

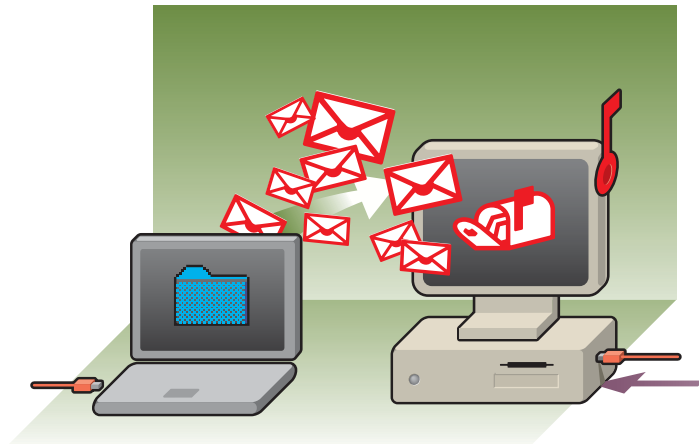
## Zusammenfassung

Dieser Begriff stammt aus dem Internet-Bereich (genauer gesagt aus dem Usenet), wo er massenhaft an verschiedene Newsgroups versendete Nachrichten bezeichnete. Es handelte sich dabei meistens um Werbemeldungen, die nichts mit den betroffenen Newsgroups zu tun hatten.

Da diese Art von Werbung meistens per E-Mail verschickt wird, bezeichnet der Begriff „Spam“ oder „Junk-Mail“ mittlerweile auch unerwünschte Massen-E-Mails. Technisch genauer müsste man von UBE (Unsolicited Bulk E-Mail) oder UCE (Unsolicited Commercial E-Mail) sprechen.

## Inhalt

- 1 Was ist das? →
- 2 Wer führt das Spamming durch? →
- 2 Wer führt das Spamming durch? →
- 4 Vorbeugende Maßnahmen →
- 5 So werden Sie durch die Zugangsanbieter geschützt? →
- 6 Spam in Zahlen →



### 1 Was ist das?

Es gibt keine offizielle Definition für den Begriff „Spam“. Das Wort bezeichnete ursprünglich eine in Konserven verkaufte englische Frühstücksfleisch-Marke. In einem ihrer berühmtesten Sketche hat die Monthly Python-Truppe ohne Unterlass das Wort „Spam“ in einem Gespräch wiederholt und den Begriff somit zum Ausdruck für Missfallen geprägt.

Heute wird das Wort „Spam“ allgemein verwendet, um eine an eine Vielzahl von Empfängern verschickte E-Mail zu bezeichnen. Sie stellt also für die Empfänger ein Ärgernis dar.

Diese E-Mails kosten den Versender, der nur eine Meldung an eine Vielzahl von Empfängern verschickt, praktisch nichts. Dagegen kann sie die Empfänger in Bezug auf die Verbindung und das Datenübertragungsvolumen einiges kosten. Man kann von einer wahren Verschwendung der Bandbreite und des Speicherplatzes für die Netzwerkverwalter und Nachrichtenserver sprechen. Aber auch für die Empfänger der Spams (Einzelpersonen oder Unternehmen) stellt dies eine Verschwendung der für das Downloaden, Sortieren und Löschen der empfangenen Spams aufgewendeten Zeit dar. Außerdem besteht immer die Gefahr, eine E-Mail zu löschen, bei der es sich nicht um eine Spam-Mail handelt.

### 2 Wer führt das Spamming durch?

Jeder ein bisschen ..., von Einzelpersonen über Werbetreibende bis hin zu den Marketingabteilungen der Unternehmen, bei denen es sich um die ursprünglichen Absender von Spams handelt und deren Ziel es ist, für ihre Produkte und Dienstleistungen zu werben oder Internet-Surfer auf ihre

Webseite zu locken. Dennoch muss zwischen Spams, die informativen oder werbenden Charakter haben, und Spams, deren einziges Ziel die Beeinträchtigung des E-Mail-Systems ist, unterschieden werden.

## 3 Wie werde ich zum Opfer von Spams

Um zu einem potenziellen Opfer von Junk-Mails zu werden, benötigen Sie lediglich eine E-Mail-Adresse.

