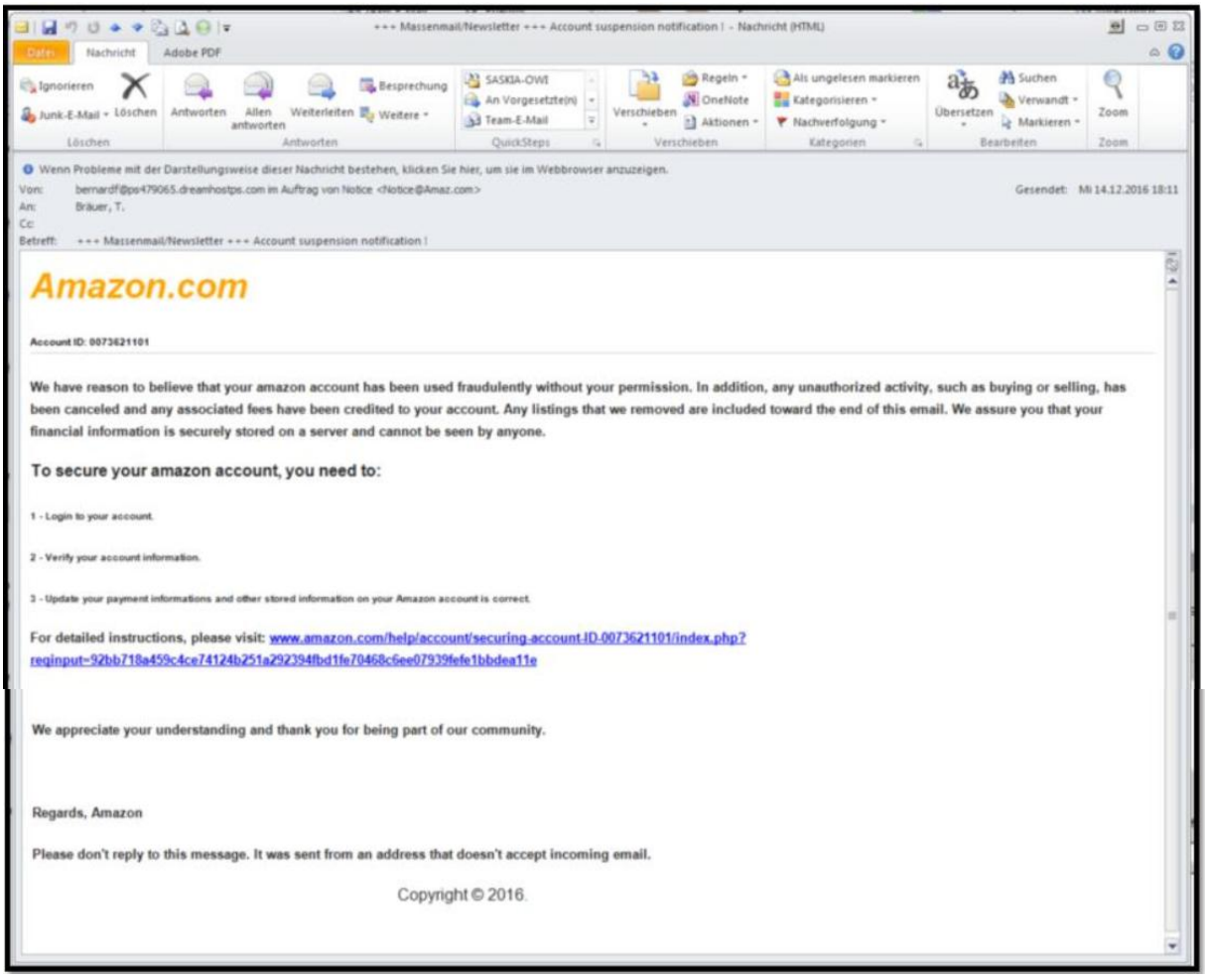
Liebe Kolleginnen und Kollegen,

der beste Schutz vor Viren- und Phishing-Attacken sind Vorsicht, Aufmerksamkeit und Wissen ☺.

Um letzteres wieder einmal zu erweitern bzw. aufzufrischen, möchte ich Ihnen heute mit einem Beispiel aus meinem Posteingang von heute zeigen, worauf Sie bei E-Mails mit enthaltenen Internet-Links achten können (sollten) um nicht in eine Falle zu tapsen:

Hier die Mail:




Auch wenn ich bei Amazon.de unter dieser Mailadresse Kunde bin, wundere ich mich schon, dass ich in englischer Sprache kontaktiert werde. Der Internet-Link, den ich anklicken soll um meine Zugangs- und Zahlungsdaten bei Amazon.com (nicht .de) zu überprüfen und zu korrigieren, sieht auf den ersten Blick ungefährlich aus, da er nicht als formatierter, einfach lesbarer Text-Link (z.B.: …please visit: Kundencenter AMAZON, oder klicken Sie hier) sondern **scheinbar** eben als komplette, unformatierte Internetadresse dargestellt wird.

