



E-Mail[©]

Gefahrenerkennung

DEUTSCHE FERNSEHLOTTERIE gGmbH • Axel-Springer-Platz 3 • 20355 Hamburg

0344027/224

155974/1111/042

Gefahrenabwehr

An alle, die Millionen gewinnen und
gleichzeitig Tausenden helfen möchten

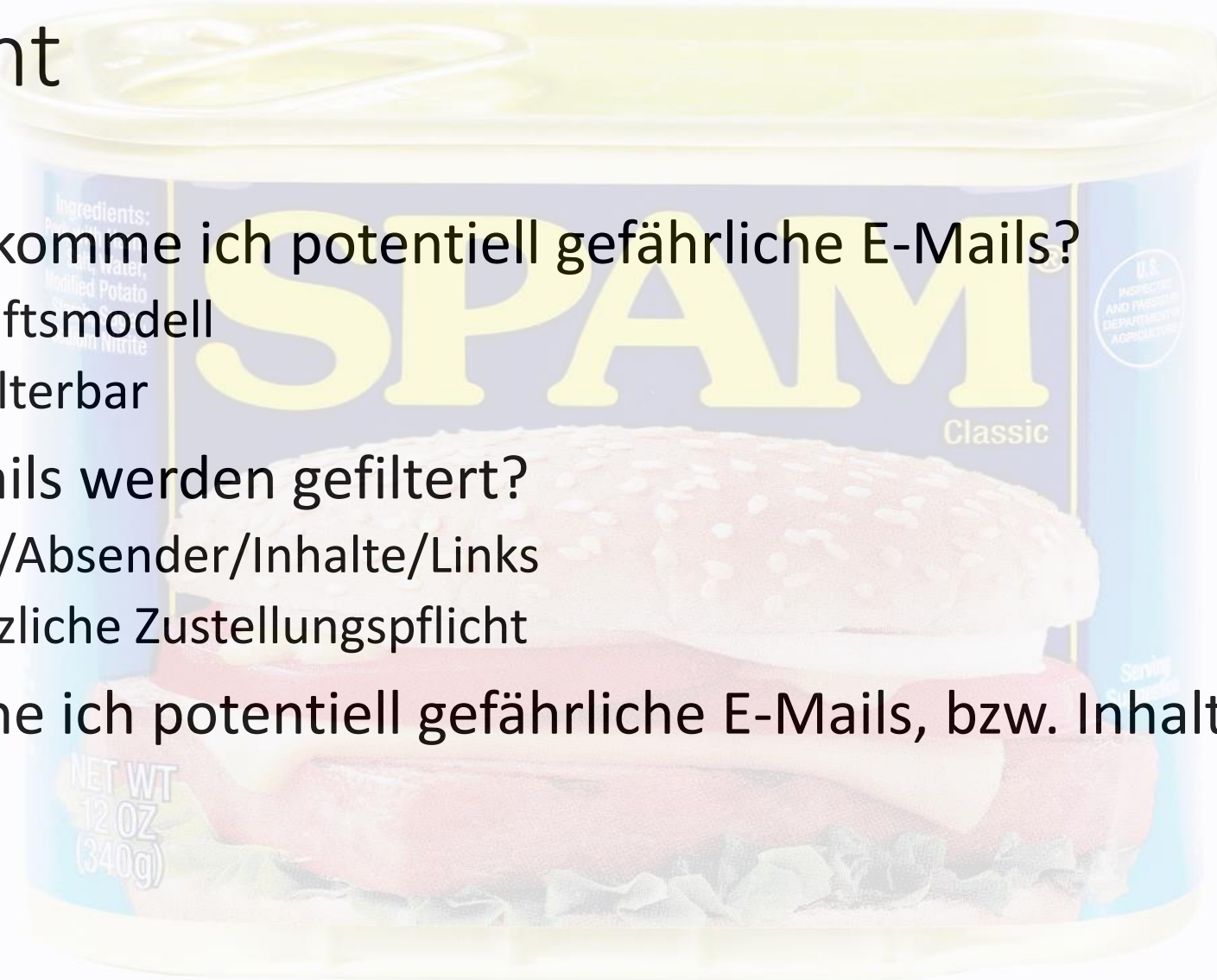
67346 Speyer



JETZT MITSPIELEN, HELFEN UND
BIS 1.500.000 EURO GEWINNEN!

Übersicht

- Warum bekomme ich potentiell gefährliche E-Mails?
 - a) Geschäftsmodell
 - b) nicht filterbar
- Welche Mails werden gefiltert?
 - Anhänge/Absender/Inhalte/Links
 - grundsätzliche Zustellungspflicht
- Wie erkenne ich potentiell gefährliche E-Mails, bzw. Inhalte?



