

mandem eintraf, die Adresse also wirklich genutzt wird und er Sie weiterhin bombardieren kann.

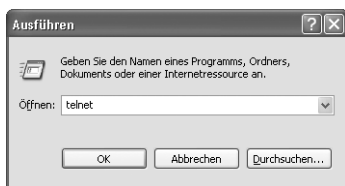
Der Fachbegriff für diese in der EU und anderen Staaten eigentlich vorgeschriebene Funktion heißt Opt-Out: Solange Sie nichts von sich hören lassen, dulden Sie den Empfang der Werbung. Erst wenn Sie die Nase voll haben, lassen Sie sich aus der Empfängerliste austragen. Mit Opt-In ist genau das Gegenteil gemeint: Bevor Sie die erste Werbebotschaft bekommen, müssen Sie dazu Ihre Einverständniserklärung abgeben. Oft ist das ein unscheinbares Häkchen bei der Anmeldung zu irgendeinem Angebot. Natürlich ist es schon aktiv, denn vielleicht übersehen Sie es ja und dann haben Sie ganz unbewusst die Opt-In-Option wahrgenommen und freuen sich über den vollen Posteingang – eigentlich müsste man fast schon wieder von Opt-Out sprechen. Dass sich die Anbieter auch nicht immer an die Wahl des Besuchers halten, zeigt der bereits oben erwähnte Bericht des Center for Democracy & Technology.

7.2 Wie die Spammer anonyme E-Mails verschicken

Damit ein Spammer nicht in der Flut von Beschwerden erstickt, die sein Werbemüll verursacht, wird oft auf ein altes Verfahren zurückgegriffen, um E-Mails anonym und auch noch mehr oder weniger kostenlos zu verschicken. Die meisten Spammer sind nämlich gar nicht über die Absenderadresse der E-Mail erreichbar, da diese einfach ausgedacht wurde. Weil außerdem alle seriösen Serviceanbieter im Internet allergisch auf Spam reagieren und Dienstleister umgehend boykottieren, die das Verschicken von Spam-E-Mails zulassen, kann ein Spammer auch nicht einfach von zu Hause aus arbeiten. Dass es trotzdem immer mal wieder Spammer gibt, die Ihren AOL-Account o. Ä. missbrauchen, zeigen die Beiträge in der Newsgruppe *de.admin.net-abuse.mail* (<http://groups.google.com/groups?group=de.admin.net-abuse.mail>), in der eifrig über Inhalt und Abwehr von Spam diskutiert wird.

Wie einfach Sie selbst eine E-Mail anonym verschicken können, zeigt das folgende Beispiel, bei dem eine Schwäche des **Simple Mail Transfer Protocol** (SMTP) ausgenutzt wird: Das Protokoll ist für die Annahme und den Transport von E-Mails zuständig und überprüft bei zu lascher Konfiguration nicht die Berechtigung desjenigen, der dem System eine E-Mail unterschieben will.

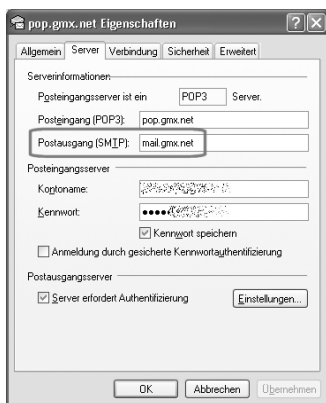
- 1 Starten Sie über *Start/Ausführen* und die Eingabe von *telnet* die Terminalemulation Telnet, mit der Sie auf entfernte Rechner über das Internet zugreifen können, um dort dann Befehle auszuführen.



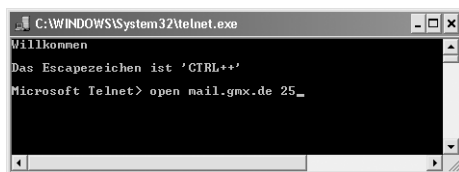
INFO Straftbar oder nicht?

Um keine rechtlichen Schwierigkeiten zu bekommen, wird in diesem Selbsttest mit einem Account gearbeitet, der Ihnen gehören muss. Anstatt also einen anonymen Open Relay zu benutzen, werden Sie sich regulär anmelden – genauso wie es auch Ihr E-Mail-Programm macht, wenn dieses E-Mails abrufen. Die E-Mail ist dann nicht anonym. Es kann allerdings sein, dass Ihr Provider den folgenden Zugang nicht gestattet und Sie dann nicht weiterkommen.

- 2 Schauen Sie in Ihrem E-Mail-Programm nach, wie der von Ihrem Anbieter benutzte SMTP-Server heißt. Bei Outlook Express finden Sie die Angabe auf der Registerkarte *Server* im Menü *Extras/Konten*. Um dies zu sehen, müssen Sie im Fenster *Internetkonten* auf der Registerkarte *E-Mail* Ihr Konto auswählen und dann *Eigenschaften* anklicken.



