Europa-Universität Flensburg
Zentrum für Informations- und Medientechnologien (ZIMT)

Europa-Universität Flensburg | Auf dem Campus 1 | 24943 Flensburg

Angehörige der
Europa-Universität Flensburg

Jürgen Frahm
IT-Administrator

Besucheranschrift
Europa-Universität Flensburg
Auf dem Campus 1a
Erweiterungsbau (EB) | Raum 333
24943 Flensburg

Tel. +49 461 805 2878
Fax +49 461 805 95 2878
Juergen.frahm@uni-flensburg.de

Flensburg, 08. Mai 2017

Verhaltensregeln im Umgang mit SPAM-E-Mails

Sehr geehrte Damen und Herren,
sehr geehrte Kolleginnen und Kollegen,

diese Information erläutert kurz, welche Möglichkeiten derzeit an der EUF bestehen, mit unerwünschten E-Mails umzugehen und liefert einige Hinweise, welche Vorkehrungen von den Benutzern für einen relativ sicheren Umgang mit E-Mails getroffen werden sollten.

1. Was ist „Spam"?
Spam bezeichnet das massenweise Auftreten von E-Mails und Newsartikeln, die nicht angefordert wurden. In den meisten Fällen handelt es sich dabei um Werbung, oft mit pornografischem Inhalt und Kettenbriefe, sowie durch Viren versandte E-Mails.

2. Welche Auswirkungen hat SPAM?
Der Kampf gegen Spam ist mit viel Aufwand und auch Kosten verbunden. Durch das Speichern von Spam in den Mailkonten werden nicht nur unnötig Ressourcen im Netz und auf Servern belegt. Auch geht wertvolle Arbeitszeit durch die Kontrolle und das Löschen von Spam bzw. durch die ständige Pflege von Filterregeln zum Aussortieren derartiger E-Mails verloren. Beim Sichten von Spam besteht zudem die Gefahr, dass hierbei schädliche Programme eingeschleust werden und Rechner oder Netz lahmlegen.

2.1 Was macht das ZIMT?
Universitätsweit wird ein effizientes Verfahren mit dem Produktnamen „IronPort" eingesetzt. Hierbei werden alle eingehenden E-Mails bereits vor der Annahme automatisch auf SPAM untersucht und bei einer positiven SPAM-Erkennung abgelehnt bzw. in die SPAM-Quarantäne geschoben. Trotz dieser Möglichkeit ist leider eine hundertprozentige SPAM-Erkennungsrate nicht möglich. Unsere derzeitige Erkennungsrate liegt bei 98,9 %.
Daher werden bei Ihnen auch weiterhin vereinzelt unerwünschte E-Mails ankommen, die Sie mit der notwendigen Vorsicht und Skepsis behandeln sollten.

- **Das ZIMT wird Sie niemals per E-Mail anschreiben und nach Ihren Zugangsdaten fragen!**

Z I M T

- **Das ZIMT wird Ihnen niemals E-Mails zusenden, in denen Links enthalten sind, die auf Webseiten verweisen, auf denen Sie Ihre Zugangsdaten eingeben sollen!**

2.2 Was kann ich selber tun?
Anbei ein paar Verhaltensregeln:

Misstrauen Sie dem E-Mail-Inhalt
E-Mails können leicht von Dritten manipuliert werden.

- Misstrauen Sie E-Mails, deren Inhalt Ihnen verdächtig vorkommt.
- Lassen Sie sich von Sicherheitswarnungen oder generell von Androhungen via E-Mails nicht beeindrucken. Löschen Sie solche E-Mails!
- Überlegen Sie, ob Sie einem Unternehmen (z.B. Amazon) tatsächlich diese E-Mailadresse mitgeteilt haben.

Misstrauen Sie unbekannten Absendern
Absenderadressen können leicht gefälscht werden. Trauen Sie deshalb auch
keinem bekannten Absender, wenn Ihnen der Inhalt verdächtig erscheint.

- Antworten Sie auf keine E-Mail eines Ihnen unbekannten Absenders
- Löschen Sie E-Mails ungelesen bei denen Sie den Absender nicht kennen oder schon in der Betreffzeile verdächtige Wörter vorkommen.

Öffnen Sie keinen unbekannten Anhang
Hinter E-Mailanhängen versteckt sich oftmals Schadsoftware, welche sich beim Öffnen auf Ihrem Rechner einschleust.

