legal sein kann, ist die Verwendung der gesammelten Adressen zumindest in der Europäischen Union illegal und wird höchstwahrscheinlich Spamtrap-Adressen enthalten. Verwenden Sie niemals diese Art von Software!
- Gekaufte Listen: Einige Listenanbieter arbeiten legal und sauber, andere nicht. Wenn Sie sicher sein wollen, kaufen Sie niemals Listen.
- Kein ausreichende Listenhygiene: Dies ist vor allem bei recycelten Spamtraps ein Problem. Senden Sie nicht an alte Adressen, die Sie seit Jahren nicht mehr verwendet haben. Bereinigen Sie inaktive Adressen sofort und nehmen Sie die Listenhygiene ernst.
- list poisoning: Dies kann entweder versehentlich (z.B. ein Tippfehler bei der Registrierung) oder absichtlich von jemandem geschehen, der Ihnen Schaden zufügen möchte, indem er bekannte Spamtrap-Adressen in Ihre Liste einträgt. Die einfache Lösung für dieses Problem ist die Verwendung von Double Opt-In beim Sammeln von Adressen.

## Ich habe trotzdem eine Spamtrap getroffen. Was kann ich nun tun?

Versuchen Sie zuerst herauszufinden, was schief gelaufen ist. Wenn Sie nie irgendwelche Probleme hatten und von einem Tag auf den anderen eine Spamtrap oder sogar mehrere Spamtraps getroffen haben, schauen Sie sich die Vergangenheit der Liste an. Hat jemand kürzlich Adressen importiert? Haben Sie E-Mails an eine Liste geschickt, die für eine Weile inaktiv war? Wenn nichts verdächtig erscheint, gruppieren Sie die Liste in kleinere Teile und versuchen Sie, den Teil zu finden, der eine Spamtrap-Adresse enthält. Im Zweifelsfall ist es besser, eine Adresse oder sogar den gesamten Cluster aus der Liste zu entfernen. Die gleiche Spamtrap erneut zu treffen ist schlimmer als ein paar Abonnenten zu verlieren.

## Fazit

Der beste und einfachste Weg, um mit Spamtrap-Hits umzugehen, ist, niemals einen Spamtrap zu treffen. Das scheint ironisch, aber Prävention ist die beste Methode, um nicht auf Probleme zu stoßen und um Ihren guten Ruf zu schützen.

Ein paar einfache Schritte helfen Ihnen, das Risiko, eine Spamtrap zu treffen, massiv zu reduzieren.:

- Nutzen Sie keine gekauften Listen oder Adressen aus Harvestern.
- Pflegen Sie Ihre Listen sorgfältig. Entfernen Sie Bounces und inaktive Teilnehmer
- Verwenden Sie double opt-in
- Überprüfen Sie E-Mail-Adressen im Zuge der Registrierung oder beim Import auf Unregelmäßigkeiten wie
  - nicht existierende Domains
  - ungültige oder fehlende MX records
  - Rollenbezogene Adressen wie info@, spam@, root@, webmaster@,...
  - und so weiter.

*Autoren: Technikteam der Certified Senders Alliance*