

Wie man eine Phishing E-Mail erkennt

Anhand echter Phishing E-Mail wird im folgenden gezeigt wie diese erkannt werden können. Oft sind es kleine Ungereimtheiten die die Phishing E-Mail als solche entlarven.

Adresse des Absenders

Der erste Ansatzpunkt ist die Adresse des Absenders. Wenn diese Adresse seltsam aussieht seien Sie vorsichtig. **Achtung:** In den meisten Fällen sind diese Adresse den Originalen ähnlich, aber nicht identisch. Es lohnt sich auch, die Absender Adresse und die E-Mail Adresse, welche in der E-Mail selbst angegeben ist, zu vergleichen. In der Beispiel E-Mail stimmen diese zwei Adressen nicht überein. Ein weiterer Hinweis ist die falsche Telefonnummer, der Absender hat angeblich eine E-Mail Adresse aus dem Bereich der Universität Freiburg, aber die Vorwahl seines Büroanschlusses ist nicht die Vorwahl von Freiburg.

[Nachrichtenliste](#) | [ungelesen](#) | [Löschen](#) [Vorherige](#) | [Nächste](#) [Weiterleiten](#) | [Als Anhang weiterleiten](#) | [Antworten](#) | [Alle](#)

Betreff: [redacted]
Von: "Marc Zinggeler" <ingresos2@lapilarica.com.mx>
Datum: [redacted]
An: it@informatik.uni-freiburg.de
Priorität: Normal
Optionen: [Alle Kopfzeilen anzeigen](#) | [Druckversion zeigen](#) | [Dies als Datei herunterladen](#)
| [Nachrichtendetails anzeigen](#) | [Add to Address Book](#)

Guten Morgen,

Ihre Rechnung vom 06.11.2018 können Sie jetzt abrufen.
Die Summe beträgt 1,803.51
€ und ist am 09/11/2018 fällig.

Wir freuen uns weiterhin auf eine gute Zusammenarbeit.

Viele Grüße

Marc Zinggeler
-
Büro: +49 8946 5935-99
Fax: +49 8946
[redacted]
[Mail: zinggele@informatik.uni-freiburg.de](mailto:zinggele@informatik.uni-freiburg.de)

Diese eMail kann vertrauliche und/oder rechtlich geschützte Informationen enthalten. Wenn Sie nicht der richtige Adressat sind oder diese E-Mail irrtümlich erhalten haben, informieren Sie bitte sofort den Absender und vernichten Sie diese eMail.
Das unerlaubte Kopieren sowie die unbefugte Weitergabe dieser E-Mail ist nicht gestattet.

Anhänge:
[RECH-A-1113-21476.doc](#) 108 k [application/msword] [Herunterladen](#)

Ungewöhnlicher Betreff

Ein ungewöhnlicher Betreff ist ein guter Hinweis auf eine Phishing E-Mail. Auch wenn die E-Mail scheinbar von einer bekannten Adresse stammt (z.B. von einem Kollegen oder Vorgesetzten) verrät der ungewöhnliche Betreff die E-Mail.

Betreff Beispiel: Prof.Dr. Max Mustermann Electronic invoice 460788520

Sollten Sie Zweifel haben, ob die E-Mail wirklich von der als Absender angegeben Person stammt, ist dies meist berechtigt.

Unpersönliche Anrede

Wenn Sie eine E-Mail erhalten, die mit „Sehr geehrte Damen und Herren“ oder ähnlichem beginnt, kann es sich um eine Phishing-E-Mail handeln. Zumindest, wenn die E-Mail angeblich von einem Kollegen / einem Bekannten / einem Freund oder einem Unternehmen stammt, das Sie normalerweise persönliche in einer E-Mail anspricht.

Ungewöhnliche Formatierung

Rechnung haben in der Regel bestimmte Formatierungsvorgaben, auch im Fall, dass sie per E-Mail zugestellt werden.

Rechnung Beispiel:

Zwischensumme ohne USt.: EUR 75,58

Umsatzsteuer: EUR 14,35

Endbetrag inkl. USt.: EUR 89,93

und nicht

Die Summe beträgt 1,803.51

€ und ist am 09/11/2018 fällig.

Diese Zahlungsaufforderung enthält mehrere offensichtliche Fehler. Zum einen würde es keinen Zeilenumbruch zwischen Betrag und Währungszeichen (€) geben und zum anderen fehlt der Ausweis der Umsatzsteuer. Weitere Fehler sind die Darstellung als Punktzahl (anstelle Kommazahl), die ebenso wie das verwendete Datumsformat in Deutschland sehr ungewöhnlich sind.

Aufforderung zur Bestätigung persönlicher Daten

Viele Phishing E-Mails erfordern die Bestätigung persönlicher Daten. Einige enthalten auch Drohungen wie „Wenn Sie Ihre Daten nicht angeben, wird Ihr Konto gesperrt / geschlossen. Dies geschieht oft in Verbindung mit einer Frist. Diese Aufforderung umfassen meist sehr spezifische Informationen über Sie / Ihr Konto oder vertrauliche Daten wie PIN, TAN oder ein Passwort. Gelegentlich wird auch nach der Anschrift beziehungsweise dem Geburtstag gefragt.

Weder Unternehmen noch die Universität werden Sie in einer E-Mail nach solchen

Informationen fragen.

Links zu Webseiten

Wenn Sie unsicher sind, ob Sie gefahrlos auf einen Link in einer E-Mail klicken können, **klicken Sie nicht**. Die angezeigte Adresse muss nicht identisch sein mit der Adresse auf die der Link verweist.

Sollten Sie die angegebene Seite dennoch besuchen wollen, tippen Sie die Adresse manuell in die Browser Leiste oder Suchen diese Adresse (oder Teile davon) per Google.

Häufig führen diese Links zu Seiten, auf denen automatisch ein Virus oder ähnliches heruntergeladen wird.

E-Mail Anhang

In keinem Fall Anhänge von verdächtigen E-Mails öffnen. Auch nicht in vermeintlichen Ausnahmesituationen.

Wenden Sie sich im Zweifel an Ihre lokale Systemadministration / Benutzerbetreuung.

Neben E-Mail stehen heutzutage eine Vielzahl von weiteren Kommunikationskanälen für Rückfragen zur Verfügung.

From:

<https://wiki.uni-freiburg.de/tf-infoportal/> - **Entwicklungs-Wiki für das Infoportal der Technischen Fakultät**

Permanent link:

<https://wiki.uni-freiburg.de/tf-infoportal/doku.php?id=imtek:phishing>

Last update: **2019/03/19 17:39**