Geschäftsmodell / Hintergrund

- 2022: ~90% „unerwünschte“ E-Mails
- tech. Kosten einer Mail¹: 0,7g CO₂ oder 0,1Wh, leider: 0 Cent
- Kosten Spam/Phishing: ~1Cent/Empfänger

Kriminelle Netzwerke benötigen Mailserver mit guter Reputation, diese werden häufig ihrerseits in Phishing-Kampagnen akquiriert.

Mittlerweile tritt unerwünschte Werbung (SPAM) in den Hintergrund, häufiger sind kriminelle Ziele (Erpressung, Ausspähen von Daten), meist über die Verteilung von Malware.

¹ „How Bad are Bananas?“
Mike Berners-Lee, 2010

Filterung

Grundsatz: Mail muss zugestellt werden

Filter: **Malware** wird meist mit Mustererkennung detektiert. Dies ist nur bedingt zuverlässig, darum werden ausführbare Dateien (einschließlich aktiver Inhalte in Dokumenten!) entfernt.

Versandadressen lassen sich nur bedingt als Kriterium für eine automatische Filterung nutzen, gleiches gilt für den **Inhalt**, insbesondere **Links**.

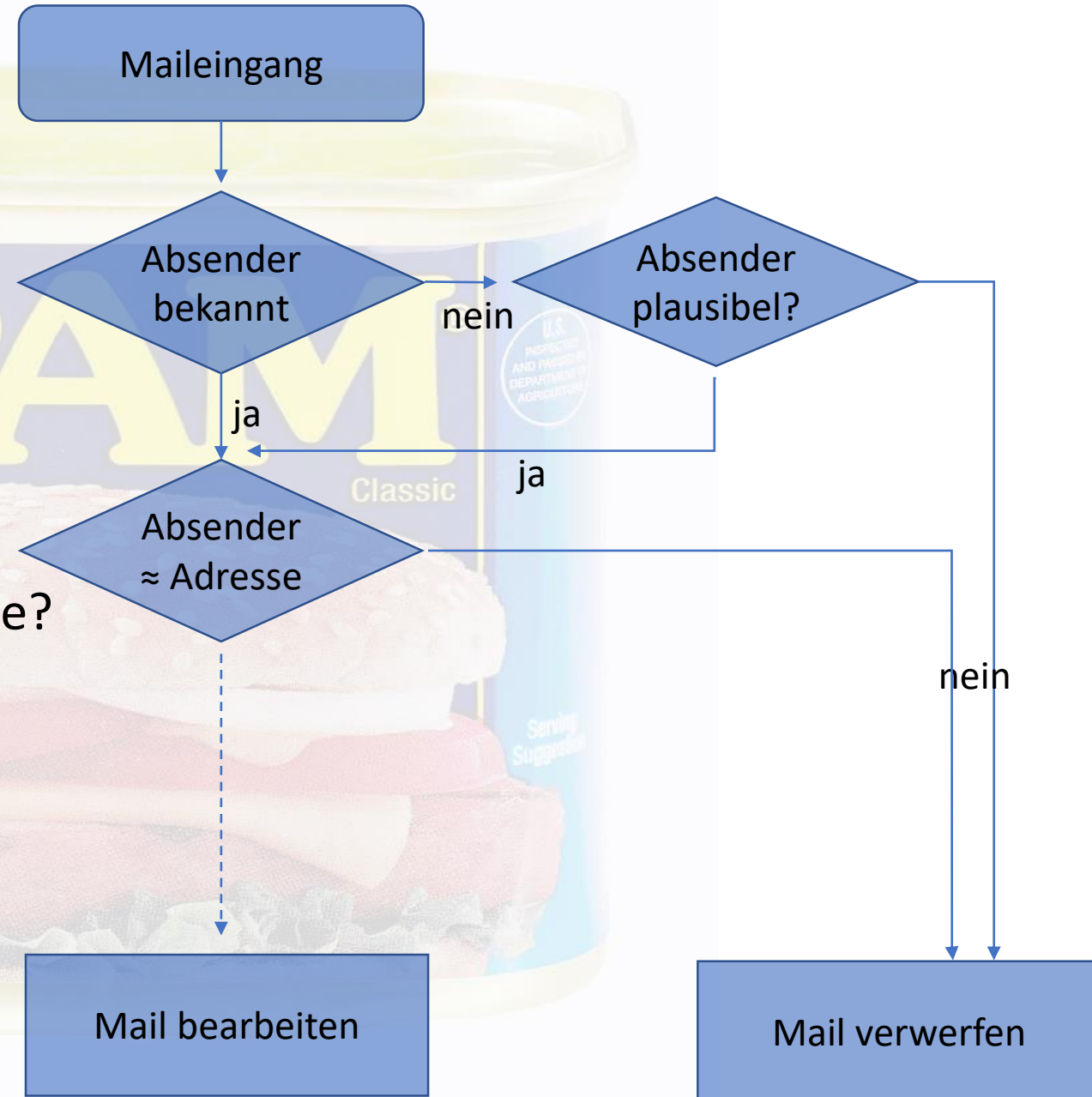
Eine inhaltsbasierte Filterung wird zunehmend aufwendiger und ineffektiver.