### 3.1 Methoden zur Erfassung der E-Mail-Adresse

Absender von Spams verfügen über verschiedene Mittel zur Erfassung Ihrer E-Mail-Adresse im Internet (in Foren, auf Internetseiten, in Diskussionsgruppen etc.). Mithilfe von speziellen Softwareprogrammen (die als „Robots“ bezeichnet werden) werden die verschiedenen Seiten durchsucht und alle dort aufgeführten E-Mail-Adressen in einer Datenbank gespeichert.

Nebenbei erwähnt: Bill Gates erhält pro Tag 4 Millionen E-Mails, die meisten davon Spams, aber nur 10 Mails gelangen tatsächlich in seine Inbox. Alle anderen Mails werden durch Anti-Spam-Lösungen herausgefiltert. (Quelle: BBC News – 18. Nov. 2004)

#### → Ihre E-Mail-Adresse wurde verkauft.

Durch den Weiterverkauf seiner Verteilerliste an einen Dritten, der diese wiederum an einen anderen weiterverkauft etc., hat Ihr Internet Provider die Verteilung Ihrer Adresse an eine Vielzahl von Unternehmen und Einzelpersonen im Internet ermöglicht. Achtung, dieser Vorgang ist legal, wenn Sie akzeptiert haben, dass Ihre Adresse verbreitet werden darf.

#### → Sie haben die Adresse im Internet veröffentlicht

Haben Sie Ihre E-Mail-Adresse auf Ihrer persönlichen Homepage angegeben? Haben Sie Ihre Adresse in Diskussionsforen im Internet oder in Newsgroups mitgeteilt? Seien Sie sich bewusst, dass es Softwareprogramme gibt, die automatisch so veröffentlichte E-Mail-Adressen erfassen können. In all diesen Fällen kann Ihre E-Mail-Adresse bereits in Adressdateien enthalten sein.

#### → Sie haben einer Webseite Ihre E-Mail-Adresse mitgeteilt.

Durch eine Bestellung auf einer e-Commerce-Webseite, durch das Abonnement von Diensten auf einer Internetseite oder durch die Eintragung in einer E-Mail-Verteilerliste haben Sie zwangsläufig Ihre E-Mail-Adresse mitgeteilt. Wenn Sie vergessen haben, das kleine Kästchen unten im Formular zu aktivieren, haben Sie die Verbreitung dieser Adresse genehmigt.

#### → Ihre Adresse wurde zufällig generiert.

Nehmen Sie einerseits die Listen mit den gängigsten Vor- und Nachnamen und andererseits die Liste der bekannten Zugangsanbieter, und nutzen Sie dann alle möglichen Kombinationen aus (Vorname.Name, Name.Vorname, NVorname etc.) – so können Sie Hunderttausende E-Mail-Adressen generieren, die mit hoher Wahrscheinlichkeit wirklich existieren! Und genau das machen einige Absender von Spams.

### 3.2 Beispiel für eine Spam-E-Mail:

Objet : Make Easy Money from Home !

Brand New - Ultimate Business Opportunity !  
Just Released World Wide !

Want an income independant of your job ?  
Want To Be Your Own Boss and Own Your Own Business ?  
Want To Easily make \$200 - \$1,000 per day... paid daily ?  
Want To Earn Long Term Residual Income for Life ?  
Want Unlimited Leads to Start Earning Big Immediately !  
Click Here to learn more !

## 4 Vorbeugende Maßnahmen

### 4.1 Antworten Sie vor allem nicht auf eine Spam-Mitteilung

Absender von Spams verwenden normalerweise falsche Absenderadressen. Daher ist es völlig nutzlos, auf Spams zu antworten. Außerdem informieren Sie den Absender, wenn seine Adresse richtig ist, nur darüber, dass Ihre E-Mail-Adresse wirklich existiert, und Sie werden noch mehr Spams erhalten.

### 4.2 Die beste Lösung bleibt die Vorbeugung

→ Verwenden Sie niemals öffentlich die von Ihrem Zugangsanbieter oder Unternehmen zugewiesene E-Mail-Adresse. Nutzen Sie diese Adresse nur für einen beschränkten Freundes- oder Kollegenkreis, dem Sie voll und ganz vertrauen können.

