



Der Hoax – Guide

Ein Überblick über die am meisten verbreiteten Varianten von E-Mail-Hoaxes,
Web-Legenden und anderer schädlicher E-Mail-Kommunikation

Was sind Hoaxes?

Das Wort "Hoax" leitet sich vom lateinischen Wort "hocus" ab und bedeutet im englischen etwa "Scherz". Gemeint waren damit ursprünglich gefälschte Warnungen, meist vor nicht existenten Bedrohungen durch Viren oder Wurm-verseuchte E-Mails, die vor allem Internet-Neulinge mit besten Absichten weiterleiteten. Inzwischen wird die Bezeichnung als Sammelbegriff für verschiedenste Arten von Falschmeldungen im Web gebraucht, die im günstigsten Fall lustig, im ungünstigeren lästig und im schlimmsten Fall gefährlich sind. Auf den Folgenden etwa 15 Seiten erfahren Sie alles, was sie wissen müssen, um Ungemach durch schädliche E-Mail-Kommunikation aus dem Weg zu gehen.

Inhalt:

1. Der Godfather der Hoaxes: Für eine Handvoll Dollar	2
2. 2. A Cry For Help – Die Mitleidsmasche	3
3. Diese E-Mail rettet Ihre Hardware – Oder Ihr Leben	5
4. Der reiche Onkel aus Nigeria	7
5. Petri-Heil: Phishing-Mails auf Dummen-Fang	10
6. Zum Schluss: Eine Checkliste	13

Stand: 26.02.2005

© 2005 Stephan Ehlert - Alle Rechte vorbehalten.

Der Autor übernimmt keinerlei Gewähr für die Inhaltliche Richtigkeit der folgenden Informationen. Der Autor übernimmt nicht die presserechtliche Verantwortung bei Print-Veröffentlichung. Dieser Text wurde Ihnen kostenlos zur Verfügung gestellt. Er darf unverändert vervielfältigt und unentgeltlich begrenzten Personenkreisen zur Verfügung gestellt werden (etwa Im Rahmen einer Mitarbeiterschulung). Die entgeltliche Verwertung jeglicher Art ist ohne vorherige Einwilligung des Autors ausdrücklich untersagt.

1. Der Godfather der Hoaxes: Für eine handvoll Dollar

Dies ist der erste Hoax, mit dem ich in Berührung kam, und ja, ich gebe es zu: Ich bin darauf hereingefallen und habe mir insgeheim schon ausgemalt, was ich mit den 1.000 Flocken so alles anstellen würde, dir mir versprochen wurden: Urlaub. Stereoanlage. Einen neuen Videorecorder.

Videorecorder? Ja, sowas gab es damals noch, man schrieb das Jahr 1997 und ich hatte gerade mein erstes Modem bei Macromarkt (Gab es damals auch noch) erstanden. Ein 33.6 Kbps state-of-the-art Gerät, mit dem man sogar Faxe versenden konnte. Angeblich. Schon einige Tage nach der Neuanschaffung trudelte eine E-Mail ein, deren Absender mir den Atem verschlug: Sie kam von niemand anderem als Bill Gates. Genau, *der* Bill Gates, vom Microsoft-Team, so stand es im Absender.

Und Bill schrieb mir Folgendes:

Hello Everyone,
 And thank you for signing up for my Beta Email Tracking Application or (BETA) for short. My name is Bill Gates. Here at Microsoft we have just compiled an e-mail tracing program that tracks everyone to whom this message is forwarded to. It does this through an unique IP (Internet Protocol) address log book database. We are experimenting with this and need your help. Forward this to everyone you know and if it reaches 1000 people everyone on the list you will receive \$1000 and a copy of Windows98 at my expense.
 Enjoy.

Note: Duplicate entries will not be counted. You will be notified by email with further instructions once this email has reached 1000 people. Windows98 will not be shipped until it has been released to the general public.
 Your friend,

Bill Gates & The Microsoft Development Team.

Gut - Heutzutage haut eine "nagelneue" copy von Windows98 niemanden mehr vom Hocker, aber damals war das was. Und dann die tausend Dollar...Inzwischen sind dankenswerterweise aber auch an die aktuellen Begebenheiten angepasste Versionen im Umlauf. Und die gehen etwa so:

Netscape and AOL have recently merged to form the largest Internet company in the world. In an effort to remain at pace with this giant, Microsoft has introduced a new mail tracking system as a way to keep internet explorer as the most popular browser on the market.

This Email is a beta test of the new software and Microsoft has generously offered to compensate those who participate in the testing process. For each person you send this email to, you will be given \$ 5. For every person they give it to, you will be given an additional \$3. For every person they send it to, you will be given \$ 1.

Microsoft will tally all the emails produced under your name over a two week period and then email you with more instructions. This beta test is only for Microsoft Windows users because the email tracking device that contacts microsoft is embedded into the code of Windows 98, ME and XP.

I knowyou guys hate forwards. But I started this a month ago,

because I was very short on cash. A week ago I got a mail from microsoft asking me for my adress. I gave it to them and yesterday I got a check in the mail for \$ 800. It really works. I wanted you to get a piece of the action.
You won't regret it.

Jeder, der eine solche E-Mail in seinem Postfach hat, kommt schnell auf folgenden Gedankengang: Eigentlich ist es ziemlich unwahrscheinlich, dass die Mail *wirklich* von Bill Gates kommt. Wahrscheinlich hat er tagtäglich besseres zu tun, als mir Emails zu senden. Andererseits: Wem tut's schon weh, wenn ich tue wie mir geheißten, vielleicht ist ja doch was dran...

