Universität Regensburg

Elena Maria Kellinghaus
IT-Sicherheitsbeauftragte
Rechenzentrum

Merkmale einer Phishing-Mail – „Fake“-Mails erkennen

So manch betrügerische E-Mail sieht täuschend echt aus. Jedoch gibt es einige Punkte, die erkennen lassen, dass ein Übeltäter seine Angel ausgeworfen hat.

1. Grammatik- und Orthografie-Fehler
2. Mails in fremder Sprache
3. Fehlender Name
4. Dringender Handlungsbedarf
5. Eingabe von Daten
6. Aufforderung zur Öffnung einer Datei
7. Links oder eingefügte Formulare
8. Bisher noch nie E-Mails von der Bank erhalten oder kein Kunde
9. Verdächtiger Absenderadresse

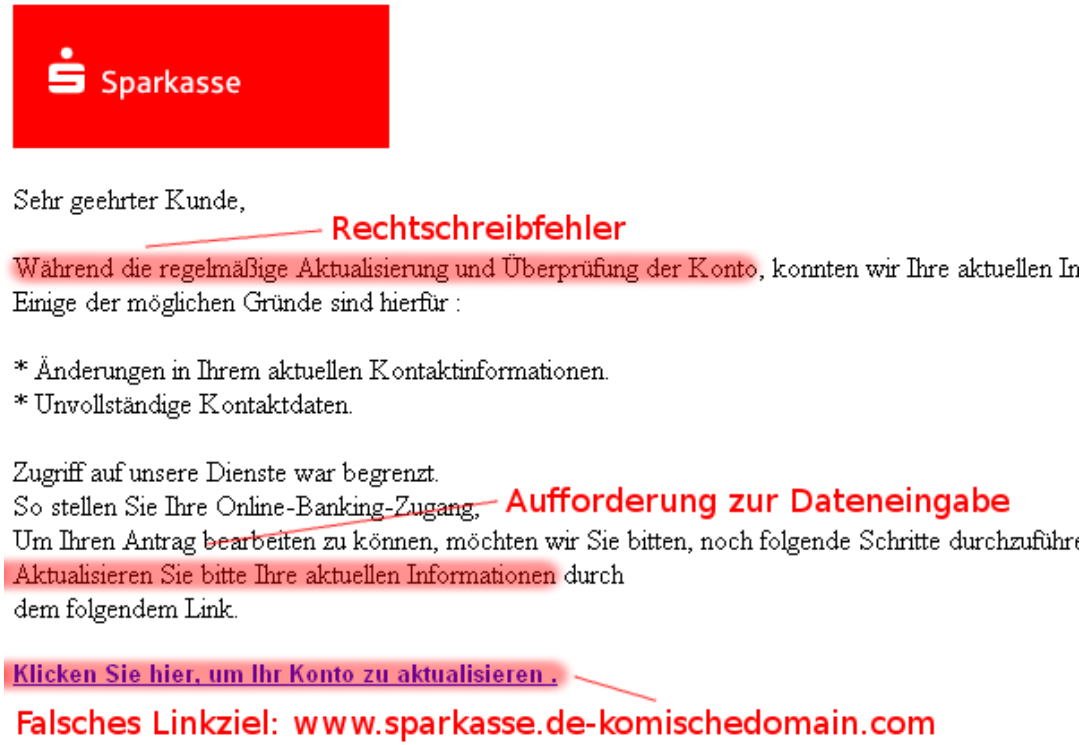
Universität Regensburg

Elena Maria Kellinghaus
IT-Sicherheitsbeauftragte
Rechenzentrum

Merkmale einer Phishing-Mail – „Fake“-Mails erkennen

1. Grammatik- und Orthografie-Fehler

Phishing-Mails sind sehr oft in fehlerhaftem Deutsch geschrieben. Diese reichen von kleineren Komma-Fehlern bis zu komplett unverständlichen Texten. Ausländische Betrüger machen sich keine große Mühe bei der Übersetzung ihrer Texte, sie arbeiten mit einfachen Online-Übersetzern. Fehlende Umlaute oder kyrillische Zeichen sind ein weiteres Indiz für eine gefälschte E-Mail.



