

Erste dt. Hoax-Mini-FAQ

Inhalt der Mini-FAQ:

0. Vorwort
1. Worum geht es hier?
2. Fakten, Fakten, Fakten
3. Welche Hoaxes sind bekannt?
4. Wie erkenne ich einen Hoax?
5. Was mache ich, wenn ich eine solche Mail erhalte?
6. Warum soll ich das glauben was hier steht und nicht den Warnungen?
7. Wo erhalte ich weitere Informationen zu diesem Thema?
8. Kostenloser Hoax-Info-Newsletter

0. Vorwort

Diese Mini-FAQ ist die erste Ausgabe einer gekürzten Fassung der Hoax-FAQ. Die Hoax-FAQ ist noch in Bearbeitung und umfaßt weitere, verwandte Themengebiete wie Kettenbriefe und Malware in Attachments. An der Erstellung der Hoax-FAQ wirken weitere Personen mit, die z.T. im 'richtigen' Leben für Antivirus-Firmen arbeiten. Insbesondere sei hier die Virus Help Munich (VHM) erwähnt (<http://www.vhm.haitec.de>). In dieser Mini-FAQ geht es ausschließlich um falsche Viruswarnungen.

1. Worum geht es hier?

Seit Jahren kursieren Warnungen vor (angeblichen) Viren, die sich per E-Mail verbreiten sollen. Diese 'Warnungen' werden meist von gutgläubigen Usern verbreitet, die diese per E-Mail von ihresgleichen erhalten haben. Sie zeigen dabei oft sogar ein Engagement, das man sich sonst nur wünschen könnte, im Glauben, sie täten den Adressaten einen Gefallen, in dem sie sie vor gefährlichen Viren warnen.

Die Empfänger werden aufgefordert, E-Mails, die im Betreff (*subject*) einen der weiter unten genannten Begriffe enthalten, nicht zu lesen sondern sofort zu löschen. Andernfalls würde ein Virus furchtbare Dinge mit dem Rechner des Empfängers anrichten.

2. Fakt ist...

... daß alle diese Warnungen keinen ernstzunehmenden Hintergrund haben (was die Gefährlichkeit der vermeintlichen Viren angeht). Es handelt sich wohl mehr um ein soziologisches Phänomen. Weder die E-Mails noch die Viren, vor denen gewarnt wird, sind jemals irgendwo aufgetaucht. Diese Warnungen werden Hoaxes genannt (Hoax: engl. f. Jux, Scherz; v. lat. *hocus*).

Diese 'Warnungen' stellen die eigentlichen Viren dar, denn sie richten erheblichen Schaden an, in dem sie Menschen verunsichern und Arbeitszeit binden. Außerdem belasten sie durch ihre nicht geringe Zahl das Internet durch nutzlosen Datenverkehr.

Generell werden nie echte Virus-Warnungen auf diese Weise in die weite Welt geschickt!

3. Welche Hoaxes sind bekannt?

Die Zahl der Hoaxes ist nicht gering, die meisten sind letztlich nur Nachahmungen („copycats“) des ersten dokumentierten Hoax „GoodTimes“.

Folgende sind erwiesenermaßen Hoaxes (ohne Anspruch auf Vollständigkeit):

A little girl needs help (4)
A.I.D.S. (1)
AOL4FREE (1)
Baby New Year
Bill Gates(4)
Bloat MPEG Virus
Bud[weiser] Frogs Screensaver (BUDDYLST.ZIP)
Deeyenda
Elvira
GET MORE MONEY Virus Warnung (5)
Ghost
GoodTimes
Irina
Join the Crew
Make Money Fast (4)
Mirabilis ICQ virus
NaughtyRobot
New virus debug device
Nike(4)
(no subject)(3)
Open: Very Cool
Penpal Greetings
PKZIP300 (1)
Red Alert
Returned or undeliverable mail (2)
TimeBomb
Win a holiday

(1) Einige Hoaxes basieren auf (ehemals) realen Gefahren, haben aber ein Eigenleben entwickelt und ihre Ursache um einiges überlebt.

(2) Das ist i.d.R. eine ganz normale Fehler-Nachricht von einem E-Mail-Server.

(3) Das heißt nur, daß der Absender kein Betreff (subject) angegeben hat.

(4) Das ist ein Kettenbrief, kein Hoax, hat aber ähnliche Wirkung.

(5) Warnt vor einem Virus, das aber „nur“ ein Kettenbrief ist.

Eine vollständige Liste kann hier leider nicht wiedergegeben werden. Sie wäre ziemlich lang.

Wenn Sie eine verdächtige E-Mail erhalten, die hier nicht aufgeführt ist, schauen Sie mal bei Barn Owl (<http://www.kumite.com/myths/>) rein.

4. Wie erkenne ich einen Hoax?

- Das Subject (Betreff) enthält oft den Begriff „Virus Warnung“ oder sinnverwandtes.
- Der Adressat wird aufgefordert, die „Warnung“ an möglichst viele Menschen weiterzuleiten.
- Die Wirkung des Virus wird sehr drastisch dargestellt und beinhaltet Dinge, die ein Computer-Virus gar nicht kann (z.B. Hardware beschädigen).
- Häufig wird als Quelle eine namhafte Firma oder Organisation genannt, um die Glaubwürdigkeit zu verbessern.

