

Angehörige der
Europa-Universität Flensburg

Flensburg, 08. Mai 2017

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

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!**



- **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 unbekanntem 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 unbekanntem Absenders
- Löschen Sie E-Mails ungelesen bei denen Sie den Absender nicht kennen oder schon in der Betreffzeile verdächtige Wörter vorkommen.

Öffnen Sie keinen unbekanntem Anhang

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

- Öffnen oder speichern Sie keinen verdächtigen oder unbekanntem 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 unbekanntem 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

Typische Beispiele für SPAM-E-Mails

Antworten | Allen antworten | Weiterleiten

Do 28.07.2016 14:11

ZIMT-Servicedesk <john.voirol@hslu.ch>
[ZIMT] Universität Postfach-Quota Überschritten!

An

Bitte betrachten Sie diese Angelegenheit als Vertraulich.
Diese Nachricht wurde mit der Priorität "Hoch" gesendet.

 Europa-Universität
Flensburg

Das Universität-Postfach-Quota überschritten hat die Grenze, können Sie möglicherweise nicht auf Senden/Empfangen e-Mails.

Bitte löschen Sie ein beliebiges Element, das Sie nicht benötigen aus Ihrem Postfach und Entfernen der gelöschten Elemente oder [HIER ANMELDEN](#), damit wir die Größe Ihrer Postfach.

Das Amt des Inforamtion Sicherheit halten dies aktualisiert, wenn Informationen ändern sollten, aber wir empfehlen allen Anwendern ihre Aktualisierungen nach der erwarteten Version dieses Patches ausgeführt.

Mit freundlichen Grüßen
Ihr ZIMT-Servicedesk Team

--
Europa-Universität Flensburg (EUF)
Zentrum für Informations- und Medientechnologien (ZIMT)
Internet: uni-flensburg.de/zimt/

http://zimt-flensburg.eu.pn/universitaet_postfach-quota.htm
Klicken oder tippen Sie, um dem Link zu folgen.

Generell schwerste Rechtschreib- und Grammatikfehler im Betreff sowie im gesamten Text.

Keine ordentliche Signatur.

Etwas scheint nicht mit der Absender-Adresse zu stimmen.
Anzeigename "ZIMT-Servicedesk" und eigentliche E-Mail-Adresse "john.voirol@hslu.ch" haben keinen Zusammenhang.

Bewegt man die Maus über den Link (ohne zu Klicken!), erkennt man eine fremde Domain.
Die offizielle Domain der EUF ist "uni-flensburg.de", nicht "zimt-flensburg.eu.pn".

Fr 27.05.2016 10:53

support@sipcall.org
[SPAM] Neue Abrechnung Nr. 670338

An

INV54150-670338.docm
48 KB

Guten Tag

Im Anhang erhalten Sie die neue Rechnung des vergangenen Monats mit der Abrechnungsnummer 670338.

Für eine fristgerechte Bezahlung danken wir Ihnen. Bei Fragen oder Anregungen steht Ihnen unser Kundendienst gerne zur Verfügung.

Freundliche Grüsse
Ihr VoIP Provider

Dies ist eine automatisch generierte Nachricht. Antworten auf diese E-Mail können nicht bearbeitet werden.

Ein völlig unbekannter Absender.

Das E-Mail-Programm vermutet bereits, dass es sich um SPAM handelt.

Office-Formate (wie .doc) sind anfällig für Viren und andere gefährliche Skripte. Datei nicht anklicken oder öffnen!
Rechnungen werden zudem in der Regel als PDF-Datei versendet.

Amazon | Sicherheitsbenachrichtigung über ihr Amazon Kundenkonto



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!



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.

Mit dieser Regelung ist Amazon als EU-Ansässiges Unternehmen dazu verpflichtet sicherzugehen, dass Ihre angegebenen Zahlungsinformationen rechtssicher sind. Daher gehen wir davon aus, dass Sie dazu auf, die folgenden Informationen nachzutragen und somit ihre Identität zu Bestätigen.

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.

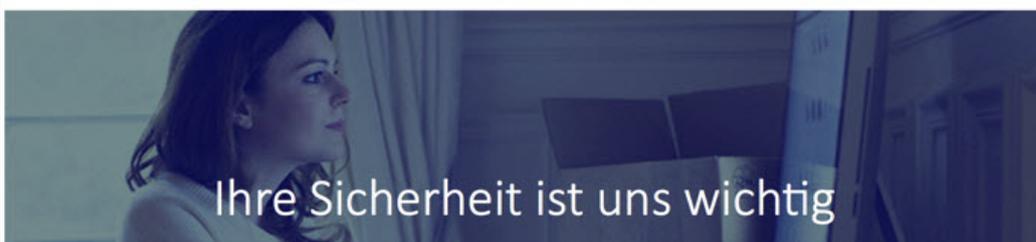
Sollten Sie dieser Aufforderung nicht nachkommen, sind wir dazu gezwungen Ihr Benutzerkonto bis zur Bestätigung vollständig zu sperren.

Warum ist dieser Schritt nötig?



Ziel ist es, dass grenzüberschreitende Zahlungen sicher werden wie 'nationale' Zahlungen. Außerdem soll der Wettbewerb verbessert werden. Zahlungsverkehrsmärkte für neue Anbieter geöffnet werden, was zu höherer Effizienz und geringeren Kosten führt. Gleichzeitig schafft die Richtlinie die nötige rechtliche Basis für den einheitlichen Euro-Zahlungsverkehrsraum (SEPA).

Sie als Empfänger der E-Mail werden unter Druck gesetzt. Dies macht keine seriöse Firma.



So 11.12.2016 16:16
warnung@deutschebank.de <christian@the-clothing-company.de>
[SUSPECTED SPAM] Ihr Konto wurde eingefroren, Christian Berger

An Berger, Christian
Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den auto

 **Deutsche Bank Mitteilung**

Sehr geehrter Herr Christian Berger,

leider mussten wir aus technischen Gründen Ihr Deutsche-Bank Konto temporär einfrieren, da es zu Unstimmigkeiten in Bezug auf Ihren persönlichen Adressdaten gekommen ist, welche veraltet oder ungültig sind. Wir bitten Sie, diese schnellstmöglich zu aktualisieren, da es sonst zu einer dauerhaften Sperre führen kann.

[Jetzt beheben!](#)

Nach einem Login werden Sie automatisch nach einer Aktualisierung gebeten, welche zwei Minuten Ihrer Zeit erfordert und eine sofortige entsperrung Ihres Kontos herbeiführt.

Wir danken Ihnen,
Ihr Serviceteam der Deutschen Bank

© 2016 Deutsche Bank Privat- und Geschäftskunden AG, Frankfurt am Main

Die Absender-Adresse ist verdächtig.
"warnung@deutschebank.de" ist nur der sogenannte Anzeigename. Die eigentliche Absende-E-Mail-Adresse steht in <>-Klammern dahinter.

Das Logo ist verzerrt dargestellt und die Farben stimmen nicht. Eine große Firma würde das niemals zulassen.

Banken versenden in der Regel keine direkten Links.

Rechtschreibfehler enthalten. Große Konzerne lassen Ihre E-Mails vor dem Versand mehrfach Korrekturlesen.

Stellen Sie sich vorab immer gleich zwei Fragen:
1. Bin ich überhaupt Kunde bei dem angeblichen Unternehmen?
2. Habe ich ihm **diese** E-Mail-Adresse zur Verfügung gestellt?