



---

Der Selbstschutz durch strikte Einhaltung von Verhaltensregeln ist der derzeit wirksamste Schutz. Wir wollen Ihnen daher mit dieser Aufstellung eine Hilfestellung geben.

Die Maßnahmen gegen SPAM lassen sich in Vorbeugung und Schadensbegrenzung einteilen. Wir empfehlen vor allem die Regeln zur Vorbeugung. Denn wenn Ihre Email-Adresse einmal bekannt ist, gibt es keine wirkliche "Heilung" mehr, sondern nur noch Bekämpfung der Symptome.

- Grundsätzlich gilt: „**Verhalten Sie sich passiv!**“
  - Öffnen Sie nur Emails und Dateianhänge von Personen, die sie kennen und von denen Sie auch ein Email mit entsprechendem Anhang erwarten.
  - Öffnen und versenden Sie keine Dokumente im Microsoft Word Format (.doc) per Email. Speichern Sie Ihre Dateien im RTF oder PDF-Format. Damit verhindern Sie die Verbreitung von Makroviren.
  - Kettenemails und unsinnige Emails sofort löschen.
  - Öffnen Sie nie Dateien, welche mehr als eine Dateiendung haben. (Bsp.: beispiel.doc.exe)
  - Meiden Sie Adressverzeichnisse. Email-Dienste bieten bei Anmeldung den Eintrag in virtuelle "Telefonbücher" an. Dabei ist Vorsicht geboten, die Adressen sind dort leicht "abzuholen".
  - Wenn Sie eine Website betreiben, geben Sie dort nicht "offen" (in Textform) Ihre Mailadresse an. Diese können leicht automatisiert ausgelesen werden. Verwenden Sie besser eine Bilddatei mit Ihrer Email-Adresse.
  - Öffnen Sie möglichst keine Emails mit Spam-Inhalt. Diese können Bilder auf einer Website laden oder ein kleines Script enthalten, wodurch der Absender beim Öffnen des Mails über die erfolgreiche Übermittlung informiert wird. Löschen Sie diese Emails, wenn aus dem Absender, oder aus dem Betreff bereits die Email als SPAM eindeutig zu identifizieren ist.
  - Kein seriöses Unternehmen arbeitet mit Spam. Antworten Sie nur, wenn Sie sicher sind, dass es sich um eine vertrauenswürdige Quelle handelt.
  - Absender-Adressen können gefälscht sein, sodass der Ursprung der Spam-Mail nur mühsam gefunden werden kann. Oft wechseln die Spammer den Internet- Service-Provider, was die Suche nach dem Verursacher zusätzlich erschwert.
  - Oft ist es für Spam-Mail-Empfänger verwirrend, dass seine Adresse nicht in der Empfängeradresse aufgeführt ist: Die wirklichen Empfängeradressen werden in einer Mailingliste oder als Bcc:-Adresse versteckt.
  - Achten Sie darauf, wo Sie Ihre Email-Adresse hinterlassen. Seien Sie vorsichtig, wenn Sie Ihre Email-Adresse öffentlich nutzen wollen, beispielsweise in Diskussionsforen oder auf Homepages (Gästebücher). Spammer generieren einen Großteil ihres Adressbestandes, in dem sie mit Robotern Websites und News-Gruppen vollautomatisch nach Email-Adressen durchsuchen. In vielen News-Gruppen ist die Angabe einer gültigen Email-Adresse erforderlich, überlegen Sie sich deshalb für diesen Zweck eventuell die Anlage einer Email-Adresse bei einem Mail-Dienstleister oder überlegen Sie gegebenenfalls, in dieser News-Gruppe schlicht nicht mitzudiskutieren.
-

- Beantworten Sie nicht Spam. In der Regel werden die meisten Spam-Mails ohne die richtige Absenderadresse ausgeliefert, weil die meisten Spammer nicht sonderlich daran interessiert sind, die erbosten Antworten vieler Opfer zu lesen. Beachten Sie deshalb, dass Sie mit einer direkten Antwort auf eine Spam in den seltensten Fällen den Spammer direkt erreichen, sondern meist eine unschuldige Person, die das Pech hat, dass ihre Email-Adresse als Absender für eine Spam-Aktion missbraucht wurde.
- Klicken Sie nicht auf Hyperlinks, die in Spam-Mails beworben werden. Oft sind Hyperlinks, die in Spam-Mails angegeben sind, personalisiert und ermöglichen nach einem Klick den Rückschluss, welcher Spam-Empfänger genau die Spam gelesen und den Hyperlink betätigt hat. Ein Spammer könnte auf diese Weise die Besucher ermitteln und diese mit noch mehr Spam "beglücken".
- Seien Sie misstrauisch gegenüber Abmeldeoptionen. In fast jeder Spam wird meist am Ende der Mail versichert, dass man sich über einen bestimmten Hyperlink abmelden, also seine Email-Adresse angeblich aus dem Verteiler entfernen lassen kann, um zukünftig keine Mails von diesem Anbieter zu erhalten. Die Erfahrung zeigt jedoch, dass diese Abmeldeoptionen gar nicht zum Abmelden, sondern zum Verifizieren von Email-Adressen genutzt werden. Die Idee, die dahinter steckt, ist perfide: Ein Spammer geht davon aus, dass eine so angegebene Email-Adresse mit hoher Wahrscheinlichkeit funktionsfähig sein dürfte, weshalb so eine vermeintliche Abmeldung letztendlich erheblich mehr Spam zur Folge hat.
- Bestellen Sie nicht bei Spammern. Bei einem Spammer nicht einzukaufen, ist nicht nur aus moralischen Gründen anzuraten, sondern auch aus Gründen der Sicherheit. Machen Sie sich klar, dass ein Spammer, wenn er sich schon nicht darum schert, an wen er seine Mails sendet, sich auch nicht sonderlich um die Sicherheit des Käufers kümmern dürfte. Die meisten Websites von Spammern enthalten, gerade deshalb, weil sie ständig ihren Standort wechseln, keinerlei Verschlüsselungsmöglichkeiten. Zudem ist das Geschäftsgebahren in diesem Milieu alles andere als freundlich.
- Wenn Sie "Bilder" zugeschickt bekommen, seien Sie vorsichtig. Auch wenn das Bild von einer bekannten Quelle stammt. Möglicherweise hat die bekannte Quelle keine Vorsicht walten lassen und schickt Ihnen unwissentlich ein Schadprogramm. Beachten Sie den Grundsatz: Keine Speicherung von Daten ohne Virens Scanner!

Wir müssen mit dieser Art von Mail leben und vermehrt Emails löschen, genauso wie wir Werbung im Briefkasten zum Altpapier werfen.

---