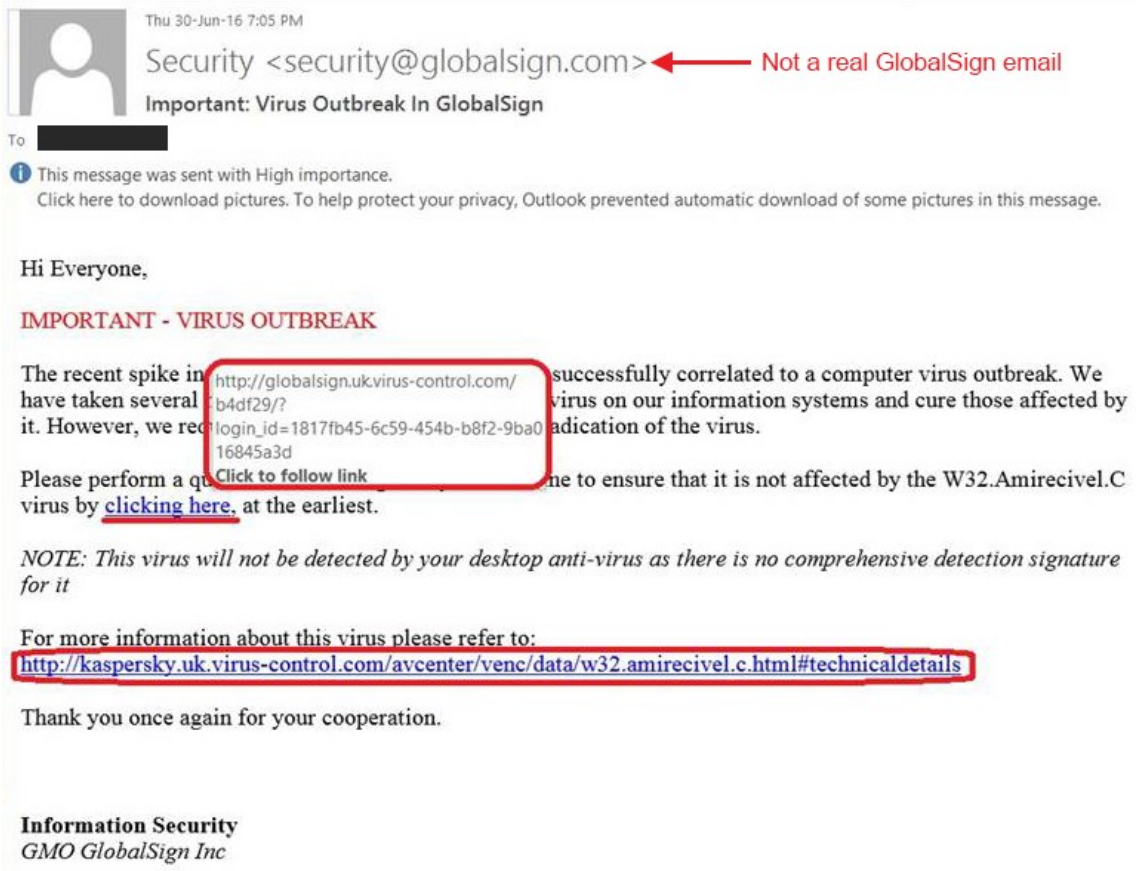
Universität Regensburg

Elena Maria Kellinghaus
IT-Sicherheitsbeauftragte
Rechenzentrum

Merkmale einer Phishing-Mail – „Fake“-Mails erkennen

2. Mails in fremder Sprache

Leicht zu identifizieren sind Phishing-Mails, die in einer anderen Landessprache verfasst sind. Ihre Bank würde nie auf die Idee kommen, Ihnen eine dringliche E-Mail auf Französisch zu schicken.



Thu 30-Jun-16 7:05 PM

Security <security@globalsign.com> ← Not a real GlobalSign email

Important: Virus Outbreak In GlobalSign

To [redacted]

This message was sent with High importance.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Hi Everyone,

IMPORTANT - VIRUS OUTBREAK

The recent spike in [redacted] successfully correlated to a computer virus outbreak. We have taken several [redacted] virus on our information systems and cure those affected by it. However, we rec[redacted] adication of the virus.

http://globalsign.uk.virus-control.com/b4df29/?login_id=1817fb45-6c59-454b-b8f2-9ba016845a3d
Click to follow link

Please perform a qu[redacted]ne to ensure that it is not affected by the W32.Amirecivel.C virus by clicking here, at the earliest.

