IT-UserDesk

Klaus Deiss
Neuenhofer Str. 6
42349 Wuppertal
Tel.: 49 (0) 202 – 7560706
Fax.: 49 (0) 202 – 7560705
www.it-userdesk.de

Erkennen Sie verseuchte Mails

Aus gegebenem Anlass möchten wir Ihnen in dieser Anleitung zeigen, wie Sie mit einfachen Mitteln erkennen können, ob eine Mail gefälscht ist.

Seien Sie bitte extrem vorsichtig im Umgang mit per Mail zugestellten Rechnungen.

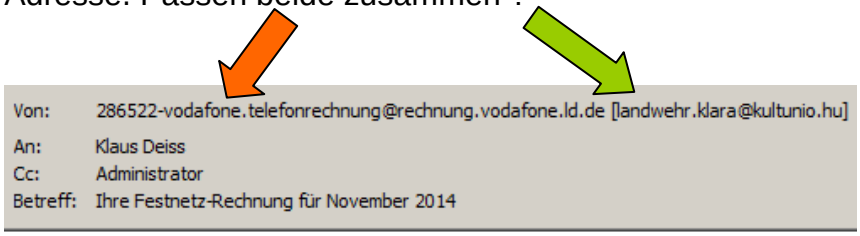
Es wäre zwar gerade für die großen Firmen wie Telekom, Vodafone und Sparkasse eine Kleinigkeit ihre Mails mit digitalen Zertifikaten zu signieren (und somit fälschungssicher zu machen).

Sie machen es aber aus uns unerfindlichen Gründen nicht und öffnen somit Gangsterbanden aus Nah und Fern Tür und Tor um sich Zugriff auf die Rechner ihrer Opfer zu verschaffen.

Die Angreifer setzen auf Ihre Neugierde - seien Sie sich dessen immer bewußt !!!

1) Schauen Sie auf den Absender !

E-Mail Adressen bestehen immer aus einem frei wählbaren Teil und der eigentlichen Adresse. Passen beide zusammen ?



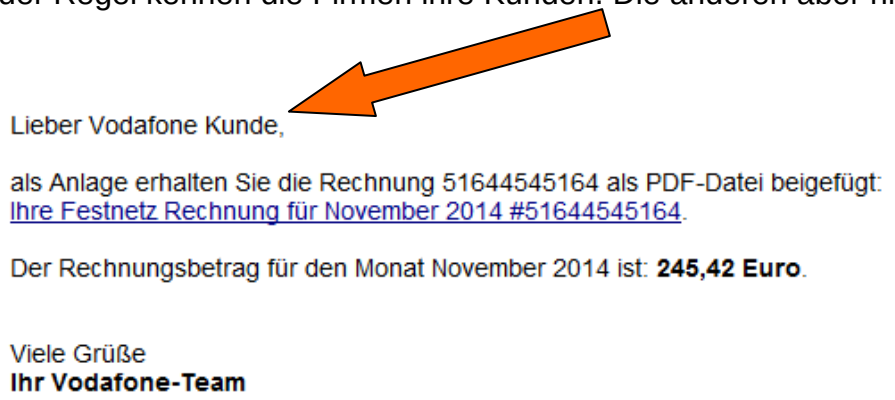
Ihre neue Rechnung ist online

Im Beispiel sendet Klara Landwehr aus Ungarn eine Mail für Vodafone. Diese Mail ist definitiv Spam oder Schlimmeres, ab in die Tonne !

Achtung: Es ist für Hacker kein Problem die Absenderadresse zu fälschen, eine Absenderadresse "Telekom Deutschland GmbH {NoReply} Noreply-Rechnung@telekom.de" bietet keinerlei Gewähr für die Echtheit des Absenders.

b) Achten Sie auf die Ansprache

In der Regel kennen die Firmen ihre Kunden. Die anderen aber nicht!



Lieber Vodafone Kunde,

als Anlage erhalten Sie die Rechnung 51644545164 als PDF-Datei beigefügt:
Ihre Festnetz Rechnung für November 2014 #51644545164.

Der Rechnungsbetrag für den Monat November 2014 ist: **245,42 Euro**.

Viele Grüße
Ihr Vodafone-Team

Ein echtes Schreiben dieser Firmen richtet sich i.d.R. stets an Sie persönlich !

c) Überprüfen Sie die Quelle des Downloads

Die Viren, Trojaner und Würmer liegen zu 100% auf Web Servern, die die Angreifer zuvor gekapert haben.

Sie können sehr leicht erkennen wohin der Download Link zeigt. Bewegen Sie den Mauszeiger über den Link. Ihnen wird der echte Link eingeblendet.