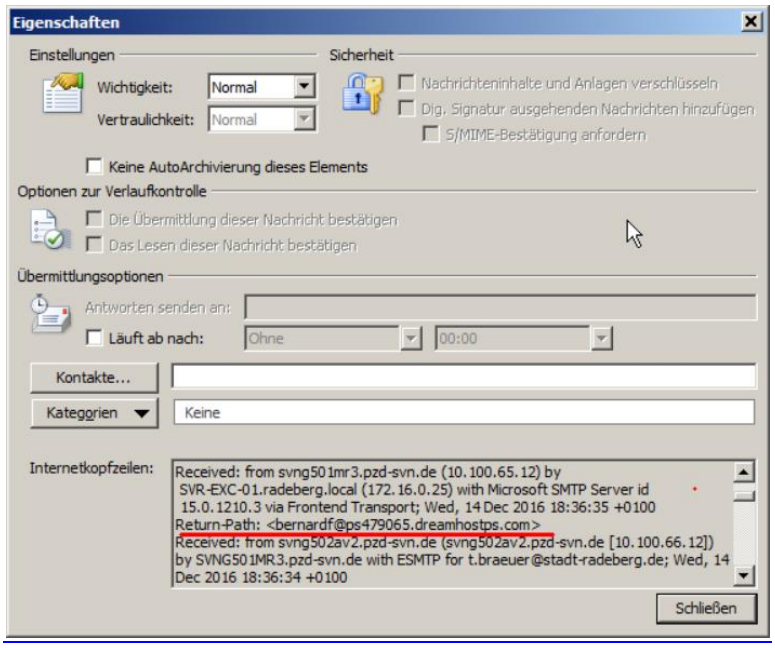
Da die Nachricht eh schon suspekt ist, zeige (nicht klicken!!) ich also mit dem Maus-Pfeil auf den Link und es erscheint eine kleine Sprechblase mit dem eigentlichen Ziel dieses Links:


Der da lautet: www.shizembetours.co.za/... Und das hat weder was mit www.amazon.de noch mit Reichen die bisherigen Hinweise (falsche Sprache, keine persönliche Anrede, verschleierte Internetlinks) nicht – es gibt durchaus Phishing-Mails, die deutlich cleverer und persönlicher gemacht sind als dieses Exemplar – hilft noch der Blick in die sogenannten Headerzeilen der Nachricht (Achtung, es wird technisch ;-)

**Anzeigen von Nachrichtenköpfen**

Outlook 2016, 2013 oder 2010:

- Klicken Sie in einer geöffneten E-Mail-Nachricht auf die Registerkarte Datei.
- Klicken Sie auf der Registerkarte Informationen auf Eigenschaften.
- Kopfzeileninformationen werden im Feld Internetkopfzeilen angezeigt.