NOTE: This virus will not be detected by your desktop anti-virus as there is no comprehensive detection signature for it

For more information about this virus please refer to:
http://kaspersky.uk.virus-control.com/avcenter/venc/data/w32.amirecivel.c.html#technicaldetails

Thank you once again for your cooperation.

Information Security
GMO GlobalSign Inc

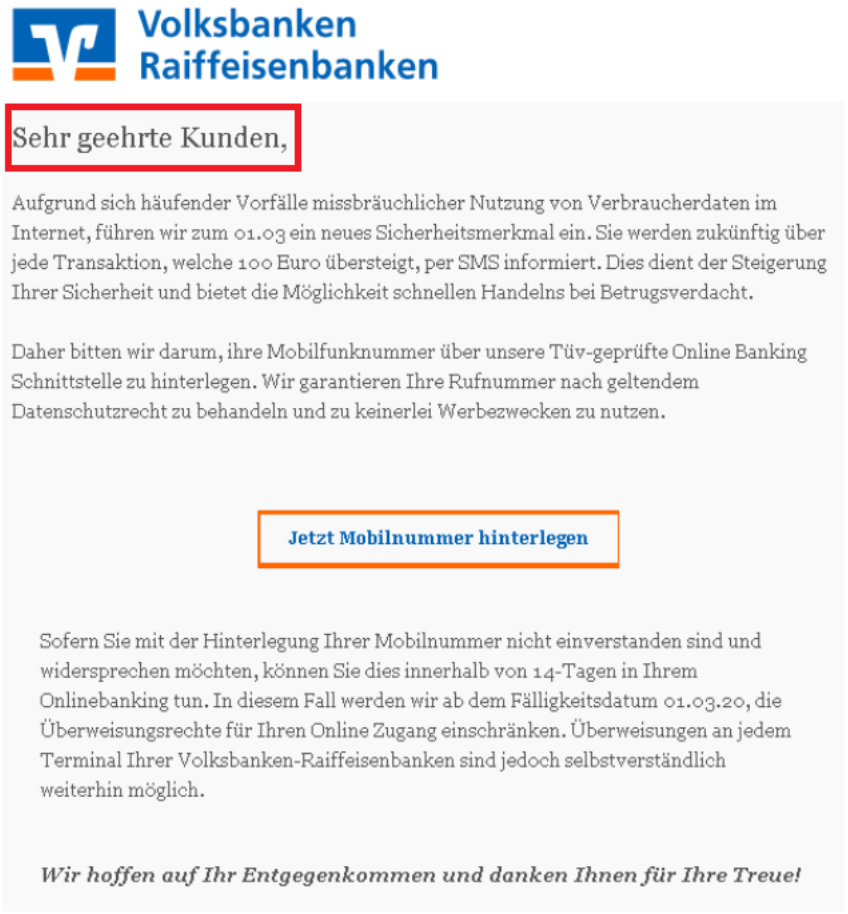
Universität Regensburg

Elena Maria Kellinghaus
IT-Sicherheitsbeauftragte
Rechenzentrum

Merkmale einer Phishing-Mail – „Fake“-Mails erkennen

3. Fehlender Name

Wenn Sie eine verdächtige E-Mail erhalten und in der Anrede nicht Ihr persönlicher Name steht, handelt es sich sehr oft um eine gefälschte Mail. "Sehr geehrter Kunde" oder "Sehr geehrter Nutzer" sind sehr unpersönlich und weisen darauf hin, dass die Absender Sie gar nicht kennen. Umgekehrt gilt aber: Auch in einer Phishing-Mail kann Ihr Name stehen! Eine E-Mail ist trotz Ihres Namens nicht immer vertrauenswürdig.