Weiteres Filterkriterium ist die Reputation des Ausgangsservers, inkl. historischer Daten wie typischer Mailvolumina.

Erkennung I

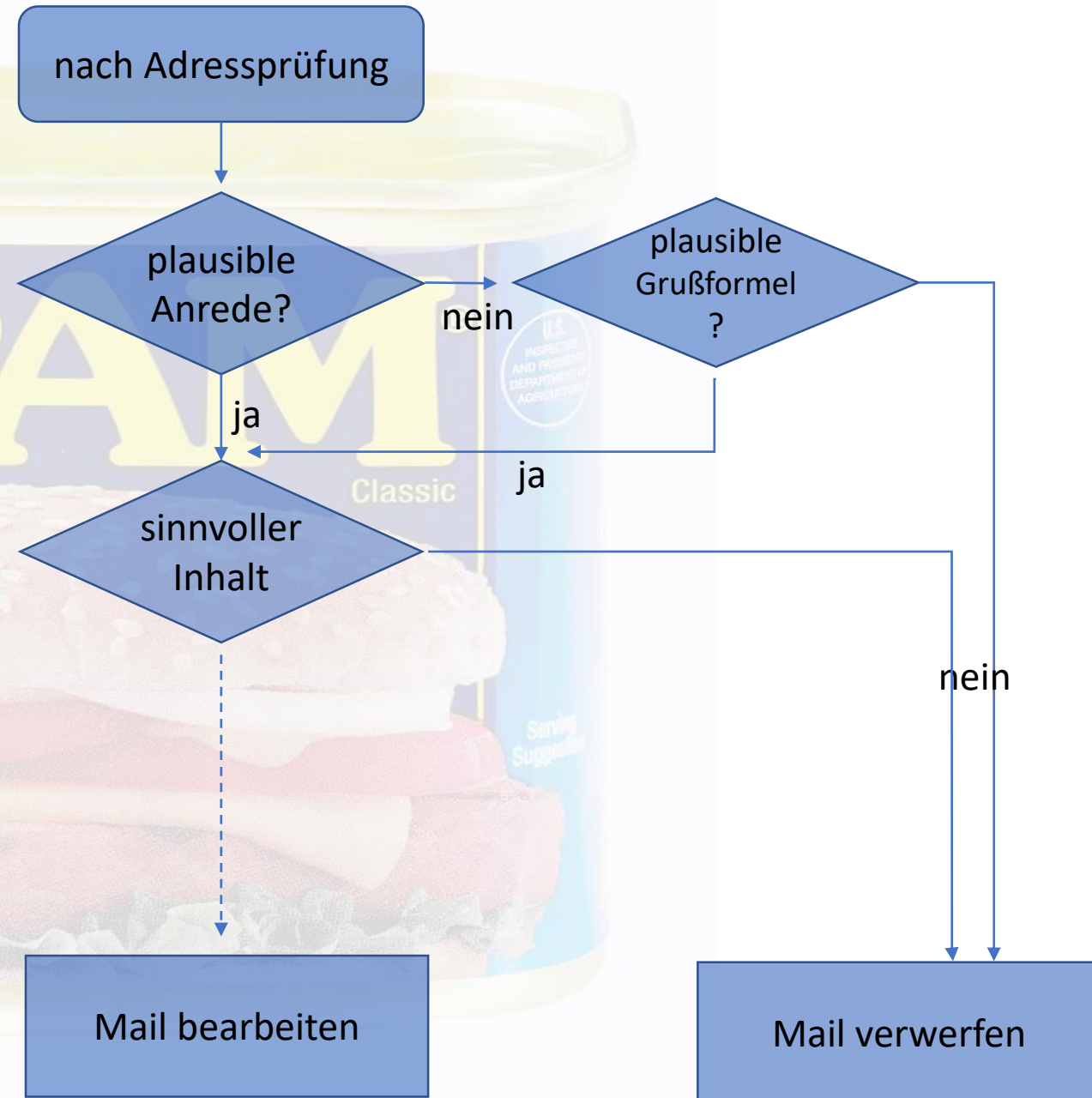
- Absender – Teil 1 (sozial)
 - Kenne ich den Absender?
 - Wenn nein, plausibel?
- Absender – Teil 2 (technisch)
 - Entspricht der Absender der Adresse?
 - Paßt die Adresse zum Versandweg?

Mailheader beachten!