Keine der genannten Firmen hat tatsächlich jemals Warnungen dieser Art publiziert. Es werden generell nie echte Virus-Warnungen auf diese Weise in die weite Welt geschickt – das sind alles Hoaxes!

5. Was mache ich, wenn ich eine solche Mail erhalte?

Da sind zwei Fälle zu unterscheiden:

5.1. Sie erhalten eine E-Mail mit einer Warnung vor einem Virus:

- Leiten Sie sie auf keinen Fall weiter!
- Löschen Sie sie.
- Verweisen Sie den Absender auf diese FAQ.
- Vergessen Sie dann die ganze Sache – verschwenden Sie keine wertvolle Zeit damit!

5.2. Sie erhalten eine E-Mail, vor der Sie jemand gewarnt hat:

- Lautet das subject „Returned or undeliverable mail“, „(no subject)“ oder so ähnlich, handelt es sich wahrscheinlich um eine normale E-Mail, die Sie lesen sollten.
- Enthält das Betreff dagegen einen der o.g. Begriffe, erlaubt sich wahrscheinlich jemand einen schlechten Scherz mit Ihnen, da die Mails, vor denen gewarnt wird, eigentlich gar nicht existieren.
- Auch hier gilt: Löschen und vergessen.

Und eines noch: Viren können sehr wohl per E-Mail verbreitet werden.

Sie können nämlich im Anhang (*Attachment*) als Teil eines ausführbaren Programms verschickt werden. Hier sei auch auf Macro-Viren hingewiesen (spez. MS Word ab v6.0, *.doc; aber auch andere).

Es gibt nur einen wirksamen Schutz gegen Hoaxes: Information! Also, informieren Sie sich, lesen Sie weiter.

6. Warum soll ich das glauben, was hier steht und nicht den Warnungen?

Eine gute Frage. Vielleicht, weil Sie glauben, diese FAQ wurde von ausgewiesenen Antivirus-Experten erstellt. Gut, aber was beweist das? Also: Schauen Sie unter den unten angegebenen Adressen nach, dort finden Sie seriöse Quellen, aus denen auch diese Informationen stammen. Sie sind leider fast alle auf englisch, wie so vieles im Internet.

7. Wo erhalte ich weitere Informationen zu diesem Thema?

- TU Berlin (dt.) Hier ist die Hoax-FAQ 'zu Hause'
<http://www.tu-berlin.de/www/software/hoax.html>
- Uni Hamburg (dt.)
<http://minerva.sozialwiss.uni-hamburg.de/majordomo/hoax.html>
- Dr. Solomon Viren-Lexikon (z.T. dt.)
<http://www.drsolomon.de/virenlab/index.cfm>
- Barn Owl Software - computer virus myths & hoaxes
<http://www.kumite.com/myths/>
- ICSA - International Computer Security Association (vormals: NCSA)
<http://www.ncsa.com/services/consortia/anti-virus/alerthoax.html>
- CIAC - U.S. Department of Energy Computer Incident Advisory Capability
<http://ciac.llnl.gov/ciac/CIACHoaxes.html>
- Data Fellows (F-Prot, F-Secure)
<http://www.datafellows.com/news/hoax.htm>
- Symantec Antivirus Center (Norton AntiVirus)
<http://www.symantec.com/avcenter/hoax.html>
- NAI/McAfee (VirusScan)
<http://www.nai.com/services/support/hoax/hoax.asp>
- IBM (IBM AntiVirus)
<http://www.av.ibm.com/BreakingNews/HypeAlert/>
- Stiller Research (Integrity Master)
<http://www.stiller.com/myths.htm>
- AVP Virus Encyclopedia
<http://www.avp.ch/avpve/>
- GoodTimes-FAQ von Les Jones (engl.)
<http://www.public.usit.net/lesjones/goodtimes.html>
- GoodTimes-FAQ, deutsche Übersetzung von Markus Seifert
<http://privat.swol.de/rafaelseifert/goodtime.htm>

8. Hoax-Info-Newsletter

Sie können sich aktuelle Informationen über Hoaxes und E-Mail-Sicherheitsfragen per E-Mail zuschicken lassen. Dafür gibt es den Hoax-Info-Newsletter, den Sie auf der Hoax-Seite der TU Berlin (s.o.) bestellen können. Die bislang erschienenen Ausgaben sind auch im WWW verfügbar.

(C) Copyright TU Berlin, Frank Ziemann, 1998, alle Rechte vorbehalten

Jede Art der Vervielfältigung, Speicherung und Weitergabe (außer zum persönlichen Gebrauch), auch auszugsweise, bedarf der schriftlichen Einwilligung des Autors.

–

Informieren Sie sich über sog. E-Mail-Viren:

<http://www.tu-berlin.de/www/software/hoax.html>

Information ist das einzige Gegenmittel!