Und genau an diesem Punkt lohnt es sich, etwas innezuhalten, denn möglicherweise wurde die Frage danach *wem das denn schon weh tut* nicht vollständig korrekt beantwortet. Allgemein lässt sich zwar nicht die Frage nach dem "wem", wohl aber die danach, "wie vielen" das weh tut, nämlich schon mathematisch beantworten: Nehmen wir an, "Bill" hat zunächst mal 1000 Leute angeschrieben, von denen 30% der Bitte "Forward this to everyone you know" folge leisteten, von denen dann wieder 30%.. und so weiter. Das sind eine Menge E-Mails, die eine Menge Traffic erzeugen, den irgendwer bezahlen muss. Eine Menge Leute müssen Zeit aufwenden, um diese Mails zu lesen, und diese wird ihnen in der Zeit von 9 bis 17 Uhr meist ebenfalls bezahlt. Von irgendwem.

Aber die 1000 Dollar!

Aber wie es eben so ist, Bedenken lassen sich bei entsprechender Entlohnung zerstreuen. Es geht ja immerhin um bares Geld - Oder?

Wer die Gier mal einen Augenblick abschaltet, dem könnten hier leise Zweifel kommen. Warum muss ich nirgendwo meinen *Namen oder meine Bankverbindung* angeben? Was für einen *Sinn* soll dieses System eigentlich machen und warum hat es so einen *becknackten Namen*? Vor allem: Wie sollen die E-Mails *gezahlt* werden? Schließlich: Woher weiß ich, dass die ganze Aktion nicht längst abgebrochen wurde und alle ihr "piece of the action" bereits bekommen haben?

Sie ahnen es vielleicht spätestens jetzt: Weder Bill Gates noch AOL werden sie dafür entlohnen, dass sie anderen auf die Nerven fallen. Sie sind einem vermeintlich harmlosen Scherz aufgesessen - der so harmlos gar nicht ist, da er, wie oben erwähnt, reale, in Euro und Dollar messbare Schäden verursacht. Wenn sie eine wirklich gute Tat vollbringen, dann leiten sie die Mail dorthin weiter, wo sie hingehört, nämlich nach "/dev/null", oder wie Bill Gates sagen würde: In den "Papierkorb".

2. A Cry For Help – Die Mitleidsmasche

im bekannten BETA-Hoax ging es für das Opfer noch um ganz profanes Geld - Die zweite Art von klassischen Hoaxes wählt einen subtileren Ansatz, um Sie dahin zu bekommen, wo sie sie haben will, nämlich mit dem Finger auf der "Weiterleiten"-Taste: Nach immer gleichem Muster berichtet Ihnen hier eine E-Mail von Menschen mit einem - vermeintlich - ergreifenden Schicksal, die Sie natürlich retten können. Allerdings nur, in dem sie diese E-Mail *sofort* und „*an alle*“ weiterleiten.

Sie finden das zynisch? In der Tat, das ist sogar ziemlich geschmacklos, was aber viele Menschen nicht daran hindert, Dinge wie die Folgenden weiterzuleiten.

Die Steinigungs-Petition

Sie werden davon gehört haben: In einigen afrikanischen und asiatischen Staaten werden gerade Frauen für vermeintliche "Vergehen" drakonische Strafen angedroht. Eine der abstoßensten ist der Tod durch "Steinigung", der für Dinge wie Ehebruch (unter den durchaus auch eine Vergewaltigung fallen kann) vorgesehen ist. Regelmäßig machen in diesem Zusammenhang Nachrichten wie diese die Runde:

Bitte verteilt diese Nachricht:

Das Obergericht von Nigeria hat das Todesurteil gegen Amina Lawal durch Steinigung ratifiziert. Sie haben nur die Hinrichtung um 2 Monate verschoben, um ihr die Zeit zu lassen, sich von ihrem Baby zu trennen! Nach diesem Aufschub wird sie bis zum Hals in die Erde begraben und dann gesteinigt, wenn nicht eine Lawine von Unterschriften kommt, um die nigerianische Behörde zu überzeugen.

Hier könnte man schon einmal fragen, ob es sehr wahrscheinlich ist, dass ein totalitärer Staat sich von noch-so-vielen "Unterschriften" per E-Mail auf irgendeine Weise beeindrucken lässt.

Aber fahren wir fort:

Amnesty International bittet Euch die Petition auf ihrer Webseite zu unterschreiben. Mit einer ähnlichen Unterschriftskampagne wurde eine andere Frau gerettet, "Safiya", die sich in einer ähnlichen Situation befand.

Hier sehen wir ein Muster, dass in allen Kettenbrief-Hoaxes auftaucht. Irgendeine Autorität - AOL, Microsoft, Walt Disney, Amnesty international - steht angeblich hinter der Sache. Das Ziel ist klar: "Wenn *ai* mich bittet, die Mail weiterzuleiten, dann tu ichs natürlich". Nur: Bloß weil in einer Email die Worte "Amnesty international" fehlerfrei auftauchen, heisst das noch nicht, dass die Mail von von dort kommt, oder dass auch nur *irgendein Zusammenhang* zwischen dem Inhalt der E-Mail und der darin genannten Autorität besteht.