→ Überprüfen Sie, dass Ihre E-Mail-Adresse nicht ohne Ihr ausdrückliches Einverständnis verbreitet wird. Einige Zugangsanbieter oder Dienstleister können Sie automatisch in ein Webverzeichnis eintragen.

→ Vermeiden Sie möglichst die Preisgabe Ihrer E-Mail-Adresse in Foren oder auf Internetseiten.

→ Erstellen Sie eine oder mehrere „Mülleimer-Adressen“, die ausschließlich für die Eintragung auf nicht vertrauenswürdigen Webseiten dienen.

→ Geben Sie im Zweifelsfall eine falsche Adresse ein oder verschleiern Sie Ihre wirkliche Adresse beispielsweise mithilfe der Spam Safe Notation.

#### 4.3 Verwendung einer Anti-Spam-Software

Es gibt Anti-Spam-Maßnahmen, die eine Erkennung und gegebenenfalls das Unterdrücken von unerwünschten Meldungen aufgrund von fortgeschrittenen Regeln ermöglichen. Im Allgemeinen wird zwischen zwei Anti-Spam-Softwareprogrammen unterschieden:

- ➔ Die Client-seitigen Anti-Spam-Programme, die sich auf der Ebene des E-Mail-Clients befinden. Es handelt sich hierbei üblicherweise um Systeme, die über Filter verfügen, die

eine Erkennung von Spams auf der Grundlage von vordefinierten Regeln oder eines Lernprozesses ermöglichen (Junk-E-Mail in Outlook 2003).

- ➔ Die Server-seitigen Anti-Spam-Programme, die eine Filterung der Mails vor der Bereitstellung für die Empfänger ermöglichen. Diese Art des Spam-Schutzes ist bei weitem besser, da sie bereits frühzeitig unerwünschte E-Mails aufhalten und somit die Verstopfung der Netzwerke und Mailboxen der Internetnutzer verhindern.

## 5 So werden Sie durch die Zugangsanbieter geschützt

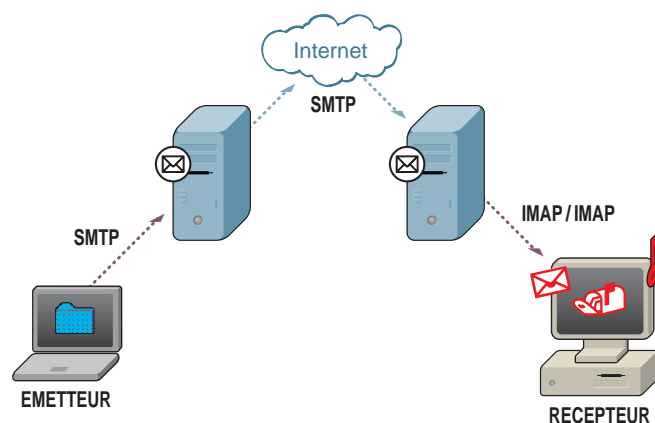
Die Internet Service Provider sind sich natürlich darüber bewusst, dass die Junk-Mails zukünftig zu einem Problem in Bezug auf das Vertrauen in die technologische Lösung der elektronischen Nachrichtenübermittlung darstellen könnten. Aus diesem Grund implementieren die meisten Dienstleister Lösungen, deren Ziel das Herausfiltern unerwünschter Mails ist (beispielsweise durch die Verwendung schwarzer Listen).

Die Qualität der Anti-Spam-Lösung kann sowohl für berufliche als auch private Anwender zu einem echten Unterscheidungskriterium zwischen den Dienstleistern werden.

Diese Technik ist auch auf PC-Ebene anwendbar, sie erfordert jedoch ein gewisses Know-how und eine konstante Wartung der Einstellung seitens des Anwenders, um wirklich effektiv zu sein.

#### 5.1 Wie funktioniert E-Mail?

Eine E-Mail ist ein Datenstrom, der von einem Absender über dazwischenliegende E-Mail-Server oder -Relays an einen Empfänger übertragen wird. Das folgende Schema veranschaulicht diesen Ablauf:



Bei den Sende- und Empfangsvorgängen werden mehrere Kommunikationsprotokolle verwendet.