Volksbanken Raiffeisenbanken

Sehr geehrte Kunden,

Aufgrund sich häufender Vorfälle missbräuchlicher Nutzung von Verbraucherdaten im Internet, führen wir zum 01.03 ein neues Sicherheitsmerkmal ein. Sie werden zukünftig über jede Transaktion, welche 100 Euro übersteigt, per SMS informiert. Dies dient der Steigerung Ihrer Sicherheit und bietet die Möglichkeit schnellen Handelns bei Betrugsverdacht.

Daher bitten wir darum, ihre Mobilfunknummer über unsere Tüv-geprüfte Online Banking Schnittstelle zu hinterlegen. Wir garantieren Ihre Rufnummer nach geltendem Datenschutzrecht zu behandeln und zu keinerlei Werbezwecken zu nutzen.

Jetzt Mobilnummer hinterlegen

Sofern Sie mit der Hinterlegung Ihrer Mobilnummer nicht einverstanden sind und widersprechen möchten, können Sie dies innerhalb von 14-Tagen in Ihrem Onlinebanking tun. In diesem Fall werden wir ab dem Fälligkeitsdatum 01.03.20, die Überweisungsrechte für Ihren Online Zugang einschränken. Überweisungen an jedem Terminal Ihrer Volksbanken-Raiffeisenbanken sind jedoch selbstverständlich weiterhin möglich.

Wir hoffen auf Ihr Entgegenkommen und danken Ihnen für Ihre Treue!

Universität Regensburg

Elena Maria Kellinghaus
IT-Sicherheitsbeauftragte
Rechenzentrum

Merkmale einer Phishing-Mail – „Fake“-Mails erkennen

4. Dringender Handlungsbedarf

In den typischen Phishing-Mails werden die Betroffenen dazu aufgefordert, innerhalb einer kurzen Frist tätig zu werden.

Diese Forderung ist meistens auch mit einer Konsequenz verbunden, sollten Sie dieser nicht nachgehen - zum Beispiel die Sperrung des Bankkontos, der Kreditkarte, des Kundenkontos, usw.

Hallo [redacted]

Ihre Mithilfe ist erforderlich!

Die neuen Datenschutzgesetze verpflichten uns nun dazu, in regelmäßigen Abständen die Konten unserer Kunden zu überprüfen. Dies dient ausschließlich zu Ihrer eigenen Sicherheit, da in der Vergangerheit immer mehr Vorfälle von Benutzung verschiedener Kundenkonten durch unbefugte Personen entstanden sind.

Um daher wie gewohnt weiterhin Ihr Konto bei uns nutzen zu können, ist Ihre aktive Mitwirkung erforderlich. Dies wird vom Gesetzgeber so verlangt.

Nachdem Sie sich über den Bestätigungsbutton angemeldet haben, werden Ihnen detailiert alle weiteren notwendigen Schritte erklärt.

Bestätigen

Bei Misachtung oder Verweigerung ist ganz klar eine Schließung des Kundenkontos vorgesehen. Der Gesetzgeber fordert in so einem Fall dazu auf.

Vielen Dank im voraus für Ihre Mitwirkung und Ihr Verständnis!