Eigentlich ist das selbstverständlich, aber manche Leute weigern sich, diesen Gedanken einmal zu fassen, bevor sie das tun, was von Ihnen verlangt wird. Genau so, wie sie nicht auf Folgendes kommen: Woher weiß ich eigentlich, dass "Amina" nicht schon lange freigesprochen - oder tot - ist?

Weiter geht's:

Sie können unterschreiben auf der Seite:

[http://\[xxx\]amnesty.org/\[xxx\]](http://[xxx]amnesty.org/[xxx])

Für die, die kein spanisch können:

jetzt wird es vollends absurd: Die Unterschrift soll auf einer Site von Amnesty International geleistet werden. Diese ist aber nun in spanischer Sprache abgefasst, weswegen diejenigen, die "kein Spanisch können", sich auf die Übersetzung in der Mail verlassen müssen (deren vertrauenswürdiger Urheber natürlich im Dunkeln liegt, aber wer wird sich daran schon stören).

Mit anderen Worten: Diejenigen, die nun nach treudoofer Gutmenschen-Art einfach mal das Formular ausfüllen, ohne Spanisch zu können, wissen im wahrsten Sinne des Wortes nicht, was sie dort tun. Wenn sie wenigstens Deutsch, Englisch oder Französisch könnten, wären Sie schon etwas schlauer und wüssten zumindest, wozu das Formular nicht da ist. Denn dick und breit liest sich unter der angegebenen URL:

*Amina Lawal is acquitted and free.
Amina Lawal est libre et la condamnation a été anulée.
Amina Lawal ist frei, ihr Urteil wurde aufgehoben.*

Das Weiterleiten Der E-Mail ist also komplett sinnlos. Über das Formular können Sie übrigens an einer so genannten „Urgent Action“ teilnehmen, die sich mit der Todesstrafe im Allgemeinen, nicht jedoch mit "Amina" befasst.

Amnesty international tritt niemals E-Mail Aktionen wie diese los. Wer uns das nicht glauben mag, darf gern noch einmal selbst nachschauen, beispielsweise auf der der österreichischen Homepage von Amnesty International¹.

Andere Kettenbriefe, die Sie über Ihr Mitgefühl ködern möchten, behaupten beispielsweise, dass ein krebskrankes Kind für jede weitergeleitete E-Mail einen bestimmten Geldbetrag für eine Operation erhält. Denken Sie nach. Los, tun Sie's, Nur dieses eine mal: Glauben sie wirklich, dass irgendeine seriöse Organisation eine derartige Todes-Lotterie betreiben würde?

Wie hat man sich denn das Ende dieser Aktion vorzustellen, wenn dabei nicht genug Mails zusammenkommen? Vielleicht etwa so: *"Sorry Kind, nur 250.000 Emails, das reicht nicht für die lebensrettende Operation - das war wirklich Pech!"*

Keiner dieser Schmarrn-E-mails hat irgendeinen realen Hintergrund, jedenfalls nicht, was das Anliegen der E-Mail und die vermeintlichen Initiatoren angeht, und sie helfen wirklich niemandem, wenn Sie diesen Blödsinn weiterverbreiten. Wenn Sie wirklich etwas gutes Tun möchten, dann spenden Sie für einen guten Zweck oder treten Sie mit dem lokalen Amnesty-chapter in Ihrer Gegend in Kontakt - dort wird man Ihnen sagen können, wie sie sich wirklich zum Beispiel gegen die Steinigung nützlich machen können.

Für den Fall, dass sie einen Tränendrüsen-Kettenbrief erhalten - und das ist nur eine Frage der Zeit - Bleibt also nur der Rat:

Ärgern sie sich darüber und werfen Sie ihn weg - aber beteiligen Sie sich um Gottes Willen nicht an diesem zynischen Unsinn. Der kostet Sie Zeit und andere Zeit, Geld und Nerven.

Wenn Sie eine Mail bekommen, in der Sie aufgefordert werden, diese weiterzuleiten, ist das immer ein sicheres Zeichen, dass der Inhalt nichts anderes als ein Versuch ist, sie hereinzulegen, egal was sonst noch darin steht.

3. Diese E-Mail rettet Ihre Hardware – Oder Ihr Leben

Angst, genauer gesagt: *Blankes Entsetzen* ist der Treibstoff für diese Kategorie der "Falschmeldung per E-Mail", die den "Hoaxes" Ihren Namen gab. Sie ist deswegen besonders "erfolgreich" bzw. einfach nicht totzukriegen, weil Sie Halbwahrheiten, die fast jeder schon einmal in den Medien gehört oder gelesen hat, dazu benutzt, um sich weiterzuverbreiten.

Haben Sie auch schon von dem *neuen, bössartigen Virus* gehört, das sich durch das bloße Ansehen einer E-Mail verbreitet und sogar die Hardware befallen kann? Alle AntiViren-Programme sind

¹ http://www.amnesty.at/urgentaction/cont/urgent/nigeria_klarstellung.htm.

dagegen chancenlos! *Norton Security* hat es gestern erst bekannt gegeben!

Wie? Sie glauben das nicht? Damit liegen Sie vollkommen richtig.

Aber leider - und an dieser Stelle wiederholen wir uns wohl - gehören Sie damit zu einer Minderheit, die es mit zunehmendem Medienhype bei jeder *realen* Würmer-Welle immer schwerer hat, sich gegen hysterische E-Mail Kontakte zur Wehr zu setzen. Virus-Warn-Hoaxes sehen normalerweise etwa so aus:

wenn sie eine Email mit dem Titel "GET MORE MONEY!!!" erhalten, öffnen sie diese unter keinen Umständen! Sie wird alle Daten löschen, die sich auf Ihrer Festplatte befinden. Dies ist ein neues, gefährliches Virus, und noch nicht sehr viele Leute wissen darüber Bescheid.