Bekanntlich ist ein Protokoll eine Form der Kommunikation, die zwischen zwei Organisationen festgelegt wird und es ihnen erlaubt, Informationen auszutauschen. Es handelt sich dabei um nicht mehr und nicht weniger als eine gemeinsame Sprache, die zwei Organisationen (in der Regel ein Client und ein Server) verwenden, um eine bestimmte Aufgabe, hier den Versand einer E-Mail, durchführen zu können

Das für den Versand einer E-Mail verwendete SMTP-Protokoll speichert beispielsweise die Liste der Server, die die E-Mail weitergeleitet haben.

#### 5.2 Prinzip schwarzer Listen

Spam-E-Mails werden häufig mit einer falschen Absenderadresse versendet. Im Allgemeinen akzeptieren die weitersendenden Server (E-Mail-Server) als Absender keine Adressen, die nicht ihrer Domain entsprechen (so akzeptieren die P&T beispielsweise nur Adressen mit der Endung @pt.lu). Bestimmte E-Mail-Server führen jedoch keine Kontrolle durch (sie werden als "Open-Relay-Server" bezeichnet). Diese Server werden daher häufig für den Versand von Spam-E-Mails genutzt.

Im Internet gibt es Listen, in denen die Erzeuger und "Relais" von Spams aufgeführt sind. Letztgenannte sind Mail-Server im Internet, die den Versand von Spams ermöglichen. Sie werden anhand Ihrer IP-Adresse und Ihrer Domain identifiziert. Diese Listen werden anschließend verwendet, um die E-Mail-Server so zu konfigurieren, dass sie diese Informationsquellen abfragen und eine Entscheidung bezüglich der Mails treffen, die von in diesen schwarzen Listen aufgeführten Absendern stammen. Die Abfrage erfolgt meistens per DNS-Request (Internetdienst, der die Konvertierung von Domainnamen in IP-Adressen und umgekehrt gewährleistet).

Wenn die Antwort eine als Absender von Spams verzeichnete Quelle angibt, muss der Server nur noch die Mail herausfiltern. Es spricht nichts dagegen, nachfolgend andere Filter- und Analysetechniken wie beispielsweise einen Inhalts- oder Betreffzeilenfilter auf die akzeptierten Mails anzuwenden.

### 5.3 Typen schwarzer Listen

Eine erste Unterscheidung kann zwischen den „lokalen“ schwarzen Listen (zum Beispiel auf Unternehmens- oder Anwenderebene) - Local Deny Lists genannt - und den öffentlichen schwarzen Listen, die per Fernabfrage abgerufen werden, gemacht werden.

Die Verwendung lokaler schwarzer Listen erfordert eine permanente Wartung sowie ein entsprechendes Know-how seitens des Anwenders. Leider erleichtern die standardmäßigen E-Mail-Tools in keinsten Weise deren Verwaltung.

Die öffentlichen Listen sind unter dem Namen DNSBL (DNS Blackhole List) oder einfach „schwarze Listen“ bekannt. Einige sind kostenlos, während andere als bezahlter Dienst angeboten werden. Einige dieser schwarzen Listen haben sich entsprechend der Kriterien, die die Eintragung in die Liste bestimmen, oder entsprechend ihrer Funktionsweise spezialisiert. Die bekanntesten dieser Listen sind Spamcop, MAPS, DSBL, SPEWS oder ORDB.

### 5.4 Vor- und Nachteile

Die Filterung der Absender verhindert, dass die Spam-Mail an den Servern ankommt, wenn die Filterung auf der Ebene der Internet Service Provider erfolgt. Hieraus ergeben sich Einsparungen in Bezug auf die Bandbreite, den Speicherplatz und die CPU-Leistung. Außerdem erfordert diese Technik bei Abfrage einer lokalen Datenbank sehr wenig Ressourcen und ist folglich sehr schnell. Aus diesen Gründen wurde und wird auch heute noch die Filterung per Liste vielfach von den Internet Service Providern genutzt. Häufig löschen Letztgenannte einfach die von Absendern auf den schwarzen Listen stammenden Meldungen.