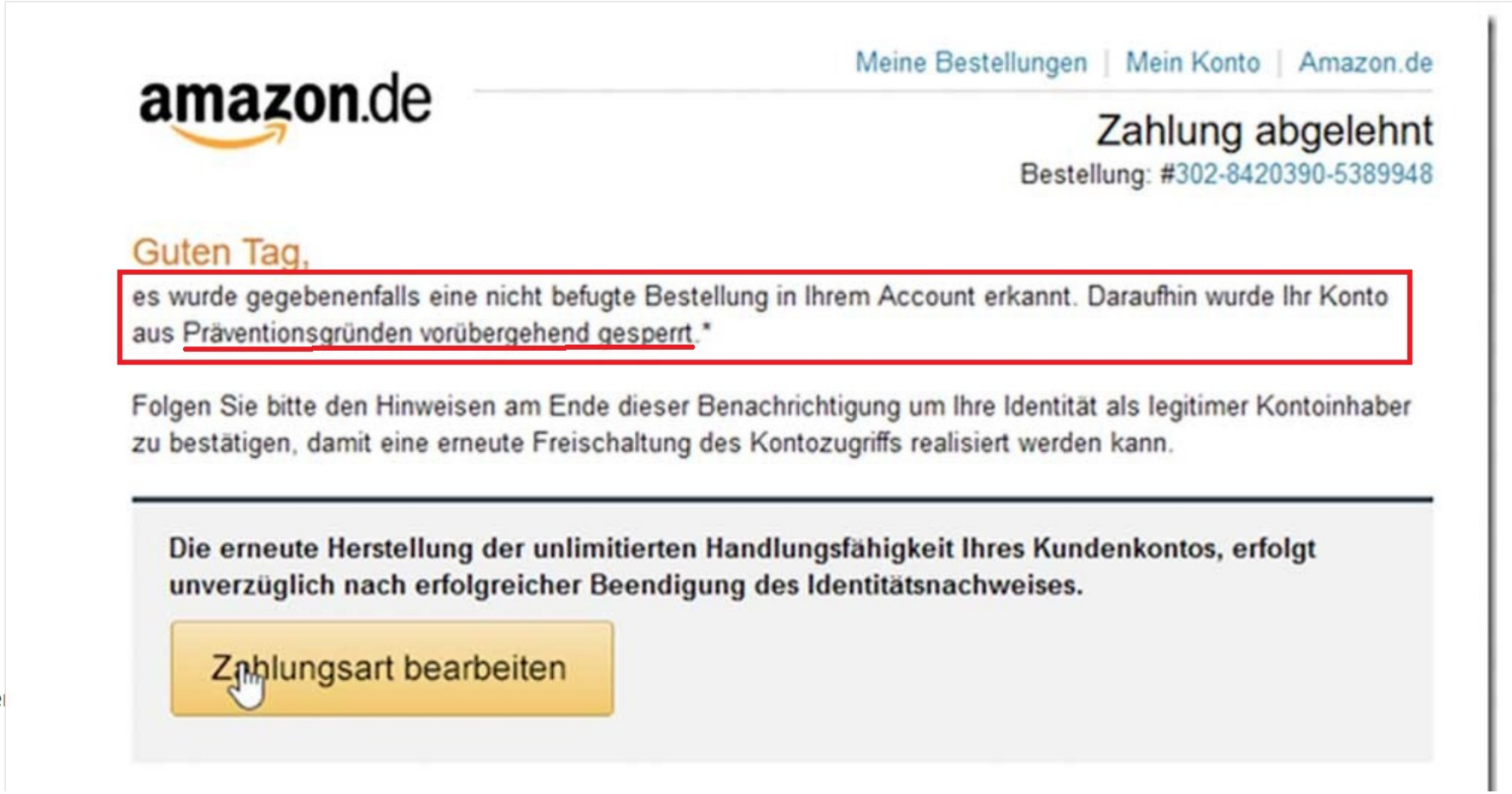
Mit freundlichen Grüßen
Ihr PayPal Kundensupport

Universität Regensburg

Elena Maria Kellinghaus
IT-Sicherheitsbeauftragte
Rechenzentrum

Merkmale einer Phishing-Mail – „Fake“-Mails erkennen

4. Dringender Handlungsbedarf



Universität Regensburg

Elena Maria Kellinghaus
IT-Sicherheitsbeauftragte
Rechenzentrum

Merkmale einer Phishing-Mail – „Fake“-Mails erkennen

5. Eingabe von Daten

Sollten Sie dazu aufgefordert werden, sich mit PIN oder TAN auf einer Seite einzuloggen, ist das ein Zeichen für eine Phishing-Mail. Seröse Absender würden Sie niemals darum bitten, da solche Eingaben immer nur auf verschlüsselten Websites eingegeben werden. Niemand außer Ihnen sollte Ihre Passwörter und TAN-Nummern kennen.

Universität Regensburg

Elena Maria Kellinghaus
IT-Sicherheitsbeauftragte
Rechenzentrum

Merkmale einer Phishing-Mail – „Fake“-Mails erkennen

6. Aufforderung zur Öffnung einer Datei
7. Links oder eingefügte Formulare

Eine sehr beliebte Masche von Online-Betrügern ist das Senden einer vermeintlichen Rechnung oder Mahnung im Anhang der E-Mail. Sobald Sie auf den Anhang klicken, wird sich zwar eine Datei öffnen, die installiert allerdings unbemerkt einen Virus auf Ihrem Computer. Sogar die gesamte Fernsteuerung und Echtzeit-Überwachung Ihres PCs sind dann möglich.