Erkennung II

- Inhalt – Teil 1 (sozial)
 - Stimmt die Anrede/Grußformel?
 - Sinnvoller Inhalt?
 - Auffällige Fehler?
- Inhalt – Teil 2 (technisch)
 - Sinnvolle Links (URL beachten)?
 - Anhänge?



Filterung III

- Warum bekomme ich kein vollständiges Rezept für die Spamerkennung?



Beispiele – klassische SPAM-Mail



Antworten Allen antworten Weiterleiten



Do 13.04.2023 02:48

HondroFrost <imhajyn@easye.nov.su>

Gelenkschmerzen loswerden

An singler@uni-landau.de



Freigegebene einzigartige inländische medizinische Entwicklung.
Wird seit 1960 des XX Jahrhunderts von Astronauten verwendet, deren Gelenke unter Schwerelosigkeit starken degenerativen Veränderungen ausgesetzt waren. Das Medikament beugte alle pathologischen Prozesse in der Gelenkkapsel bei Verletzung von Stoffwechselprozessen, erhöhter körperlicher Anstrengung und pathologischer Veränderung von Gelenken vor.

[Hondrofrost >>](#)

**Das einzige nanotechnologische Medikament, da Gelenke auf natürliche Art und Weise wiederherstellt.
Die patentierte Formel hat keine Analoga!**

INNOVATIVE ENTWICKLUNG!
HONDROFROST

- Stellt in 99% der Fälle das Gewebe beschädigter Gelenke wieder her!
- Stoppt in nur 10 Minuten den Schmerz.
- Verleiht Gelenken in nur 14 Tagen die Beweglichkeit!
- Genesung und Unterstützung der Gelenke auf Mikroebene.
- Die patentierte Formel hat keine Analoga!

Best Price

**Stellt in 99% der Fälle das Gewebe beschädigter Gelenke wieder her!
Stoppt in nur 10 Minuten den Schmerz.
Verleiht Gelenken in nur 14 Tagen die Beweglichkeit!
Genesung und Unterstützung der Gelenke auf Mikroebene.**

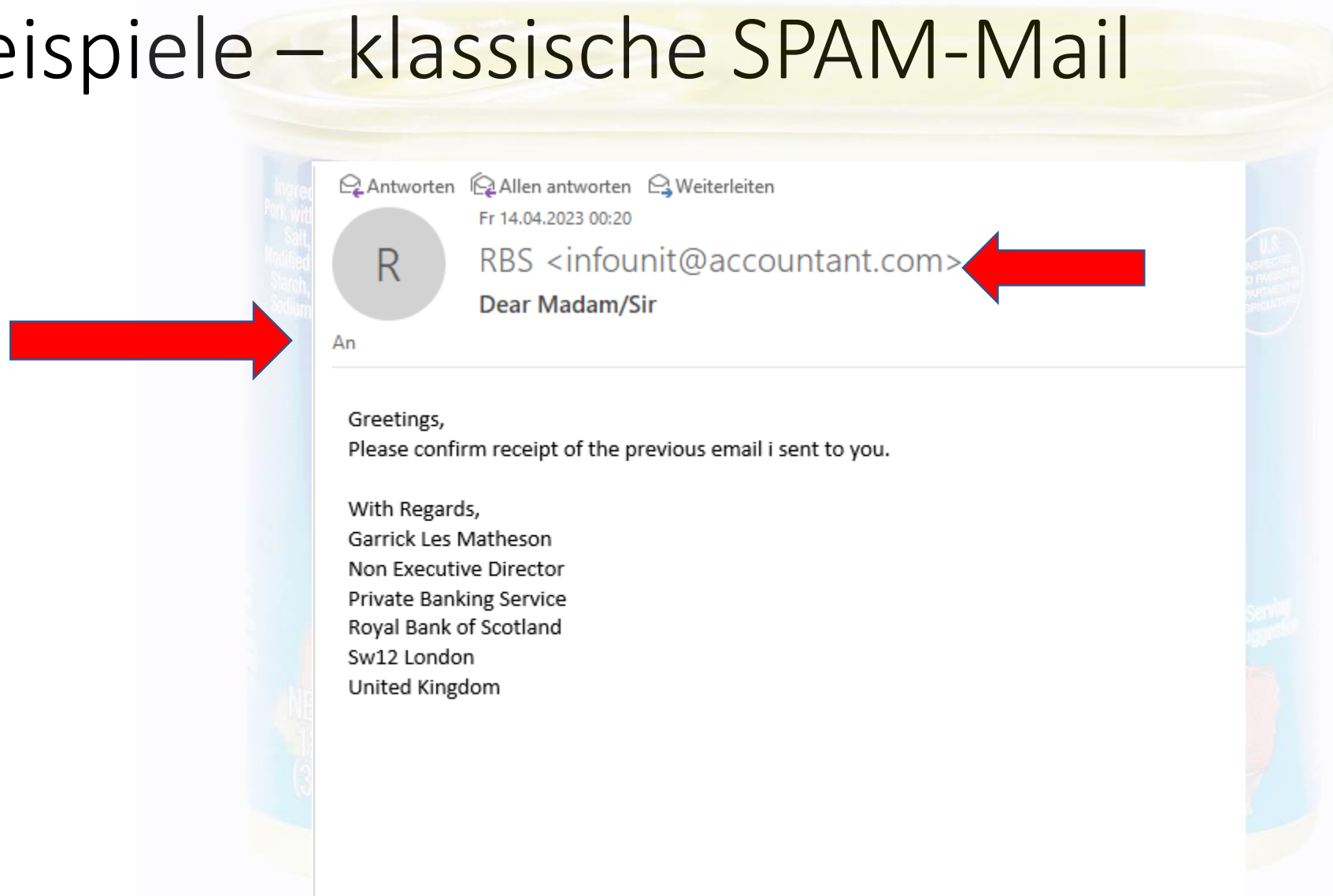
[Wem wird das Hondrofrost empfohlen >>](#)