- Öffnen oder speichern Sie keinen verdächtigen oder unbekannten Anhang und löschen Sie die E-Mail!
- Typisch kritische E-Mailanhänge sind wie folgt: Bilder (z.B. jpg- oder gif-Dateien), ppt-Dateien, doc-Dateien, xls-Dateien, pdf-Dateien

Folgen Sie keinem unbekannten Link
E-Mails enthalten häufig Links oder Verweise auf betrügerische Internetseiten.

- Folgen Sie keinem Link und löschen Sie verdächtige E-Mails.
- Klicken Sie nie auf einen Link der mit «Remove me» oder « Unsubscribe » bezeichnet ist
- Sollten Sie Mails von Banken o.ä. erhalten, benutzen Sie nicht die Links in der E-Mail selbst, sondern öffnen Sie die Website manuell durch direkte Eingabe der Adresse in Ihrem Browser
- Typisch verdächtige Links wie z.B. promote.de, success.com
- Links mit Schreibfehlern z.B. uni-fensburg.de

Versenden Sie keine Zugangsdaten per E-Mail
Vermeiden Sie beim Versenden oder Weiterleiten von E-Mails die Angabe von Zugangsdaten!

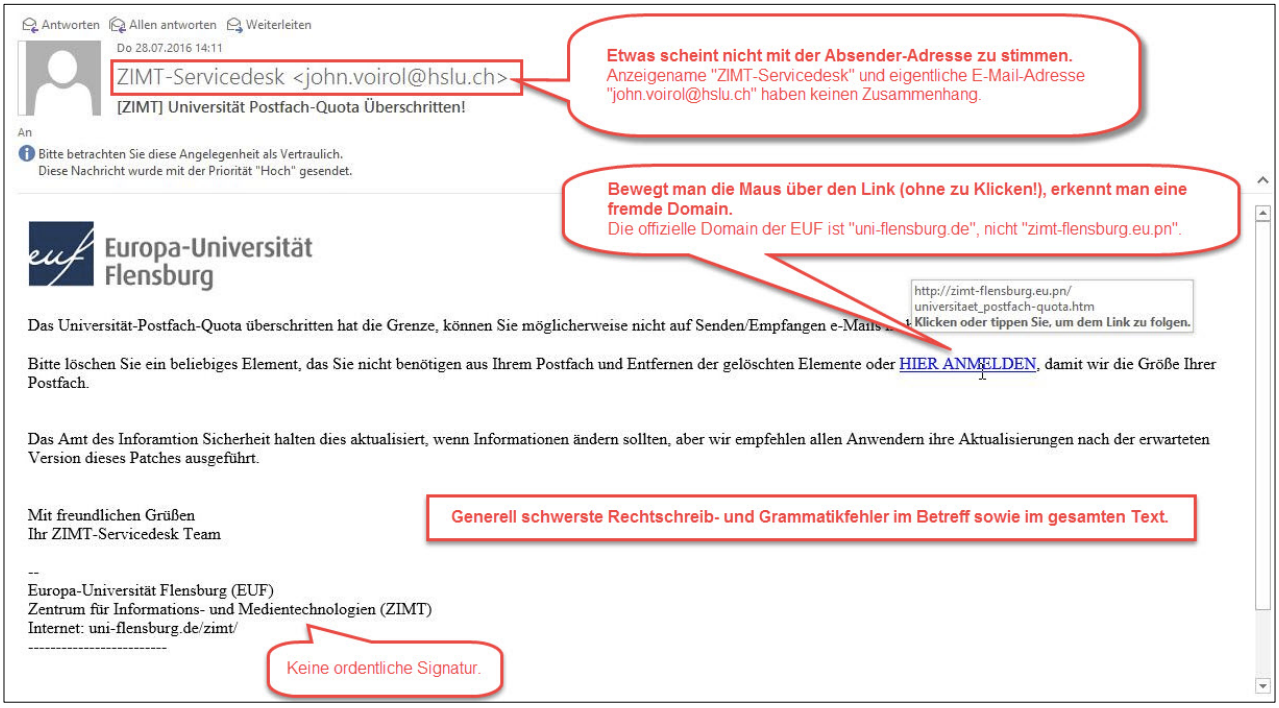
Falls Sie sich bei einer E-Mail absolut nicht sicher sein sollten, ob es sich um SPAM handelt, wenden Sie sich bitte vertrauensvoll an den ZIMT-Service (Tel.-Nr. 2112) oder den Postmaster (Tel.-Nr. 2878).