Für die Betrüger ein leichtes Spiel.

Klicken Sie niemals auf einen eingefügten Link.

Universität Regensburg

Elena Maria Kellinghaus
IT-Sicherheitsbeauftragte
Rechenzentrum

Merkmale einer Phishing-Mail – „Fake“-Mails erkennen

8. Bisher noch nie E-Mails von der Bank erhalten oder kein Kunde

Diesmal leichtes Spiel für Sie, denn wenn Sie gar kein Kunde bei dem vermeintlichen Absender der E-Mail sind, können Sie die Mail sofort in den Papierkorb befördern.

Zukünftiges Problem: Social Engineering!

…ist essenzieller Bestandteil aller forschrittlichen Cyber-Angriffe!
Konsequenz: Phishing-Mails werden immer mehr individualisiert auf den Empfänger zugeschnitten sein…

Das Medium Mail ist ungeeignet für die Weitergabe von Informationen wie z.B. Bewerbungen, Dokumentenaustausch.

Universität Regensburg

Elena Maria Kellinghaus
IT-Sicherheitsbeauftragte
Rechenzentrum

Merkmale einer Phishing-Mail – „Fake“-Mails erkennen

9. Verdächtige Absenderadresse

Universität Regensburg

Elena Maria Kellinghaus
IT-Sicherheitsbeauftragte
Rechenzentrum

Merkmale einer Phishing-Mail – „Fake“-Mails erkennen

9. Verdächtige Absenderadresse

Untersuchung des Mailheader

Manche Phishing-Mails sind sehr gut gemacht. Die Absender-E-Mailadresse scheint vertrauenswürdig, der Link im Text auch, das Deutsch ist flüssig? Trotzdem muss diese E-Mail nicht echt sein.

Auch Absenderangaben von E-Mails lassen sich fälschen. Wenn Sie - um letzte Zweifel auszuräumen - das prüfen wollen, müssen Sie sich den so genannten **Mail-Header** anschauen. Dort steht die IP-Adresse des Absenders. Nur diese ist fälschungssicher und gibt Aufschluss über den tatsächlichen Absender.

Universität Regensburg

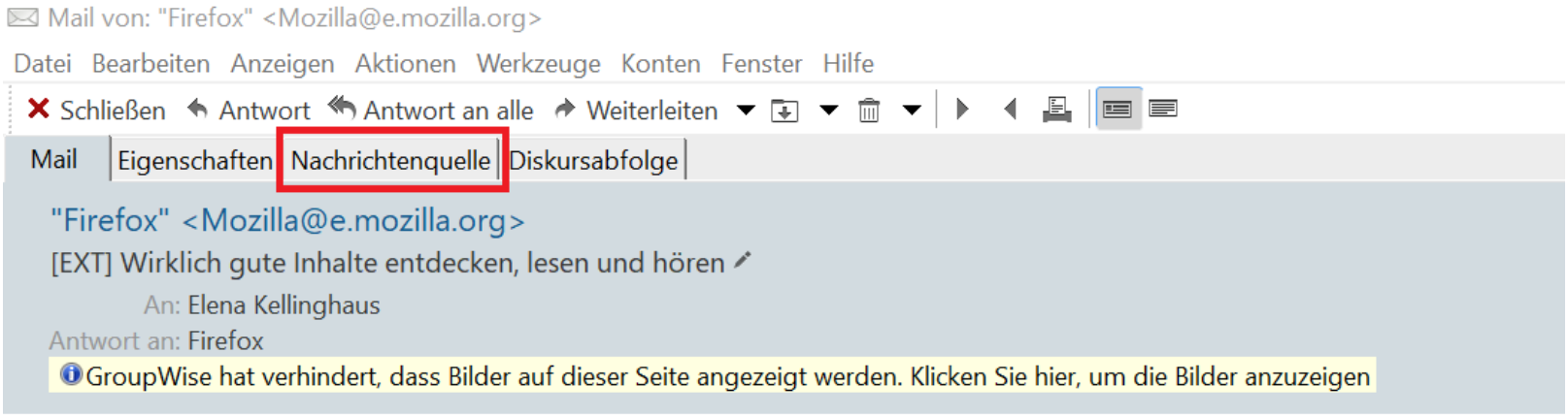
Elena Maria Kellinghaus
IT-Sicherheitsbeauftragte
Rechenzentrum

Merkmale einer Phishing-Mail – „Fake“-Mails erkennen

9. Verdächtige Absenderadresse

Untersuchung des Mailheader

In der geöffneten Mail befindet sich oberhalb des Absender ein Reiter „Nachrichtenquellen“. Diesen bitte auswählen.



