



## Best Practices für die korrekte E-Mail-Kommunikation mit TOPtainer

### SPAM Policy deutsche Version

Welche Dinge muss ich als Postmaster/Mailadmin beachten, um an TOPtainer Mitarbeiter E-Mails zu verschicken?

TOPtainer Mitarbeiter verfügen per Default über einen mehrstufigen und einzeln konfigurierbaren Spamschutz.

Dazu gehören auch individuelle Whitelists bzw. Blacklists. Der User kann selbst entscheiden, ob vom Spamschutz erkannte E-Mails geblockt (bounce bzw. Löschung) oder gefiltert (Zustellung in Spamverdachtsordner) werden.

Davon abgesehen sollten Einlieferer die folgenden Hinweise beachten:

**E-Mails müssen den in RFC 2822 definierten Standards genügen.**

<http://www.rfc-editor.org/rfc/rfc2822.txt>

Die Mail darf nicht direkt an unsere MX-Rechner aus Dialup-Netzen heraus zugestellt werden.

Ein Reverse DNS-Eintrag (FQDN) des einliefernden Servers muss vorhanden sein.

**Ein sinnvolles und plausibles HELO/EHLO im Sinne von RFC 2821 muss gesendet werden.**

<http://www.rfc-editor.org/rfc/rfc2821.txt>

Wir prüfen auf Wunsch des Kunden die SPF Records. Die Absenderadressen von weitergeleiteten E-Mails müssen daher mittels SRS umgeschrieben werden.

Der einliefernde Server darf kein Open Proxy sein, das heißt, er muss gegen unberechtigten Zugriff geschützt sein.

Im Fehlerfall geben wir immer eine aussagekräftige Fehlermeldung im SMTP-Dialog zurück. Bitte verfolgen Sie im Zweifelsfall Ihr Log zurück bis zum ersten Auftreten eines Fehlers.

Wir prüfen verschiedene etablierte RBLs. Sollte eine davon zutreffen, gibt der SMTP-Dialog weitere Auskunft.

Für Massenmail-Versender gilt insbesondere Folgendes:

Der Versender muss E-Mail-Adressen sofort aus seinen Versandlisten entfernen, wenn nach dem Versenden an diese Adressen Hard-Bounces erfolgen.

Werden Zustellversuche an zahlreiche unbekannte (oder mittlerweile deaktivierte) TOPtainer Adressaten unternommen, erfolgt eine zeitweise Sperrung.

Wir behalten uns in solchen Fällen auch dauerhafte Sperrungen vor.

Der Auftraggeber, das heißt der Vertragspartner des Versenders, muss für den Empfänger klar erkennbar sein.

Der Empfang der Massen-E-Mail (Newsletter, Werbung etc.) muss für den Empfänger schnell und einfach widerrufbar sein.

Ein entsprechender Link sollte in der E-Mail enthalten sein, ein Widerruf kann aber auch durch Bereitstellung einer gültigen Antwortadresse erfolgen.

Angeforderte Massen-E-Mails sollen gültige, nicht-elektronische Kontaktinformationen des Versenders einschließlich der Telefonnummer und einer realen Anschrift beinhalten.

Ein Mailbombenschutz bei TOPtainer sperrt einliefernde Server zeitweise, wenn zu viele Mails an den selben Empfänger eingeliefert werden.



## Best Practices for correct E-Mail-Communication with TOptainer GmbH

### SPAM Policy - English Version

For administrators: Important facts to recognize when delivering mails to TOptainer employees

TOptainer provides advanced spam protection for its customers.

Many individually configurable modules work together and each user can decide whether spam will be blocked or - which is the default setting - delivered to a special "probably spam" folder. In addition there are user defined whitelists and blacklists.

Besides, the following rules apply:

**E-Mails must comply to the standards described in RFC 2822.**

**<http://www.rfc-editor.org/rfc/rfc2822.txt>**

E-mails should not be delivered from within dialup IP ranges. The default setting for each user is to not accept such e-mail in order to prevent the spreading of mail worms.

The delivering server must have a reverse DNS entry with a fully qualified domain name.

**A complete and plausible HELO/EHLO as described in RFC 2821 must be sent.**

**<http://www.rfc-editor.org/rfc/rfc2821.txt>**

We do check the sending server for SPF compliance if the user hasn't disabled this setting. The addresses of forwarded e-mail therefore **MUST** be rewritten using SRS standards.

The communicating server must not be an open proxy and must be protected against unauthorized access.

In case of any error we ALWAYS provide an error message in the SMTP dialog which clearly indicates the source of the problem. Please check your server logs if you experience problems.

In case of reoccurring errors it is useful to identify the very first instance when the error occurred.

We check several well established RBLs. Should one of them match our SMTP answer will tell you which, why and what to do.

Particularly mass mailers should consider the following:

You must immediately remove addresses from your mailing lists that hard bounce.

If too many delivery attempts to unknown or deactivated addresses occur the sending server will be banned for a certain time period.

TOptainer might decide to ban a server permanently if this behaviour persists.

The sender's customer (if sending mail on a contract basis) must be clearly identifiable in the "from" field of any advertising mail.

Mass mailings must be easily revocable for the receiver. An appropriate link should be in each mail.

Mass mailers may also provide a valid answer address the receiver can use to complain or to cancel his subscription.

Requested mass mailings should contain non electronic contact information of the sender, including postal address and a telephone number.

We use mail bomb protection. If one server tries to deliver too many mails to one receiver it will be banned temporarily.