Jetzt gilt der günstiger Preis!

Schnelle Lieferung in ganz Deutschland und der EU



Beispiele – klassische SPAM-Mail



Beispiele – klassische SPAM-Mail

Antworten Allen antworten Weiterleiten

Mi 12.04.2023 14:07



Mini-Handstaubsauger <support@holidayanddestinations.com>

Aw: Einfache Reinigung für Auto Zuhause Küche Tierhaare -32% Rabatt

An Hoffmann, Hendrik

Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.

Hallo,

Der Handstaubsauger ist mit mehreren verschiedenen Düsen zum Reinigen an verschiedenen Orten ausgestattet, mit denen Sie jede Ecke reinigen können.

Und es kann mit verschiedenen Abfällen, Staub, Papierresten, Haaren und Schmutz los reinigen.

Praktisch zum Entfernen von Schmutz in engen Ecken und Zwischenräumen, der perfekte Autobegleiter.

http://tracking.shoppingdirect.shop/index.php/
campaigns/ak54542rhg7ea/track-url/
bp527ww4gpaeb/
cce5ee1b526e5ba6fae253129372d19d3bc1da5
Klicken oder tippen Sie, um dem Link zu folgen.


>> [Klicken Sie hier, um Mini-Handstaubsauger zum Sonderpreis zu bestellen 32% RABATT](#)


Viele liebe Grüße,
Mini-Handstaubsauger


H&F
Sredskistraße 34
Berlin 12524
Germany

[abmelden](#) | [Weniger E-Mails erhalten?](#)

Beispiele – Malware

○ **Linda Evans (via Google Drive)** <drive-shares-noreply@google.com> 12.4.2023 17:37 

An  **Kopie** carstikowski@web.de, virginie.levi@yahoo.de, simione.boie@web.de, emind@bluewin.ch, dirkveit@gmx.net, kingman48@gmx.de, 46020441460204@gmail.com, grhandels@aol.com, hasylein82@web.de, castors.lodge@gmx.de, schweitzer.patrick@gmail.com, mark.weisheit@gmx.de, inezdrews@googlemail.com, christianschilitz@web.de, info@cnielsen.de, jasminschultes@yahoo.com, bad.salzuflen@bundk.de, muggensturm@googlemail.com, malikrahim26@gmail.com, mschmidtj@web.de, laeti.spilmont@laposte.net, gagagawolf@gmail.com, bernhard0703@gmx.de, andreaheitele@aol.com, mdahl387@gmail.com, hedkezzip@googlemail.com, amire_isuf@hotmail.com, weissenbacher.martina@hotmail.com




[Antworten](#) [Allen antworten](#) [Weiterleiten](#) [Löschen](#) 

Linda Evans shared a folder



Linda Evans (felbankwebta1989@dj.t.gsft.quest) has shared a link to the following folder:

niasahourgpecde

  1274 3UR [Holen Sie es sich jetzt](#) 

[Open](#)

Beispiele – Phishing

Bitte überprüfen Sie Ihre Daten [6.4.2023]

○ Ihr DKB berater - Maria Hoffmann <it@10iro.jp>

6.4.2023 14:14

An

Antworten

Allen antworten

Weiterleiten

Löschen



DKB

Hallo @gmX.de

Bitte bestätigen Sie Ihre Daten, um prüfen zu können, ob Ihr Konto vom Datenleck vom 3. April 2023 betroffen war.

Andernfalls wird Ihr Konto vorübergehend gesperrt, bis Sie sich zur Bestätigung der Daten in der nächstgelegenen Filiale melden.

Wir entschuldigen uns bei allen unseren Kunden für diese Unannehmlichkeiten, aber nur mit Ihrer Hilfe können wir betrügerische Konten erkennen oder die Gefahr laufen, betrogen zu werden, da unser Callcenter für die nächsten 72 Stunden gesperrt ist.