Merken Sie's? Hoaxes sehen wirklich immer gleich aus, nur der "Treibstoff" variiert. Wie bei allen anderen Arten von E-Mail-Hoaxes kann man hier ebenfalls früh skeptisch werden: *Was heißt denn "neu" eigentlich genau? Gestern ? letzte Woche? letztes Jahr? Vor drei Jahren?*

Die E-Mail trifft naturgemäß keine Aussage hierzu, allerdings kann der Autor dieses Textes ihnen sagen, wann er wortwörtlich diese E-Mail zum allerersten Mal in seiner Mailbox hatte: Vor sechs Jahren, also 1998. Und immernoch ist das Virus "brandneu". Und brandgefährlich, natürlich...

Öffnen sie auch keine Mail die den Titel "Returned or unable to deliver" trägt. Dieses Virus wird sich an Ihre Computerverbindungssteile heften und sie unbrauchbar machen.

Dieses Muster finden wir in allen Virus-Hoaxes: Wahrhaft apokalyptische Folgen soll dieser Schädling haben, Die *Computerverbindungssteile*, ich vermute damit ist die Hardware gemeint, werden "befallen". Kein Virus kann das - Lassen sie sich nicht kirre machen. Auffällig auch, wie wolzig das angebliche Schadensprogramm beschrieben wird: Es ist neu, und es ist tödlich. Mehr erfahren wir nicht. Außer natürlich:

Diese Warnung wurde letzte Woche von Microsoft bekanntgegeben.

Klar, das kennen wir auch schon: Das ist doch der selbe Laden, der uns vorhin schon Geld dafür bezahlen wollte, dass wir E-Mails weiterleiten. "Jeden Tag eine gute Tat!" ist offenbar das Motto der Firma aus Redmond. Aber natürlich gilt dasselbe, was zu den anderen Hoaxes und deren vermeintlichen Urhebern gesagt wurde auch hier: Niemals verbeitet Microsoft oder Norton oder irgendeine andere seriöse Firma solche Warnungen per Ketten-E-Mail.

Wenn sie eine solche mail erhalten, löschen Sie sie bitte sofort, ohne sie sich anzusehen.

... "Denn sonst würden Sie ja merken, dass es sich nur um eine relativ harmlose Werbe-Mail bzw. die Benachrichtigung eines Mail-Servers über eine fehlgeschlagene Zustellung handelt", möchte man da noch hinzufügen. Und zum letzten Satz:

Bitte leiten sie diese Warnung an so viele Leute weiter wie möglich.

Muss wohl wirklich gar nichts mehr gesagt werden.

Ein paar Worte zu "echten" Viren und Würmern

Es gibt sie wirklich: E-Mail Würmer, die sich in schädlichen Dateianhängen verstecken, und die sich beim Klick auf den Anhang automatisch weiterverbreiten. Aus neuerer Zeit ist der Wurm "Netsky" so ein Beispiel. Aber zum einen verbreiten sich diese Programme niemals durch das bloße Ansehen einer (Text-) Nachricht, und zum anderen ist die eigentliche Schadensfunktion eines Wurms meist lediglich, sich weiterzuverbreiten, indem er sich an Ihr gesamtes Adressbuch versendet.

Merken Sie was? Wenn Sie tun, um was sie in der Hoax-Mail gebeten wurden, wird aus der Mail auf einmal genau das, wovon er angeblich warnt: Ein "manueller" Wurm, der sich explosionsartig weiterverbreitet und so Schäden anrichtet.

Wenn Sie sich gegen reale Gefahren aus dem Netz absichern möchten, dann verwenden Sie 1. ein sicheres E-Mail-Programm und 2. einen aktuellen Virensch scanner. Und klicken Sie 3. nicht auf Attachments, die sie unerwartet und/oder unkommentiert erreichen. Wenn sie dies beherzigen, sind sie einigermaßen sicher².

Zurück zu unserer Panik-Mail. Natürlich gibt es andere Warn-Texte und andere Betreff-Zeilen und inzwischen wird auch vor ganz anderen Gefahren gewarnt: Mal sollen von Terroristen tausende UPS-Uniformen gestohlen worden sein, um sie bei Terroranschlägen als Tarnung zu verwenden (weswegen sie sich natürlich vor dem UPS-Mann in Acht nehmen müssen), ein anderes Mal haben Islamisten die Cola vergiftet (weswegen sie nur noch Milch trinken dürfen). Die Liste ist schier endlos. Eines aber haben alle diese Warnungen gemeinsam: Sie sind vollkommen gegenstandslos.

Lassen Sie sich also nichts vormachen: Kettenbriefe sind kein Mittel zur Kommunikation seriöser Anliegen. Niemals. Es gibt zu dieser Regel keine Ausnahme. Deswegen tun sie mit ihnen bitte das, was sie verdienen: Löschen und vergessen Sie sie. Aber leiten sie sie nicht weiter.

4. Der reiche Onkel aus Nigeria

Jeder E-Mail-Nutzer hat sie früher oder später in seinem elektronischen Postfach: Ungebetene E-Mails in schlechtem, oft durchgehend großgeschriebenem Englisch von angeblichen Schwiegersöhnen, Enkeln oder sonst irgendwie Verwandten des früheren Finanzministers, Nationalbankdirektors oder irgendeines anderen hochrangigen Vertreters von Nigeria, Zambia oder anderen exotischen Staaten.