## Es folg der komplette Inhalt der Internetkopfzeilen:


**Received:** from **SVR-EXC-01.radeberg.local** (172.16.0.25) by SVR-EXC-01.radeberg.local (172.16.0.25) with Microsoft SMTP Server (TLS) id 15.0.1210.3 via Mailbox Transport; Wed, 14 Dec 2016 18:36:37 +0100
**Received:** from **SVR-EXC-01.radeberg.local** (172.16.0.25) by SVR-EXC-01.radeberg.local (172.16.0.25) with Microsoft SMTP Server (TLS) id 15.0.1210.3; Wed, 14 Dec 2016 18:36:35 +0100
**Received:** from **svng501mr3.pzd-svn.de** (10.100.65.12) by SVR-EXC-01.radeberg.local (172.16.0.25) with Microsoft SMTP Server id 15.0.1210.3 via Frontend Transport; Wed, 14 Dec 2016 18:36:35 +0100
**Return-Path: <bernardf@ps479065.dreamhostps.com>**
**Received:** from **svng502av2.pzd-svn.de** (svng502av2.pzd-svn.de [10.100.66.12]) by SVNG501MR3.pzd-svn.de with ESMTP for t.braeuer@stadt-radeberg.de; Wed, 14 Dec 2016 18:36:34 +0100
**Received:** from **svng300mr2.pzd-svn.de** (unknown [217.7.17.137]) by svng502av2.pzd-svn.de with smtp
(TLS: TLSv1/SSLv3,256bits,ECDHE-RSA-AES256-GCM-SHA384)
id 0482 5b26 1d72a9f5 0b21 485d 9a60 47c33be5c395;
Wed, 14 Dec 2016 18:36:34 +0100
**Received: from ps479065.dreamhost.com ([64.111.108.91] helo=ps479065.dreamhostps.com)**
by svng300mr2.pzd-svn.de with esmtps (TLSv1.2:DHE-RSA-AES256-GCM-SHA384:256)
**(envelope-from <bernardf@ps479065.dreamhostps.com>)**
id 1cHDTm-0004Wz-E7
for t.braeuer@stadt-radeberg.de; Wed, 14 Dec 2016 18:36:34 +0100
**Received: by ps479065.dreamhostps.com** (Postfix, from userid 15963769)
id 7E999388888F32; Wed, 14 Dec 2016 09:11:18 -0800 (PST)
To: <t.braeuer@stadt-radeberg.de>
X-PHP-Originating-Script: 15963769:RebelfDz.php
**From: Notice <Notice@Amaz.com>**
MIME-Version: 1.0
Content-Type: text/html
Message-ID: <20161214171949.7E999388888F32@ps479065.dreamhostps.com>
Date: Wed, 14 Dec 2016 09:11:18 -0800
X-SGG-UMAMSID: 20161214173633Z17421svng300mr2.pzd-svn.de 1cHDTm-0004Wz-E7
X-SGG-RESULT: 20161214173633Z17421svng300mr2.pzd-svn.de C1:OK E1:FAIL MX1:OK BL:OK SPF:off CT:Bulk CM: SIP:64.111.108.91 SMF:bernardf@ps479065.dreamhostps.com
X-SGG-MF: bernardf@ps479065.dreamhostps.com
X-SGG-CTRefId: str=0001.0A0C0207.58517DD9.0155,ss=3,sh,re=0.000,recu=0.000,reip=0.000,cl=3,cld=1,fgs=0
X-Junkmail: UCE(40)
Sender: <bernardf@ps479065.dreamhostps.com>
X-WatchGuard-Spam-ID: str=0001.0A0C0207.58518323.001D,ss=3,re=0.000,recu=0.000,reip=0.000,cl=3,cld=1,fgs=0
X-WatchGuard-Spam-Score: 3, bulk; 0, virus threat unknown
X-WatchGuard-Mail-Client-IP: 10.100.65.12
X-WatchGuard-Mail-From: bernardf@ps479065.dreamhostps.com
X-WatchGuard-Mail-Recipients: t.braeuer@stadt-radeberg.de
Subject: +++ Massenmail/Newsletter +++ Account suspension notification !
X-WatchGuard-AntiVirus: part scanned. clean action=allow
X-MS-Exchange-Organization-Network-Message-Id: 87b26c65-1ddc-4cbb-252b-08d42447c03a
X-MS-Exchange-Organization-AuthSource: SVR-EXC-01.radeberg.local

Interessant hier sind vorallem die „Received:"-Zeilen. Diese dokumentieren von oben nach unten in umgekehrter Reihenfolge die bei der Übermittlung der Nachricht beteiligten Mailserver. Und hier tauchen neben unseren eigenen „svr-wxc-01" und den Mailservern des Sächs. Verwaltungsnetztes „svn…@pzd-svn.de" nur noch einer mit der Domäne „dreamhostsps.com" auf – kein einziger Server stammt von amazon.com oder amazon.de!

Damit ist der letzte Zweifel über die Vertrauenswürdigkeit dieser Mail ausgeräumt und der beste Weg, sie zu entsorgen ist die geschlossene Mail in der Ordneransicht bei gedrückter Umschalttaste zu löschen. Damit wird sie nicht erst in den Papierkorb verschoben, sondern gleich richtig gelöscht.

Wie immer zum Schluss der Hinweis: Wenn Sie sich bei einer Mail nicht sicher sind, fragen Sie Ihren Admin ;-). Vier Augen sehen mehr als zwei. Sollte ich länger nicht erreichbar sein (Urlaub…), ist es ratsam, eine verdächtige Mail ein paar Tage unbeachtet zu lassen. Falls sich in den Anlagen doch ein Virus versteckt oder die enthaltenen Links zu bösen Seiten führen, ist die Wahrscheinlichkeit der Entdeckung durch unsere Schutzprogramme deutlich höher, als gleich am Tag des Mail-Eingangs.

Mit freundlichen Grüßen

T. Bräuer
EDV-Verantwortlicher
Stadtverwaltung Radeberg
Markt 19, 01454 Radeberg
Tel. : 03528 / 450-217
Fax : 03528 / 450-100
E-Mail:

mailto://t.braeuer@stadt-radeberg.de
www : http://www.radeberg.de