Kunden-ePortal

Wenn Sie diese E-Mail ignorieren und sich weigern, Ihre Daten zu bestätigen, kann dies zu erheblichen Verlusten führen, und die Bank übernimmt diese Verluste nicht.

Hinweis: Bitte antworten Sie nicht an die E-Mail-Adresse des Absenders, da die Adresse nur zum Senden von E-Mails konfiguriert ist.

Ihr DKB

Beispiele – Phishing

Antworten Allen antworten Weiterleiten

Mo 17.04.2023 07:32



Postbank <goedemondt@sympatico.ca>

Neue Info

E5UXH3T

An ingdebanking@bugfoo.com

Postbank Sicherheitswarnung

Guten Tag, geschätzter Kunde,

Damit Sie weiterhin vollständig an der Anwendung Postbank BestSign teilnehmen können, bitten wir Sie, das neue Sicherheitsupdate einzureichen um eine weitere Unterbrechung unseres Dienstes zu vermeiden.

[Jetzt ausfüllen](#)

Dieser Prozess dauert nur wenige Minuten und hilft uns, Ihr Konto besser gegen verdächtige Aktivitäten zu schützen. Wir empfehlen Ihnen dringend, dieses Formular so bald wie möglich auszufüllen, um Unterbrechungen bei Ihren Transaktionen zu vermeiden.

E5UXH3T

https://mgmail.harvestapp.com/c/eJxczr1uhyAUQPgnkOByVRIVKmr28cunQ-w_lh3orff8YUHddcW25YdHoAlAMjx8Fy01vQItHm0-re1ZHx2mg_P31a6ejSfueENG5Uq5-JLY4CTARaGA4BJgETYsRgxcCjhElJlhwoiREMHwzGfuRCCqZ6-IFYHFY0Jw2RatSzBdo-E_U1TdBIGENpo9g_yNKMV9NIqtrrlPEtt5FsjXo14bZT2NZDqhUi1zke-Sod5a8SLHW72c8pf9zctd2xUH655yvnJ7Kp0PCsLvRBS2

Beispiele – Phishing (Header)

Authentication-Results: mailgate-3.zdv.net; dkim=none (message not signed) header.i=none; spf=Pass smtp.mailfrom=goedemondt@sympatico.ca; spf=Pass smtp.helo=postmaster@cmx-torrigo001.bell.net

Received-SPF: Pass (mailgate-3.zdv.net: domain of goedemondt@sympatico.ca designates 209.71.212.29 as permitted sender) identity=mailfrom; client-ip=209.71.212.29;

receiver=mailgate-3.zdv.net;
envelope-from="goedemondt@sympatico.ca";
x-sender="goedemondt@sympatico.ca"; x-conformance=spf_only;
x-record-type="v=spf1"; x-record-text="v=spf1
ip4:206.47.72.0/24 ip4:184.150.200.0/24 ip4:199.243.119.244
ip4:209.71.208.0/24 ip4:209.71.212.0/24 ~all"

Received-SPF: Pass (mailgate-3.zdv.net: domain of postmaster@cmx-torrigo001.bell.net designates 209.71.212.29 as permitted sender) identity=helo; client-ip=209.71.212.29;

receiver=mailgate-3.zdv.net;
envelope-from="goedemondt@sympatico.ca";
x-sender="postmaster@cmx-torrigo001.bell.net";
x-conformance=spf_only; x-record-type="v=spf1";
x-record-text="v=spf1 ip4:206.47.72.0/24 ip4:184.150.200.0/24
ip4:199.243.119.244 ip4:209.71.208.0/24 ip4:209.71.212.0/24

Praxistip – Mailheader I

Doppelklick auf eine Mail in der Übersicht:

FaxService-Reis		Aktueller Ordner
		Nach Datum
Älter		
Fax Service	Neues Fax von: "+494185795296" <+494185795296> Anbei erhalten Sie ein neues Fax von: "+494185795296"	25.04.2022
Fax Service	Neues Fax von: "+496232654169" <+496232654169> Anbei erhalten Sie ein neues Fax von: "+496232654169"	25.04.2022
Fax Service	Ausgehende Faxergebnisse Sent to 0080027267329	13.04.2022

Klick auf Datei



File Explorer interface showing an email header and a PDF attachment.

Mo 25.04.2022 13:42

FS Fax Service <fax@mail.r>
Neues Fax von: "+494185795296"

An 725-RZ

Wir haben zusätzliche Zeilenumbrüche aus dieser Nachricht entfernt.