Versprochen werden: Horrende Summen für den Gefallen, für ein paar Tage noch horrendere Summen ("ONE HUNDRET AND THIRTY-THREE MILLION US-DOLLARS!") auf dem Konto des Adressaten parken zu dürfen. Selbstverständlich ist noch niemand auf diese Weise reich geworden - außer dem Onkel aus Nigeria, versteht sich.

Nigerian Scam - Die "nigerianische Masche" - nennt man üblicherweise die E-Mails, die sich etwa so lesen:

² Dieses umfangreiche Thema kann hier nicht ausführlicher dargestellt werden. Einen Beitrag des Autors über einfache Maßnahmen für sichere E-Mail-Kommunikation finden Sie unter <http://www.kaffeeringe.de/Article85.html>.

FROM: FRANK MUTOBO <Frankmutobo1@netscape.net>;
 SUBJECT:REQUEST FOR ASSISTANCE IN A FINANCIAL TRANSACTION
 TO:<>

Dear Sir,

I am interested in your partnership in business dealing. This business proposal I wish to intimate you with is of mutual benefit and it's success is entirely based on mutual trust, cooperation and a high level of confidentiality as regard this transaction. I am representing the board of the contract award and monitoring committee of the Zambian Ministry of Mining and Resources. I am seeking your assistance to enable me transfer the sum of US\$30,500,000.00 (Thirty Million, Five Hundred Thousand United States Dollars) into your private/company account.

Es folgen ebenso langatmige wie holprige Ausführungen darüber, wie der Absender in den Besitz von So viel Geld gekommen sein will, und warum er unbedingt ein ausländisches Bankkonto zum Parken der Summe benötigt. Schließlich kommt er auf den Punkt:

Hence this message to you seeking your assistance so as to enable me present your private/company account details to enable me transfer the difference of US\$30,500,000.00 (Thirty Million, Five Hundred Thousand United States Dollars) into your provided account. On actualisation, the fund will be disbursed as stated below. 1. 20% of the fund will be for you as beneficiary.[...]
 For further details as to the work ability of this transaction, please reach me as soon as possible for further clarification. Please you can reach me with this email address below:
 Frankmutobo@netscape.net
 Thank you and God bless as I await your urgent response.
 Yours Sincerely,
 Mr. Frank Mutobo

Klingt das nicht prima? 20 Prozent von gut 30 Millionen - das sind ja... 6.1 Millionen (Nigerianisch: "SIX MILLION AND ONE HUNDRET THOUSAND") Dollar! Und man muss dafür nicht mal arbeiten - Ein wirklich verlockendes Angebot. Wäre da nicht die Tatsache, das dies eine - im Gegensatz zu dem Vermögen des Absenders - real existierende Betrugsmasche, ist, die bereits viele real-existierende Opfer in den Ruin getrieben hat. Und die so funktioniert:

Die Masche

Schritt 1: Massenemail versenden

Schritt eins unseres Nigerian Scam (auch: "4-1-9 Scam", benannt nach dem nigerianischen Betrugsparagrafen) besteht darin, die Angel nach möglichen Opfern auszuwerfen. Das geschieht, in dem eine E-Mail wie die obige an tausende Empfänger versendet wird. Die Methoden, an gültige Adressen zu gelangen, variieren dabei. Entweder werden automatisch zufällige Buchstabenkombinationen ausgewählt und ausprobiert, Programme, so genannte "Harvester" eingesetzt, die das Internet nach E-Mail Adresse abgrasen oder es werden Adressen ganz einfach gekauft oder gestohlen. Und bei jedem Mailing gibt es einige Unbedarfte, die tatsächlich antworten. Sodann folgt

Schritt 2: Die Kontaktaufnahme

Das Opfer nimmt nun Kontakt zu dem Absender der Scam-Email auf, um seine Bereitschaft zu bekunden, sein Bankkonto für die "Transaktion" zur Verfügung zu stellen. Nun muss Herr Mutobo nur noch den Sack zumachen, damit das Opfer den Köder endgültig schluckt. Das tut er, in dem er weitere (fiktive) Details der Transaktion mitteilt, schon mal nach der Bankverbindung für die Überweisung des Geldes fragt und danach möglicherweise eine schriftliche Übereinkunft faxt, um den Anschein von Seriösität zu erzeugen - "*Man will bei so einer Summe auf Nummer sicher gehen, das verstehen Sie ja als Geschäftsmann*". und natürlich vergisst Herr Mutobo nicht, wortreich zu versichern, wie dankbar er dem Opfer - pardon: seinem *Geschäftspartner* sei. Alles laufe wie geschmiert, schon in den nächsten Tagen könne man mit der Überweisung von so-und-soviel Millionen rechnen, und mit der Vergütung sowieso.

Das leichtgläubige Opfer denkt spätestens jetzt darüber nach, was es mit dem unverhofften Reichtum anstellen wird und vergisst dabei vollkommen, dass es das Geld noch gar nicht gesehen hat.