Universität Regensburg

Elena Maria Kellinghaus
IT-Sicherheitsbeauftragte
Rechenzentrum

Merkmale einer Phishing-Mail – „Fake"-Mails erkennen

9. Verdächtige Absenderadresse

Untersuchung des Mailheader

```
Return-Path: <user31232@lws01.ldn5.groupnbt.net>
Received:
from mail.vz-nrw.de ([unix socket]) by mail (Cyrus
v2.2.13-Debian-2.2.13-10+etch4) with LMTPA; Tue, 04 Jan 2011 20:08:52
+0100
X-Sieve:
CMU Sieve 2.2
Envelope-to: finanzwissen@vz-nrw.de
Delivery-date: Tue, 04 Jan 2011 20:08:52 +0100
Received: from [172.16.1.4] (helo=astaro.vz-nrw.de) by
mail.vz-nrw.de with esmtp (Exim 4.63) (envelope-from
<user31232@lws01.ldn5.groupnbt.net>) id 1PaCFY-00015E-Kb for
finanzwissen@vz-nrw.de; Tue, 04 Jan 2011 20:08:52 +0100
Received: from lws01.netbenefit.co.uk ([62.128.158.4]:49352
helo=lws01.ldn5.groupnbt.net) by astaro.vz-nrw.de with esmtps
(TLSv1:AES256-SHA:256) (Exim 4.69) (envelope-from
<user31232@lws01.ldn5.groupnbt.net>) id 1PaCFW-0005Dx-26
for finanzwissen@vz-nrw.de; Tue, 04 Jan 2011 20:08:50
+0100
Received: from user31232 by lws01.ldn5.groupnbt.net with local
(Exim 4.63) (envelope-from <user31232@lws01.ldn5.groupnbt.net>) id
1PaCFW-0000pj-4q for finanzwissen@vz-nrw.de; Tue, 04 Jan 2011 19:08:50
+0000
X-CTCH-RefID:
str=0001.0A0B0205.4D237042.0231:SCFSTAT3589785,ss=1,fgs=0
An: finanzwissen@vz-nrw.de
Betreff: Achtung! Ihr PayPal-Konto wurde begrenzt!
```

E-Mailadresse des Absenders

Unter der Angabe "Return-Path" finden Sie den Absender der E-Mail, bzw. dessen E-Mailadresse. Steht hier eine kryptische E-Mail-Adresse, ist das schon ein Hinweis auf eine Phishing-Mail.