- 3 Im Telnet-Fenster geben Sie an der Eingabeaufforderung den Befehl `open <SMTP-Server> 25` ein und drücken **Enter**. Dadurch öffnen Sie eine Verbindung zu dem Server über den Standard-SMTP-Port, wie er auch auf Seite 45 genannt wird.





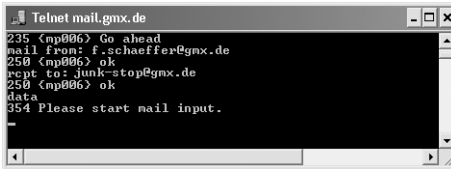
```
Telnet mail.gmx.de
235 (mp006) Go ahead
mail From: f.schaeffer@gmx.de
250 (mp006) ok
```

- 10** Den Empfänger benennen Sie mit *rcpt to: <E-Mail-Adresse>*. Um Ärger zu vermeiden, geben Sie hier auch Ihre eigene Adresse ein. So schicken Sie sich selbst die Testnachricht.



```
Telnet mail.gmx.de
235 (mp006) Go ahead
mail From: f.schaeffer@gmx.de
250 (mp006) ok
rcpt to: junk-stop@gmx.de
250 (mp006) ok
```

- 11** Geben Sie jetzt *data* ein, um die Eingabe der eigentlichen Nachricht zu beginnen.



```
Telnet mail.gmx.de
235 (mp006) Go ahead
mail From: f.schaeffer@gmx.de
250 (mp006) ok
rcpt to: junk-stop@gmx.de
250 (mp006) ok
data
354 Please start mail input.
```

- 12** Anschließend können Sie beliebigen Text eingeben. Wenn Sie als Erstes *subject: <Betreff>* eingeben, können Sie auch noch die Betreffzeile der E-Mail angeben. Haben Sie dann die Nachricht eingegeben, schließen Sie die Eingabe ab, indem Sie in einer neuen Zeile am Anfang einen Punkt eingeben und **Enter** drücken.



```
Telnet mail.gmx.de
250 (mp012) ok
rcpt to: junk-stop@gmx.de
250 (mp012) ok
data
354 Please start mail input.
subject: E-Mail schreiben per SMTP
Fast schon Spam: unbedingt kaufen!
.
```

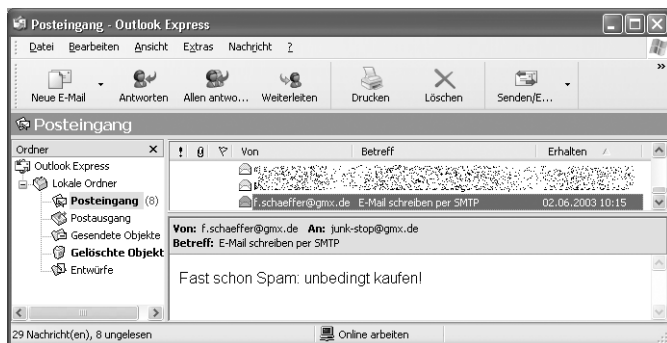
INFO Sonderzeichen sind heikel

Die meisten SMTP-Server basieren auf UNIX und kommen deshalb nicht mit den Sonderzeichen von Windows zurecht. Aus diesem Grund können Sie oft nicht **Entf** benutzen und sollten auch auf Umlaute etc. verzichten.

- 13** Mit *quit* beenden Sie die Verbindung zum SMTP-Server und die Nachricht wird verschickt. Sie können jetzt Telnet schließen.



Sobald die Nachricht durch das Internet transportiert wurde (was schnell gehen dürfte, da Sie ja an sich selbst geschrieben haben), können Sie die E-Mail wie gewohnt abrufen und lesen.



Schutz vor Open Relay

Einziges Problem für Spammer ist, dass die meisten Serverbetreiber SMTP natürlich mittlerweile so konfiguriert haben, dass eine anonyme Anmeldung nicht mehr möglich ist und nur E-Mails nach vorheriger Anmeldung entgegengenommen werden. Viele Freemailer nutzen dazu das Verfahren SMTP after POP3: Zuerst müssen Sie Ihre E-Mails abholen bzw. zumindest prüfen, ob welche da sind, wozu das POP3-Protokoll benutzt wird, das Sie am Server authentifiziert. Anschließend können Sie Ihre E-Mails verschicken, was dann via SMTP abgewickelt wird. So geschützt können Sie die meisten Server nicht mehr missbrauchen.

Allerdings gibt es im Internet zahlreiche Listen, in denen Server aufgeführt werden, die die ungeprüfte Annahme von E-Mails zulassen, was Open Relay genannt wird – sei es mit Absicht, weil Spammer geduldet werden, oder aus Unachtsamkeit. Als Gegenmaßnahme erstellt die Open Relay Database (<http://www.ordb.org>) eine schwarze Liste dieser Open Relays. Server, die auf der Liste landen, werden von den meisten seriösen Betreibern gesperrt, sodass E-Mails von diesen Servern herausgefiltert werden. Als allerdings im Mai 2003 der Freemailer GMX mehr oder weniger aus Versehen in dieser Liste auftauchte, wurde deutlich, dass der Schutz auch nach hinten losgehen