Schritt 3: Plötzliche Schwierigkeiten

Bis jetzt lief alles wie am Schnürchen, und das Opfer rechnete jeden Tag mit dem Eingang der Millionen auf dem Konto. Aber nein! Kurz vor dem Ziel tauchen Schwierigkeiten auf - Mr. Mutobo meldet sich etwas zerknirscht: Dummerweise muss er für den reibungslosen Ablauf einige Beamte bestechen, und leider kommt er aus verschiedenen Gründen im Moment gerade nicht an seine Millionen. Unwetter, Stromausfälle - Sie verstehen. Monrovia ist eben nicht Köln, da kann so was schon mal vorkommen. Deswegen bittet er das Opfer, ihm auf die Schnelle ein paar tausend Dollar vorzuschießen, die selbstverständlich zurückgezahlt werden, so bald das Geschäft abgelaufen ist. "Kein Problem - Was sind schon ein paar tausend Dollar gegen die Millionen, die zu erwarten sind, wenn alles klappt?", sagt sich das Opfer. Und zahlt.

Und an diesem Punkt nimmt das Verhängnis endgültig seinen Lauf.

Selbstverständlich bleibt es nicht bei diesem einen kleinen Problem, das der Überweisung der Summe noch im Wege steht. Immer neue Schwierigkeiten treten auf, es müssen immer neue Bestechungen, Flugkosten, Zoll-Gebühren und Ähnliches bezahlt werden. Und Wie ein Spielsüchtiger, der immer mehr Geld in den Spielautomaten wirft, weil er verzweifelt hofft, dass er *dieses mal den Jackpot knackt* und seine Investitionen sich lohnen, zahlt das Opfer. Und zahlt. Und zahlt.

Es besteht ja auch aus seiner Sicht keine andere Wahl: Der Erfolgsdruck wird mit jeder Zahlung größer. Nicht mehr zu zahlen hieße nicht nur, sich einzugestehen, dass man auf einen Betrug hereingefallen ist. Zehn, zwanzig oder dreißigtausend Dollar an "Vorschüssen" wären zum Fenster herausgeworfen, ohne eine Chance sie je wiederzubekommen. Und natürlich versichert Herr Mutobo jedes mal, dass dies bestimmt der letzte Vorschuss sei, der erbracht werden müsse.

Dies ist der eigentliche Trick des Nigerian Scam: Das Opfer gerät in eine Zahlungsspirale, aus der es nur zu entkommen meint, indem es noch mehr zahlt, denn dann, so der Strohalm, an den es sich klammert, dann werden ja endlich die Millionen fließen.

Dumm nur: Die Millionen gibt es nicht.

Wer diesen Mechanismus nicht irgendwann durchschaut, für den wird es nicht nur finanziell eng, sondern er begibt sich tatsächlich in *Lebensgefahr*. Denn früher oder später wird Mr. Mutobo mit

der freudigen Nachricht aufwarten, dass das Geld nun da sei, leider könne man es aus mehr oder weniger plausiblen Gründen nicht überweisen, sondern es müsse bar in Nigeria abgeholt werden - natürlich nicht ohne dass das Opfer bei dieser Gelegenheit eine weitere Summe in bar vorstrecken muss. Wofür auch immer.

Und die Verzweifelten, die bereits ihr gesamtes Vermögen an die Betrüger gezahlt haben, sehen keinen anderen Ausweg, als selbst das zu tun. Sie leihen sich das geforderte Geld und fliegen nach Nigeria, wo sie schließlich von Ihren Peinigern auch noch unter Androhung oder Anwendung von schlichter Gewalt ausgeraubt oder sogar als Geisel genommen werden. Es ist mindestens ein Fall bekannt, in dem das Opfer eines Nigerian Scam bei dieser Gelegenheit ermordet wurde, wenngleich dies nicht den Regelfall darstellt.

Und so endet dann der Traum vom schnellen Geld vom Onkel aus Nigeria.

Die Geschichte des Nigerian Scam

Das eigentlich interessante an der nigerianischen Masche besteht nicht unbedingt in der Art und Weise, wie die Opfer immer tiefer in den Strudel aus immer weiteren Zahlungen und schließlich in den Ruin getrieben werden - so etwas gibt es auch bei anderen betrügerischen "Geschäftsmodellen" wie etwa Schneeballsystemen, Pyramidenspielen oder so genannten "Schenkkreisen". Auch im Zeitschriftenvertrieb, also innerhalb so genannter "Drückerkolonnen" werden ähnliche Mechanismen verwendet, um Abhängigkeiten zu erzeugen und den Betroffenen den Ausstieg zu erschweren.