PDF 1650886749.273108.pdf
188 KB

Anbei erhalten Sie ein neues Fax von: "+494185795296"
An: reis.uni-speyer.de
über: +496232654485
Für: Fax RZ

Praxistip – Mailheader II

Klick auf Eigenschaften

←

Informationen

Speichern

Speichern unter

Anlagen speichern

Drucken

Schließen

Office-Konto

Feedback

Optionen

In Ordner verschieben

Nachrichtenzustellbericht öffnen

Erneut senden oder zurückrufen

Eigenschaften

Neues Fax von: "+49...

Element in einen anderen Ordner verschieben
Dieses Element in einen anderen Ordner verschieben.
■ Aktueller Ordner: FaxService-

Nachrichtenzustellbericht öffnen
Prüfen Sie den Zustellbericht für die Zustellungszeitpunkte der Nachricht, falls Regeln angewendet wurden.

Erneut senden oder zurückrufen
Diese E-Mail-Nachricht erneut senden oder zurückrufen.

Eigenschaften
Erweiterte Optionen und Eigenschaften anzeigen.
■ Größe: 213 KB

Praxistip – Mailheader III

The image shows two overlapping Outlook 'Eigenschaften' (Properties) dialog boxes. The left dialog is in the foreground, and the right one is partially obscured. Both dialog boxes have tabs for 'Einstellungen' (Settings) and 'Sicherheit' (Security). The 'Einstellungen' tab is active in both, showing options for 'Wichtigkeit' (Importance) and 'Vertraulichkeit' (Confidentiality), both set to 'Normal'. There are also checkboxes for 'Nachrichteninhalte und Anlagen verschlüsseln', 'Dig. Signatur ausgehenden Nachrichten', and 'S/MIME-Bestätigung anfordern'. Under 'Optionen zur Verlaufkontrolle' (Tracking options), there are checkboxes for 'Die Zustellung dieser Nachricht bestätigen' and 'Das Lesen dieser Nachricht bestätigen'. The 'Übermittlungsoptionen' (Delivery options) section shows 'Antworten senden an' (Reply to) set to 'fax@mail.rz.uni-speyer.de' and 'Läuft ab nach' (Deliver after) set to 'Ohne' (None) at '00:00'. There are also buttons for 'Kontakte...' and a 'Kategorien' (Categories) dropdown set to 'Keine'. The 'Internetkopfeilen' (Internet headers) section is visible at the bottom of both dialog boxes. The right dialog box has a context menu open over the header text, with 'Kopieren' (Copy) selected. The header text in the right dialog is: `d044-08da26b08d2f`
`X-MS-Exchange-Organization-AVStamp-Enterprise: 1.0`
`X-Auto-Response-Suppress: DR, OOF, AutoReply`
`X-MS-Exchange-Organization-AuthSource: zdv-e16-1d.ZDV.Net`
`X-MS-Exchange-Organization-AuthAs: Anonymous`
`X-MS-Exchange-Transport-EndToEndLatency: 00:00:00.4449930`
`X-MS-Exchange-Processed-By-BccFoldering: 15.01.23`

Praxistip – Mailheader IV

Received: from zdv-e16-1b.ZDV.Net (fd42:4323:8cdd:70a:2e60:cff:fec0:a6d1) by zdv-e16-1b.ZDV.Net (fd42:4323:8cdd:70a:2e60:cff:fec0:a6d1) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.2375.24 via Mailbox Transport; Mon, 25 Apr 2022 13:41:35 +0200

Received: from zdv-e16-1d.ZDV.Net (fd42:4323:8cdd:70e:c654:44ff:feea:922a) by zdv-e16-1b.ZDV.Net (fd42:4323:8cdd:70a:2e60:cff:fec0:a6d1) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.2375.24; Mon, 25 Apr 2022 13:41:35 +0200

Received: from mailgate-2.zdv.net (2001:4c80:40:62d::25:2) by zdv-e16-1d.ZDV.Net (fd42:4323:8cdd:70e:c654:44ff:feea:922a) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.2375.24 via Frontend Transport; Mon, 25 Apr 2022 13:41:35 +0200

Authentication-Results: mailgate-2.zdv.net; dkim=none (message not signed) header.i=none; spf=Pass smtp.mailfrom=fax@mail.rz.uni-speyer.de; spf=Pass

Received-SPF: Pass (mailgate-2.zdv.net: domain of fax@mail.rz.uni-speyer.de designates 192.124.238.230 as permitted sender) identity=mailfrom; client-ip=192.124.238.230; receiver=mailgate-2.zdv.net; envelope-from=fax@mail.rz.uni-speyer.de; x-sender=fax@mail.rz.uni-speyer.de; x-conformance=spf_only; x-record-type=v=spf1; x-record-text=v=spf1 mx a ~all