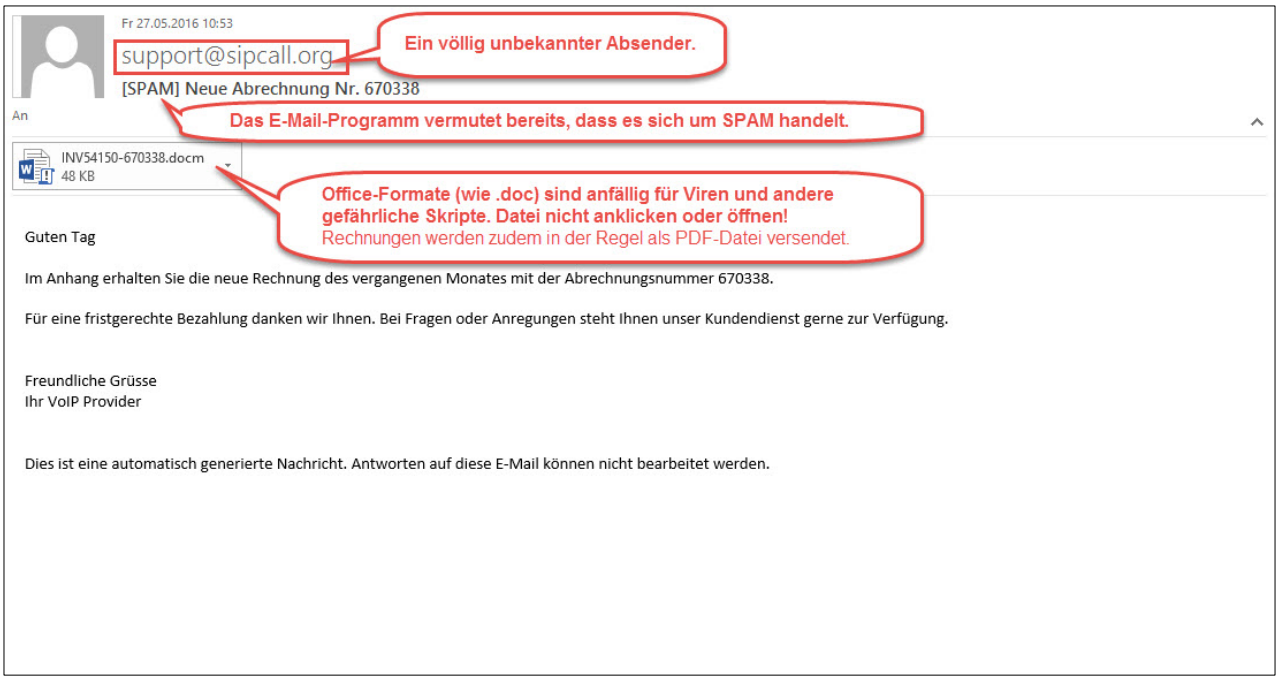
Mit freundlichen Grüßen

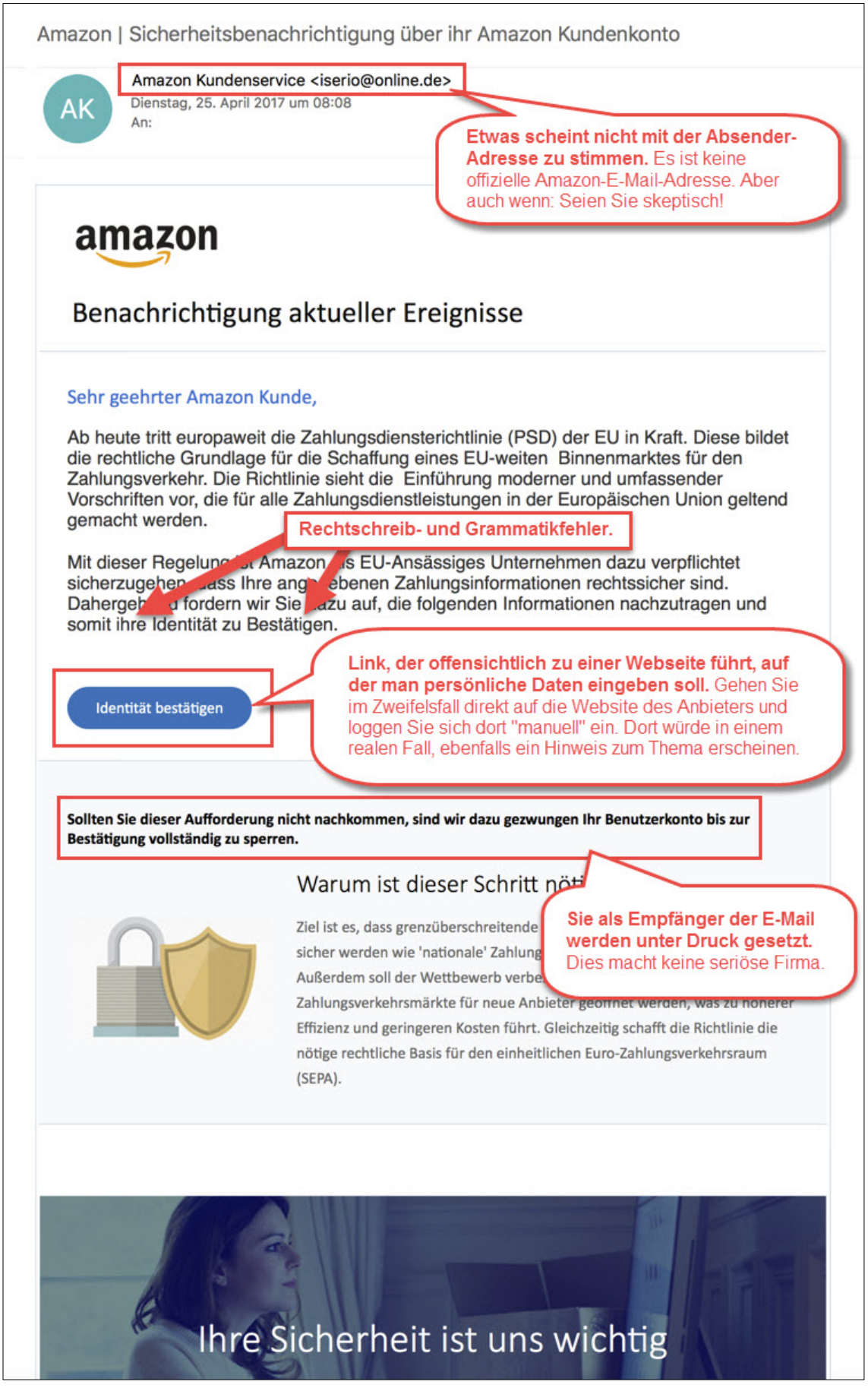
Jürgen Frahm
Postmaster

Europa-Universität Flensburg

Typische Beispiele für SPAM-E-Mails






Amazon | Sicherheitsbenachrichtigung über ihr Amazon Kundenkonto
AK
Amazon Kundenservice <iserio@online.de>
Dienstag, 25. April 2017 um 08:08
An:
Etwas scheint nicht mit der Absender-Adresse zu stimmen. Es ist keine offizielle Amazon-E-Mail-Adresse. Aber auch wenn: Seien Sie skeptisch!
amazon
Benachrichtigung aktueller Ereignisse
Sehr geehrter Amazon Kunde,
Ab heute tritt europaweit die Zahlungsdiensterichtlinie (PSD) der EU in Kraft. Diese bildet die rechtliche Grundlage für die Schaffung eines EU-weiten Binnenmarktes für den Zahlungsverkehr. Die Richtlinie sieht die Einführung moderner und umfassender Vorschriften vor, die für alle Zahlungsdienstleistungen in der Europäischen Union geltend gemacht werden.
Rechtschreib- und Grammatikfehler.
Identität bestätigen
Link, der offensichtlich zu einer Webseite führt, auf der man persönliche Daten eingeben soll. Gehen Sie im Zweifelsfall direkt auf die Website des Anbieters und loggen Sie sich dort "manuell" ein. Dort würde in einem realen Fall, ebenfalls ein Hinweis zum Thema erscheinen.
Sollten Sie dieser Aufforderung nicht nachkommen, sind wir dazu gezwungen Ihr Benutzerkonto bis zur Bestätigung vollständig zu sperren.
Warum ist dieser Schritt nöti
Sie als Empfänger der E-Mail werden unter Druck gesetzt. Dies macht keine seriöse Firma.
Effizienz und geringeren Kosten führt. Gleichzeitig schafft die Richtlinie die nötige rechtliche Basis für den einheitlichen Euro-Zahlungsverkehrsraum (SEPA).
Ihre Sicherheit ist uns wichtig

Europa-Universität Flensburg