Ihre neue Rechnung ist online

Lieber Vodafone Kunde,

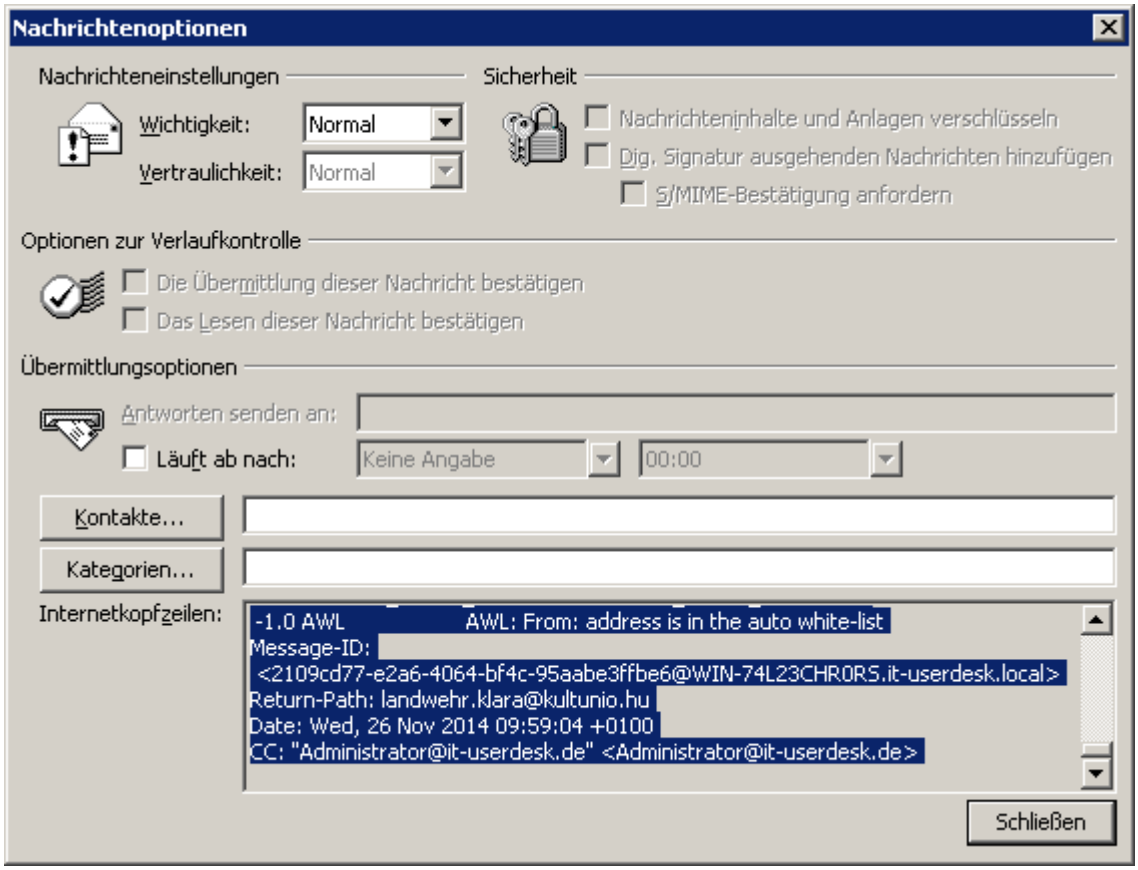
als Anlage erhalten Sie die Rechnung [illegible]644545164 als PDF-Datei beigefügt:
Ihre Festnetz Rechnung für November 2014 #51644545164.

Der Rechnungsbetrag für den M blocked::http://xinixz.com/wp-includes/5TSLKGPid2hVoq

Wenn Sie wirklich eine Rechnung von xinixz.com erwarten fahren Sie fort, ansonsten gehört diese Mail geschreddert!

d) Analysieren Sie den Header der Mail

Konnten die vorgenannten Schritte die Echtheit der Mail nicht sicher bestimmen, sollten Sie einen Blick auf den Header der Mail werden. Um die Header sichtbar zu machen bedarf es zumeist der Anwahl einer bestimmen Funktion im E-Mail Programm.



In OL2003 klicken Sie die Mail mit der rechten Maustaste an und wählen Optionen. In OL2007/2010 öffnen Sie die Mail, wählen dann Datei, dann Eigenschaften.

Kopieren Sie den Header am besten mit Strg+C und dann Strg+V in einen Texteditor oder Word, der besseren Lesbarkeit wegen.

Received: from briteon.com (195.70.36.102) by h1991771.stratoserver.net with
(AES256-SHA encrypted) SMTP; 26 Nov 2014 09:58:59 +0100

Received: from 213-193-107-74.static.cablecom.ch ([213.193.107.74]
helo=localhost) by briteon.com with esmtpsa
(TLS1.0:DHE_RSA_AES_256_CBC_SHA1:32) (Exim 4.72) (envelope-from
<landwehr.klara@kultunio.hu>) id 1XtXZ8-0003Tj-86 for k.deiss@it-userdesk.de;
Wed, 26 Nov 2014 09:03:15 +0100

Subject: Ihre Festnetz-Rechnung f??r November 2014
From: "286522-vodafone.telefonrechnung@rechnung.vodafone.ld.de"
<landwehr.klara@kultunio.hu>
To: k.deiss@it-userdesk.de

Suchen Sie den allerersten "**RECEIVED FROM**" Eintrag (von oben nach unten den Header absuchen). Jedes Transportsystem im Netz verewigt sich im Header mit einer solchen Zeile.

Die allerunterste Zeile beschreibt das System, welches die Mail ins Internet schickte. In diesem Fall ist das der Host 213-193-107-74.static.cablecom.ch mit der Adresse 213.193.107.74. Sie können über diese Adresse weitgehende Informationen abrufen. Rufen Sie dazu ein WHOIS Tool auf, z.B. folgende Internetseite:

http://www.heise.de/netze/tools/whois/

In diesem Fall handelt es sich um eine Firma aus der Schweiz, die Geschäftskunden Internetzugänge anbietet.

Sieht aus nach gekapertem Rechner in der Schweiz und nicht nach Vodafone Deutschland.

Entsorgen Sie diese Mail bitte sofort !