### 5.5 Einfluss der schwarzen Liste auf den Arbeitsplatz

Die Verwendung schwarzer Listen durch die Zugangsanbieter ist häufig an eine andere Filtertechnik gekoppelt. Es handelt sich hierbei um die Benutzerauthentifizierung während des Mail-Versands.

Diese Technik verhindert die Ausgabe des Domainnamens des Zugangsanbieters, der den E-Mail-Server im „Open-Relay“-Modus nutzt (von Hackern und Absendern von Spams verwendete Technik, um sich eine Identität oder Domain anzueignen und so die Spam-Mails weiterzuleiten). Diese Vorsichtsmaßnahme soll verhindern, dass die Domain des Zugangsanbieters nicht in den schwarzen Listen deklariert wird, weil sie von Hackern genutzt wird.

Bei dieser Technik muss die Authentifizierung bei der Parametrierung der Benutzerkonten in der E-Mail-Software (beispielsweise MS Outlook) berücksichtigt werden. Der E-Mail-Server des Zugangsanbieters lässt nur die Verbindung von durch ihn selbst authentifizierten Benutzern zu.

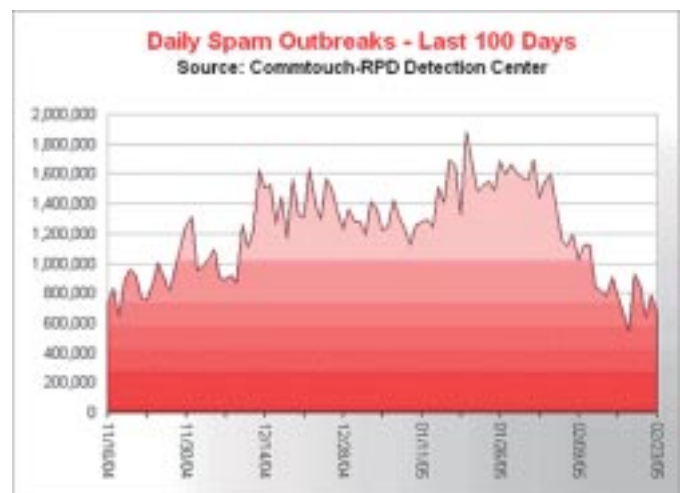
Die Verwendung dieser Authentifizierung führt zu Problemen, wenn der Zugriff auf die E-Mail über einen anderen Zugangsanbieter (Roaming) erfolgt, der die Authentifizierung während des E-Mail-Versands nicht unterstützt. Dies kann zur Folge haben, dass kein Versand von E-Mails möglich ist. Da der E-Mail-Empfang nicht durch den Open-Relay-Mechanismus betroffen ist, ist dieser weiterhin möglich.

## 6

## Spam in Zahlen

### 6.1 Einige Zahlen

Rang	Land	Prozent
1	USA	56.7 %
2	Kanada	6.8 %
3	China	6.2 %
4	Südkorea	5.8 %
5	Niederland	2.1 %
6	Brasilien	2.0 %
7	Deutschland	1.8 %
8	Frankreich	1.5 %



## Nützliche Links:

- ➔ <http://spambayes.sourceforge.net/>  
Anti-Spam-Plug-in für Microsoft Outlook 2000/XP unter Windows, aber auch für die Betriebssysteme Linux und Mac.
- ➔ [http://prdownloads.sourceforge.net/mmm3/magic-2.94b10.zip?use\\_mirror=ovh](http://prdownloads.sourceforge.net/mmm3/magic-2.94b10.zip?use_mirror=ovh)  
ermöglicht die Überprüfung des Inhalts Ihrer Mailbox direkt auf dem Server und das Löschen möglicher Spam-Mails.
- ➔ <http://spam.abuse.net/>  
hervorragende Webseite zum Thema Spam.
- ➔ <http://www.spampal.org/>  
in der Workstation zu installierende Software, die eine Filterung der empfangenen Mails mithilfe von DNSBL ermöglicht. Die empfangenen Spams werden nicht gelöscht, sondern getagged, indem zur Betreffzeile das Zeichen [SPAM] hinzugefügt wird, um sie leicht per Outlook klassifizieren zu können.