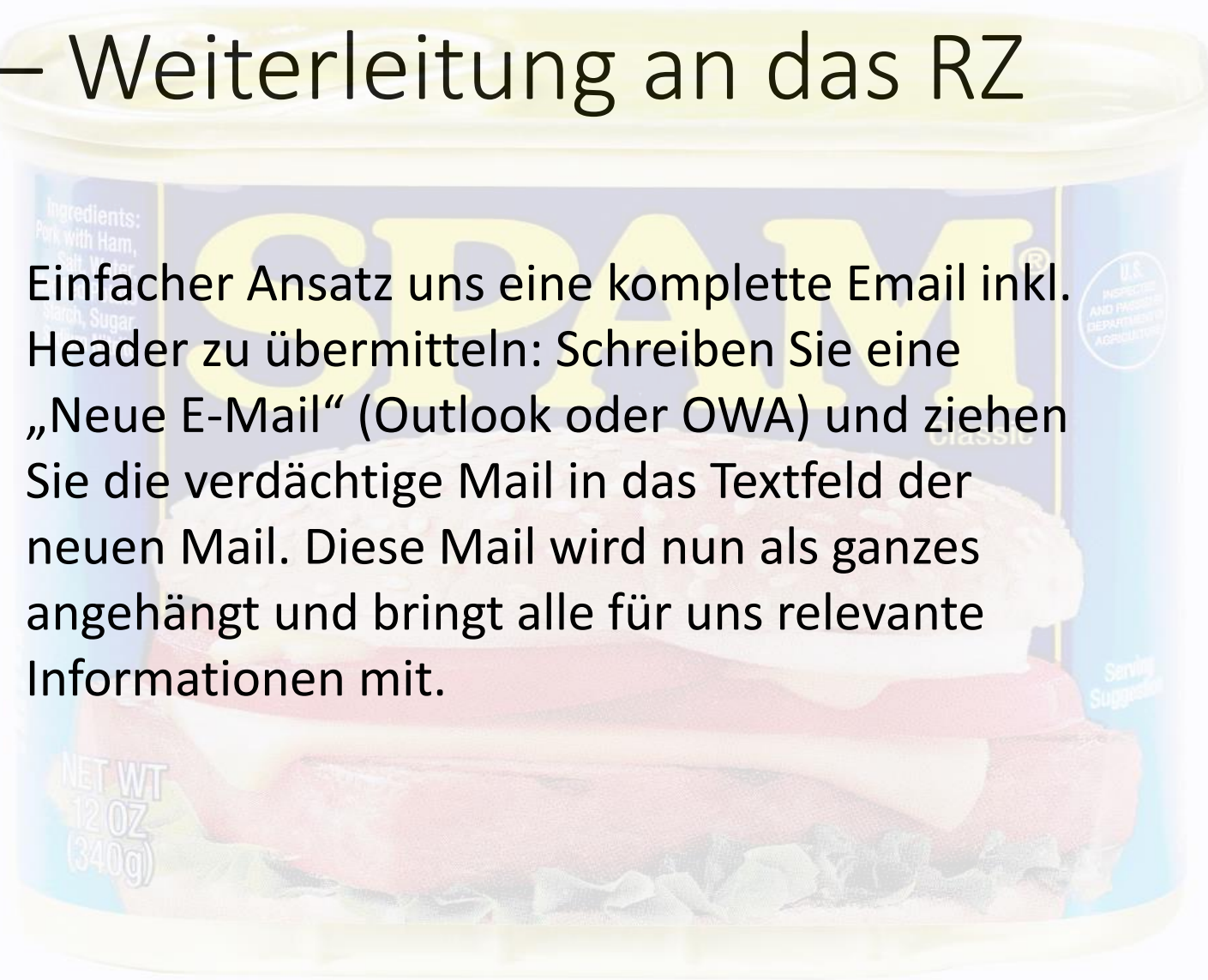
Received-SPF: Pass (mailgate-2.zdv.net: domain of postmaster@mail.rz.uni-speyer.de designates 192.124.238.230 as permitted sender) identity=helo; client-ip=192.124.238.230; receiver=mailgate-2.zdv.net; envelope-from=fax@mail.rz.uni-speyer.de; x-sender=postmaster@mail.rz.uni-speyer.de; x-conformance=spf_only; x-record-type=v=spf1; x-record-text=v=spf1 mx a ~all

X-Ironport-Dmarc-Check-Result: validskip

Der Mailheader enthält Daten zum Versandweg einer Mail und auch häufig zur wahren Herkunft.

Praxistip – Weiterleitung an das RZ

Einfacher Ansatz uns eine komplette Email inkl. Header zu übermitteln: Schreiben Sie eine „Neue E-Mail“ (Outlook oder OWA) und ziehen Sie die verdächtige Mail in das Textfeld der neuen Mail. Diese Mail wird nun als ganzes angehängt und bringt alle für uns relevante Informationen mit.



Vielen Dank für Ihr Interesse!

Sie sind Teil jedes Sicherheitskonzepts, ohne Ihre Mitarbeit kann das Campusnetz nicht sicher sein.

