

## Infos zu SPAM

Was ist Spam?

Entweder Dosenfleisch oder unerwünschte E-Mail.



Die Fachbegriffe für die umgangssprachliche Bezeichnung Spam (oder Junk-E-Mail) sind:

- UCE (unsolicited commercial email), unerwünschte kommerzielle, Werbung enthaltende E-Mail
- UBE (unsolicited bulk email), unerwünschte und in Massen versandte E-Mail

Im allgemeinen ist Spam sowohl UCE als auch UBE. Spam erkennt man an folgenden Kennzeichen (eins oder mehrere):

- E-Mail ist meist in englischer Sprache, inzwischen aber auch vermehrt in deutscher Sprache und wurde aus dem Ausland verschickt (z.B. Casino-Spam).
- E-Mail kommt aus Nigeria oder einem anderen afrikanischen Land. Man soll einem angeblich ins Exil geschickten König helfen, an sein Geld zu kommen. Das ist Spam der sogenannten Nigeria-Connection, der Betreff fängt meist mit "FROM " an, und man soll dem angeblichen König natürlich erst Geld schicken, damit er wieder an sein Geld kann und Sie danach reich belohnt.
- E-Mail enthält Werbung für eine Website, eine Dienstleistung oder ein Produkt (z.B. potenzfördernde Mittel).
- Die Absender-Adresse ist gefälscht (Fäl-

schung nicht immer direkt und eindeutig zu erkennen, aber beispielsweise pontius.pilatus@bundestag.de gibt es bestimmt nicht, denn der ist schon tot, der Pilatus).

- E-Mail wird meist von dynamischen oder Einwahl-IP-Adressen verschickt.
- Der Header ist gefälscht (z.B. zusätzliche "Received from"-Zeilen).
- Die E-Mail enthält einen Satz wie "this is not spam" (das ist logisch, denn wenn es wirklich kein Spam wäre, würde man diesen Satz nicht verwenden).
- Die E-Mail enthält einen Link oder eine Antwort-Adresse zum angeblichen Entfernen der eigenen Adresse aus der Spamliste (was die braven Spammer bestimmt auch sofort tun würden).

Beispiele für Spam:

From: "SHANTILAL6@NETZERO.COM"  
Subject: Want to meet

From: personal\_link20001@yahoo.co.jp  
Subject: FROM MISS RITA UMU

From: Dringend  
Subject: Sie haben Gewonnen

From: Anwalt  
Subject: Sehr Wichtig

From: Bank  
Subject: Rechnung

From: "Linda Rowland"  
Subject: Forget about SEX problems!

From: ALEWIS793@houston.rr.com  
Subject: RESPONSE NEEDED

From: PROF CHARLES SOLUDO  
Subject: URGENT ATTENTION

## Woran merkt man, dass die eigene Adresse in den Datenbanken der Spammer gespeichert ist?

1. Klar: In der eigenen Mailbox findet sich Spam.
2. Man findet dutzende bis tausende E-Mails in der Mailbox mit Fehlermeldungen, dass eine E-Mail nicht zugestellt werden konnte. Aber man hat keine E-Mails an die betreffenden (unbekannten) Empfänger verschickt. Das war ein Spammer. Und er hat **Ihre** Adresse als Absender genommen. Das ist „collateral spam/backscatter“. Und außerdem ziemlich gemein.

## Was kann man tun, wenn Spammer die eigene Adresse gespeichert haben?

In letzter Konsequenz nur eins: Die **E-Mail-Adresse löschen bzw. deaktivieren** und nie mehr verwenden.

Aus den Datenbanken der Spammer kommt man praktisch nie mehr heraus. Auch wenn Sie damit leben können, gelegentlich oder immer häufiger unerwünschte Werbung für Penisverlängerungen zu bekommen: Falls Sie Opfer von *collateral spam* werden, bekommen Sie innerhalb weniger Minuten bis zu mehreren tausend E-Mails (bounces). Eventuell erhalten Sie auch noch böse Anrufe und einen Brief von einem Anwalt, der den Häuptling einer kleinen christlich-orthodoxen Sekte aus Nordfriesland vertritt und sie verklagt, weil sie der 13-jährigen Pfarrerstochter den Besuch von „Teufels Sex-Seiten“ empfohlen haben sollen.

Falls Sie wirklich nicht so konsequent sein wollen, sollten Sie wenigstens die folgenden Tipps befolgen.