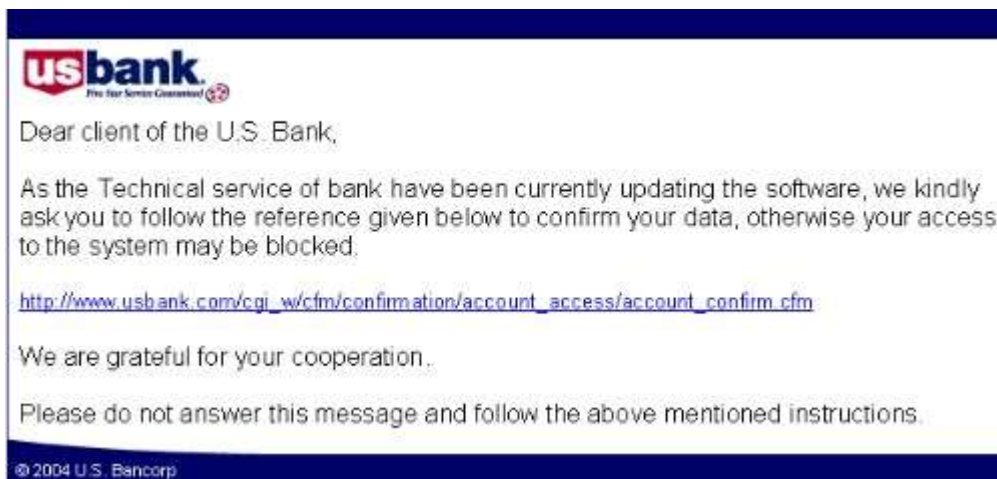
Der Nigerian Scam schreibt bis heute eine beispiellose Erfolgsgeschichte: Die Masche existiert in dieser Art bereits seit gut 20 Jahren und macht nach Schätzungen gut ein fünftel der nigerianischen Wirtschaft aus (!); Ähnliche Arten Betrug tauchten bereits in den 20er Jahren des 20. Jahrhunderts auf. Damals richteten sich die Botschaften - die per Post in die Welt hinaus getragen wurden - vor allem an gutbetuchte Geschäftsleute aus Westeuropa. Mit dem Medium "E-Mail" haben sich für die Betrüger vollkommen neue Möglichkeiten ergeben - Sehr große Zahlen potenzieller Opfer lassen sich mit extrem geringen Aufwand erreichen. Und getreu dem Motto "Kleinvieh macht auch Mist" kommen auch beim Ausnehmen von Kleinverdienern ordentliche Summen zusammen.

Wenn Sie so eine E-Mail (auch Fax, Brief pp.) erhalten - und das werden Sie früher oder später - Antworten Sie nicht darauf. Gehen Sie auf keinen Fall auf derartige Angebote ein, und wenn sie das schon getan haben: Brechen Sie den Kontakt sofort ab. Auch wenn Sie bereits Geld verloren haben, gilt: Umso früher Sie erkennen, auf einen Betrug hereingefallen zu sein, desto geringer bleibt der finanzielle Schaden. Klammern Sie sich nicht an die Hoffnung, dass es die Millionensummen doch irgendwo gibt. Es gibt sie nicht - Und sie gefährden mehr als nur Ihr Vermögen, wenn sie das nicht wahrhaben wollen.

5. Petri-Heil: Phishing-Mails auf Dummen-Fang

Kein Hoax und damit gar nicht witzig: E-Mails mit gefälschten Absendern, die vorgeblich von Banken oder anderen seriösen Unternehmen - wie beispielsweise Ebay - stammen und sich unter fadenscheinigen Vorwänden Zugangsdaten zu Online-Banking-Accounts und Bezahlssystemen zu erschleichen versuchen. Neudeutsch nennt man diese Art des Angelns nach fremden Daten "Phishing" (**Pass**word **Fishing** – Fischen nach Passwörtern).

Die typische Phishing-E-Mail sieht etwa so aus:



„Lieber Kunde,
 Da die technische Abteilung unserer Bank im Moment die Software updatet, bitten wir Sie freundlich darum, dem unten angegebenen Link zu folgen und Ihre Daten dort zu bestätigen. Ansonsten wird Ihr Zugang zum System gesperrt.
 Wir Danken Ihnen für Ihre Kooperation.
 Bitte beantworten Sie diese Nachricht nicht sondern folgen Sie den obigen Anweisungen" (URL inzwischen deaktiviert)

Nun werden wenige deutschsprachige Internet-Nutzer auf gerade diese Mail hereinfliegen, weil die US-Bank nicht allzu viele Kunden in diesem Sprachkreis haben dürfte. Trotzdem bildet sie ein gutes Beispiel.

Selbstverständlich versendet keine Bank solche E-Mails. Niemand, der es ehrlich mit Ihnen meint, wird sie jemals nach PIN- oder TAN-Nummer fragen. Leider machen es manche E-Mail Programme und Sicherheitslücken von Browsern den Phishern nur allzu leicht. So ist es sogar kein Problem, dem Benutzer des meistverwendeten Browsers - nämlich dem MS Internet Explorer - soweit dieser nicht höchst regelmäßig geeignete Sicherheits-Updates für die Software installiert, gefälschte URLs anzuzeigen. In unserem Beispiel hieße das: Stellen Sie sich vor, sie seien US-Bank-Kunde und klickten auf den angegebenen Link. über diesen werden Sie natürlich nicht zu Ihrer Bank, sondern auf eine Seite des Verfassers der Phishing-E-Mail geleitet, die der Website der Bank täuschend echt nachempfunden hat. Und, oh Schreck: Sogar Ihr Browser zeigt eine URL an, die aussieht, als wäre dies wirklich eine "offizielle" Seite.

HTML-E-Mails machen es Betrügern noch leichter

Noch leichteres Spiel haben Betrüger, die sie um Ihr Geld bringen möchten, wenn Sie in Ihrem E-Mail Programm HTML-E-mails anzeigen lassen. Denn dort kann man ihnen praktisch alles vor-spiegeln - wie auch das folgende Beispiel zeigt:

Subject: Account verification



Dear eBay user,
 During our regular update and verification of the accounts, we were not able to verify your current account information, either your information has changed or it is incomplete. Please update and verify your information by filling out the verification form. If the account information is not updated within 5 days then your access to bid and buy on eBay will be restricted.
 Click on the link below to complete the verification:

<http://cgi.ebay.com/su/cgi/eBayISAPI.dll?Verify&id=4152500162>

*** PLEASE DO NOT RESPOND TO THIS EMAIL ***

Thank you
 Account Management

As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our [Privacy Policy](#) and [User Agreement](#) if you have any questions.