Universität Regensburg

Elena Maria Kellinghaus
IT-Sicherheitsbeauftragte
Rechenzentrum

Merkmale einer Phishing-Mail – „Fake“-Mails erkennen

9. Verdächtige Absenderadresse

Untersuchung des Mailheader

```
Return-Path: <user31232@lws01.ldn5.groupnbt.net>
Received:
from mail.vz-nrw.de ([unix socket]) by mail (Cyrus
v2.2.13-Debian-2.2.13-10+etch4) with LMTPA; Tue, 04 Jan 2011 20:08:52
+0100
X-Sieve:
CMU Sieve 2.2
Envelope-to: finanzwissen@vz-nrw.de
Delivery-date: Tue, 04 Jan 2011 20:08:52 +0100
Received: from [172.16.1.4] (helo=astaro.vz-nrw.de) by
mail.vz-nrw.de with esmtp (Exim 4.63) (envelope-from
<user31232@lws01.ldn5.groupnbt.net>) id 1PaCFY-00015E-Kb for
finanzwissen@vz-nrw.de; Tue, 04 Jan 2011 20:08:52 +0100
Received: from lws01.netbenefit.co.uk ([62.128.158.4]:49352
helo=lws01.ldn5.groupnbt.net) by astaro.vz-nrw.de with esmtps
(TLSv1:AES256-SHA:256) (Exim 4.69) (envelope-from
<user31232@lws01.ldn5.groupnbt.net>) id 1PaCFW-0005Dx-26
for finanzwissen@vz-nrw.de; Tue, 04 Jan 2011 20:08:50
+0100
Received: from user31232 by lws01.ldn5.groupnbt.net with local
(Exim 4.63) (envelope-from <user31232@lws01.ldn5.groupnbt.net>) id
1PaCFW-0000pj-4q for finanzwissen@vz-nrw.de; Tue, 04 Jan 2011 19:08:50
+0000
X-CTCH-RefID:
str=0001.0A0B0205.4D237042.0231:SCFSTAT3589785,ss=1,fgs=0
An: finanzwissen@vz-nrw.de
Betreff: Achtung! Ihr PayPal-Konto wurde begrenzt!
```

Empfänger

Die E-Mailadresse und den Mailserver des Empfängers finden Sie unter "Delivered-To" oder auch "Envelope-To" und unter dem ersten "Received"-Eintrag. Die Received-Einträge sind von unten nach oben zu lesen, deswegen ist der letzte Eintrag mit dem Namen "Received" derjenige, den der Mailserver des Empfängers beim Erhalt der Mail in den Header einträgt.

Universität Regensburg

Elena Maria Kellinghaus
IT-Sicherheitsbeauftragte
Rechenzentrum

Merkmale einer Phishing-Mail – „Fake“-Mails erkennen

9. Verdächtige Absenderadresse

Untersuchung des Mailheader

```
Return-Path: <user31232@lws01.ldn5.groupnbt.net>
Received:
from mail.vz-nrw.de ([unix socket]) by mail (Cyrus
v2.2.13-Debian-2.2.13-10+etch4) with LMTPA; Tue, 04 Jan 2011 20:08:52
+0100
X-Sieve:
CMU Sieve 2.2
Envelope-to: finanzwissen@vz-nrw.de
Delivery-date: Tue, 04 Jan 2011 20:08:52 +0100
Received: from [172.16.1.4] (helo=astaro.vz-nrw.de) by
mail.vz-nrw.de with esmtp (Exim 4.63) (envelope-from
<user31232@lws01.ldn5.groupnbt.net>) id 1PaCFY-00015E-Kb for
finanzwissen@vz-nrw.de; Tue, 04 Jan 2011 20:08:52 +0100
Received: from lws01.netbenefit.co.uk ([62.128.158.4]:49352
helo=lws01.ldn5.groupnbt.net) by astaro.vz-nrw.de with esmtps
(TLSv1:AES256-SHA:256) (Exim 4.69) (envelope-from
<user31232@lws01.ldn5.groupnbt.net>) id 1PaCFW-0005Dx-26
for finanzwissen@vz-nrw.de; Tue, 04 Jan 2011 20:08:50
+0100
Received: from user31232 by lws01.ldn5.groupnbt.net with local
(Exim 4.63) (envelope-from <user31232@lws01.ldn5.groupnbt.net>) id
1PaCFW-0000pj-4q for finanzwissen@vz-nrw.de; Tue, 04 Jan 2011 19:08:50
+0000
X-CTCH-RefID:
str=0001.0A0B0205.4D237042.0231:SCFSTAT3589785,ss=1,fgs=0
An: finanzwissen@vz-nrw.de
Betreff: Achtung! Ihr PayPal-Konto wurde begrenzt!
```

IP-Adresse des Absenders (der tatsächliche Absender!)

Die IP-Adresse, also die tatsächliche physikalische Adresse des Absenders, finden Sie weiter unten, innerhalb einer der nächsten "Received from"-Angaben. Das ist der Received-Eintrag, der die Übergabe der E-Mail vom Absender-Server an den Empfänger-Server dokumentiert. Der Absender-Server ist eindeutig kenntlich gemacht durch die so genannte IP-Adresse. Diese ist nicht fälschbar, steht in einer eckigen Klammer und lautet in diesem Fall *62.128.158.4*..