## Wie kann man vorbeugen?

1. **Legen Sie sich keine zu kurzen und zu einfachen E-Mail-Adressen zu.** *meier@gmx.de* ist zu einfach. *Gmx.de* und *meier* sind in den Spammer-Datenbanken zuhauf vorhanden.
2. **Geben Sie Ihre E-Mail-Adresse nicht heraus.** Freunde sollen Ihre E-Mail-Adresse erfahren dürfen, aber seien Sie sonst vorsichtig.
3. **Geben Sie Ihre Adresse auf Ihrer Homepage nur verschlüsselt preis oder nutzen Sie besser gleich Kontaktformulare.** Spammer nutzen *Harvester*-Programme, um an E-Mail-Adressen von Webseiten zu kommen. "Verschlüsseln" heißt, dass man z.B. "meier (bei gmx (Punkt) de)" schreibt. **Vergessen Sie auch Javascript zum Entschlüsseln.** Das können Bots und Harvesters.
4. **Legen Sie sich idealerweise für unterschiedliche Gelegenheiten verschiedene Adressen zu.** Beispiele: *einkaufen-bei-OTTO@meinedomain.xx*, *yahoo-mailingliste@meinedomain.xx*. Diese zweckgebundenen Adressen können Sie auch alle in Ihre Mailbox weiterleiten lassen.
5. **Nutzen Sie eine eigene Domain.** So können Sie selbst jederzeit beliebig neue Adressen anlegen. Eine eigene Domain gibt es schon für wenige Euro jährlich. Falls Sie sogar einen eigenen Mailserver haben, konfigurieren Sie den bitte richtig: Kein Open Relay und keine Bounces (NDR). Außerdem können Sie so zur Spamschleuder werden: Als Backscatterer.
6. **Nutzen Sie bei Ihrer eigenen Domain keine Adress-Wildcards (catchall).** Wenn Sie bei Ihrer eigenen Domain den Empfang für alle Adressen aktiviert haben, so werden Sie mit Sicherheit schnell Spam für *krxlbrxl@meinedomain.xx* erhalten. Aktivieren Sie nur die Adressen bei Ihrer Domain, die Sie auch wirklich verwenden wollen.
7. **Wenn Sie keine eigene Domain haben und Ihre Mailbox bei einen großen Mailprovider**

**ist: Nutzen Sie nur lange E-Mail-Adressen.** Es werden auch Adressen wie *hans-peter.-meier@gmx.de* auf den Spammerlisten sein. Auch wenn Sie diese Adresse neu registriert haben: Vielleicht gehörte sie vorher jemand anderem, der sie ja wegen Spam abgeschaltet hat. Und Sie bekommen jetzt den Spam, den er schon nicht haben wollte. Herzlichen Glückwunsch.

8. **Wenn Sie schon in der Übersicht Ihrer Mailbox E-Mails mit obskurem Absender oder Betreff sehen: Nicht anschauen, direkt löschen.** Vielleicht enthält die E-Mail ja auch einen Wurm, einen Virus oder sonstige Malware. Wenn Ihnen der Absender unbekannt ist und der Betreff nicht eindeutig ist oder verdächtig erscheint, dann sind Sie mit Löschen auf der sicheren Seite.
9. **Keine "Remove me"-Links anklicken.** Falls Sie dann doch eine E-Mail geöffnet haben sollten, die sich dann als Spam offenbart, dann kann eine Antwort-Adresse oder ein Weblink zum Anklicken enthalten sein, mit dem man sich angeblich aus der Spammerliste austragen kann. Tun Sie es nicht. Für den Spammer ist es dann nur eine Bestätigung, dass die E-Mail-Adresse existiert und dass die E-Mail angekommen ist.
10. **Tragen Sie sich nicht in Robinson-Listen ein.** Robinson-Listen enthalten Adressen von Personen, die keine Werbung erhalten wollen. Das funktioniert vielleicht bei *snail mail* (Gelbe Post), aber nicht bei der internationalen Email-Spammer-Mafia. Eine seriöse Firma verschickt kein Spam und interessiert sich nicht für diese Listen. Eine unseriöse Firma, die Spam verschickt, stört sich nicht an den Listen. Und ein Spammer interessiert sich für solche Listen, aber nur, um die Adressen in seine Datenbank aufnehmen zu können. Also, was soll das?
11. **Verwenden Sie keine Spamfilter!** Filter für Spam sind gegen landläufiger Meinung das Sinnloseste, was es nach Robinsonlisten für E-Mail gibt. Warum?

1. Wenn Sie Spam bekommen, ist schon bei einem der oben erwähnten Punkte etwas falsch gelaufen. Korrigieren Sie das. Gehen Sie direkt dorthin, gehen Sie nicht über Los und ziehen Sie keine 4000 Mark ein.
2. Wenn Ihre empfangene E-Mail nach irgendwelchen Kriterien sortiert/gefiltert wird, so ist es ja schon zu spät: Der Spammer hat seinen Mist bereits bei Ihnen abgeladen.
3. Ihre Filterkriterien bedürfen ständiger Anpassung, was Sie selbst tun (müssen). Das ist ein falscher Ansatz: Es ist besser, dass der Mailserver solche Arbeit macht, bevor alle seiner User das Gleiche machen.
4. Filterkriterien, die auf dem Inhalt basieren, sind nicht sehr sinnvoll. Einerseits muss immer mehr Aufwand betrieben werden (Text, dann GIFs, PDF und inzwischen auch MP3), andererseits gibt es wesentlich strengere Kriterien wie die IP-Adresse.
5. Was macht Ihr Filter mit den aussortierten E-Mails? Die kommen in einen Ordner mit Namen "Spam". Was machen Sie mit den E-Mails? Wenn Sie sie einfach löschen, dann löschen Sie vielleicht auch irrtümlicherweise als Spam erkannte E-Mails von Ihrem Freund Hein Schlau („false positives“). Wenn Sie sie nicht einfach löschen, sondern erst kontrollieren, ob Sie löschen können: Wofür betreiben Sie dann eigentlich den Aufwand mit dem Filter?

**12. Blocken Sie Spam, statt zu filtern.** Das Blocken oder Abweisen geht schneller und ist die einzig sinnvolle Methode, mit Spam umzugehen. Und Hein Schlau wird sich auch freuen: Er bekommt wenigstens eine Fehlermeldung und ärgert sich nicht, dass Sie wochenlang nicht auf die E-Mail antworten.

Weitere Infos: <http://de.wikipedia.org/wiki/Spam>  
Quelle: <http://www.tuxad.com/spam.html>