Copyright 2002 eBay Inc. All Rights Reserved.
 Designated trademarks and brands are the property of their respective owners.
 eBay and the eBay logo are trademarks of eBay, Inc.

[Announcements](#) | [Register](#) | [SafeHarbor \(Rules & Safety\)](#) | [Feedback Forum](#) | [About eBay](#)

Copyright © 1995-2001 eBay Inc. All Rights Reserved.
 Designated trademarks and brands are the property of their respective owners.
 Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).



Lieber EBay-User,
 Während unserer regelmäßigen Benutzerkonten-Wartung konnten wir Ihre aktuellen Benutzerinformationen nicht verifizieren. Entweder sind Ihre Informationen falsch oder unvollständig.
 Bitte aktualisieren Sie Ihre Informationen mit dem Formular, dass sie über den Link erreichen. Sollten Sie Ihre Informationen nicht innerhalb von fünf Tagen aktualisiert haben, wird Ihr Zugriff auf die Bieten- und Kaufen-Funktionen von ebay begrenzt.

Obwohl der Link, unter dem der "Kunde" hier seine Ebay-Zugangsdaten eingeben soll, anscheinend auf eine Ebay-Seite zeigt, kommen Sie selbstverständlich auf die Site des Phishers, der sie um Ihre Daten bringen will. Die Site "hinter" dem Link hat nichts mit der hier angezeigten URL zu tun.

Eine einfache Checkliste

Es ist nicht schwer, auf "Phisher" hereinzufallen - Aber ebenso leicht ist es, Phishing-E-Mails zu erkennen.

Sollte eine E-Mail

- Sie bitten, persönliche Informationen wie Kreditkartennummern, PINs, TANs oder Benutzerdaten und Passwörter einzugeben,
- Behaupten, Sie käme von einer seriösen Firma - etwa: Banken, *Ebay* - gleichzeitig aber von Rückfragen abraten

Dann tun sie auf gar keinen Fall das, um was sie in der E-Mail gebeten werden.

Unter keinen denkbaren Umständen wird ein seriöses Unternehmen sie auf diese Weise um die Eingabe vertraulichen Informationen fragen.

6. Zum Schluss: Die Hoax-Checkliste

Nachdem wir Ihnen nun einen recht ausführlichen Überblick über die häufigsten Varianten gegeben haben, in denen Hoaxes Sie erreichen können, fehlt nur noch Eines, um Sie darauf vorzubereiten, den nächsten Angriff auf Ihre Mailbox erfolgreich abzuwehren:

Eine kurze Checkliste, mit der sie diese Art von Spam zuverlässig erkennen.

Einen Hoax zu erkennen ist nicht schwierig. Etwas schwieriger ist schon die Frage zu beantworten, wie die denn richtige Reaktion aussieht. Und natürlich: wie sie nicht aussieht.

Woran erkenne ich einen E-Mail-Hoax?

- Die E-Mail, die sie erhalten haben, verspricht Ihnen oder anderen einen Vorteil, wenn Sie sie weiterleiten.
- Die Nachricht wurde bereits mehrere Male weitergeleitet - zu erkennen an den anderen E-Mail-Adressen im Text.
- Ein bekannter Konzern oder eine andere bekannte Organisation steht angeblich hinter der Sache.
- Wenn sie immer noch unsicher sind, dann nehmen Sie einen markanten Teil des Nachrichtentextes - beispielsweise Namen, die genannt werden, oder den Betreff - und geben Sie ihn als Suchbegriff bei "google" ein.

Wie verhalte ich mich, wenn ich einen Hoax erhalte?

- Leiten Sie die E-Mail auf gar keinen Fall weiter.
- Leiten Sie die E-Mail auch dann nicht weiter, wenn sie der Meinung sind, dass sie es diesmal vielleicht doch tun sollten.
- Ob Sie den Absender über seinen Irrtum aufklären, müssen Sie selbst entscheiden. Es gibt ebenso viele Gründe, die dafür sprechen, wie solche dagegen (Verlinken Sie, wenn Sie den Absender informieren, gern auf diese Site)
- Löschen Sie die E-Mail.

Was sollte ich auf gar keinen Fall tun?

- Leiten Sie die E-Mail auf gar keinen Fall weiter.
- Nehmen sie Auf gar keinen Fall Kontakt zu seriös klingenden E-Mail-Adressen auf, die im Hoax

genannt werden. Diese Leute haben mit dem Inhalt dieser Nachrichten meist nichts zu tun und ertrinken regelmäßig in Anfragen, bezüglich dessen, was es mit der Mail auf sich habe.

- Starten Sie nicht ihren Eigenen Kettenbrief, um andere vor dem Hoax zu warnen.

Diese und weitere aktuelle Informationen können Sie auch online auf www.hoaxbusters.de abrufen.

© 2005 Stephan Ehlert - Alle Rechte vorbehalten.

Der Autor übernimmt keinerlei Gewähr für die Inhaltliche Richtigkeit der folgenden Informationen. Der Autor übernimmt nicht die presserechtliche Verantwortung bei Print-Veröffentlichung. Dieser Text wurde Ihnen kostenlos zur Verfügung gestellt. Er darf unverändert vervielfältigt und unentgeltlich begrenzten Personenkreisen zur Verfügung gestellt werden (etwa Im Rahmen einer Mitarbeiterschulung). Die entgeltliche Verwertung jeglicher Art ist ohne vorherige Einwilligung des Autors ausdrücklich untersagt.