DEUTSCHE Fernsehlotterie

E-Mail©

Gefahrenerkennung

Gefahrenabwehr

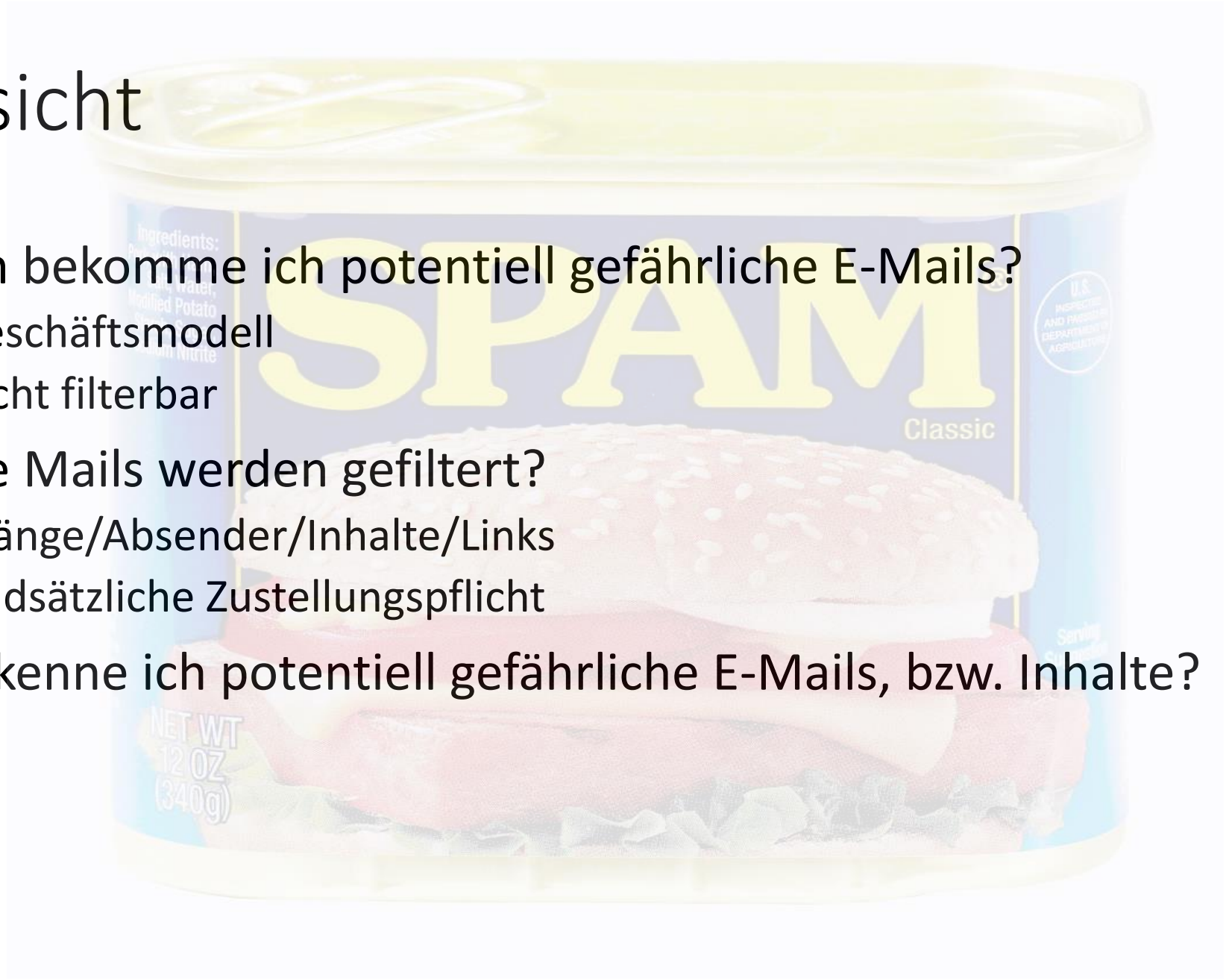
DEUTSCHE FERNSEHLOTTERIE gGmbH • Axel-Springer-Platz 3 • 20355 Hamburg

0344027/224 155974/1111/042

An alle, die Millionen gewinnen und
gleichzeitig Tausenden helfen möchten

67346 Speyer

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 Mail[1]: 0,7g CO_2 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

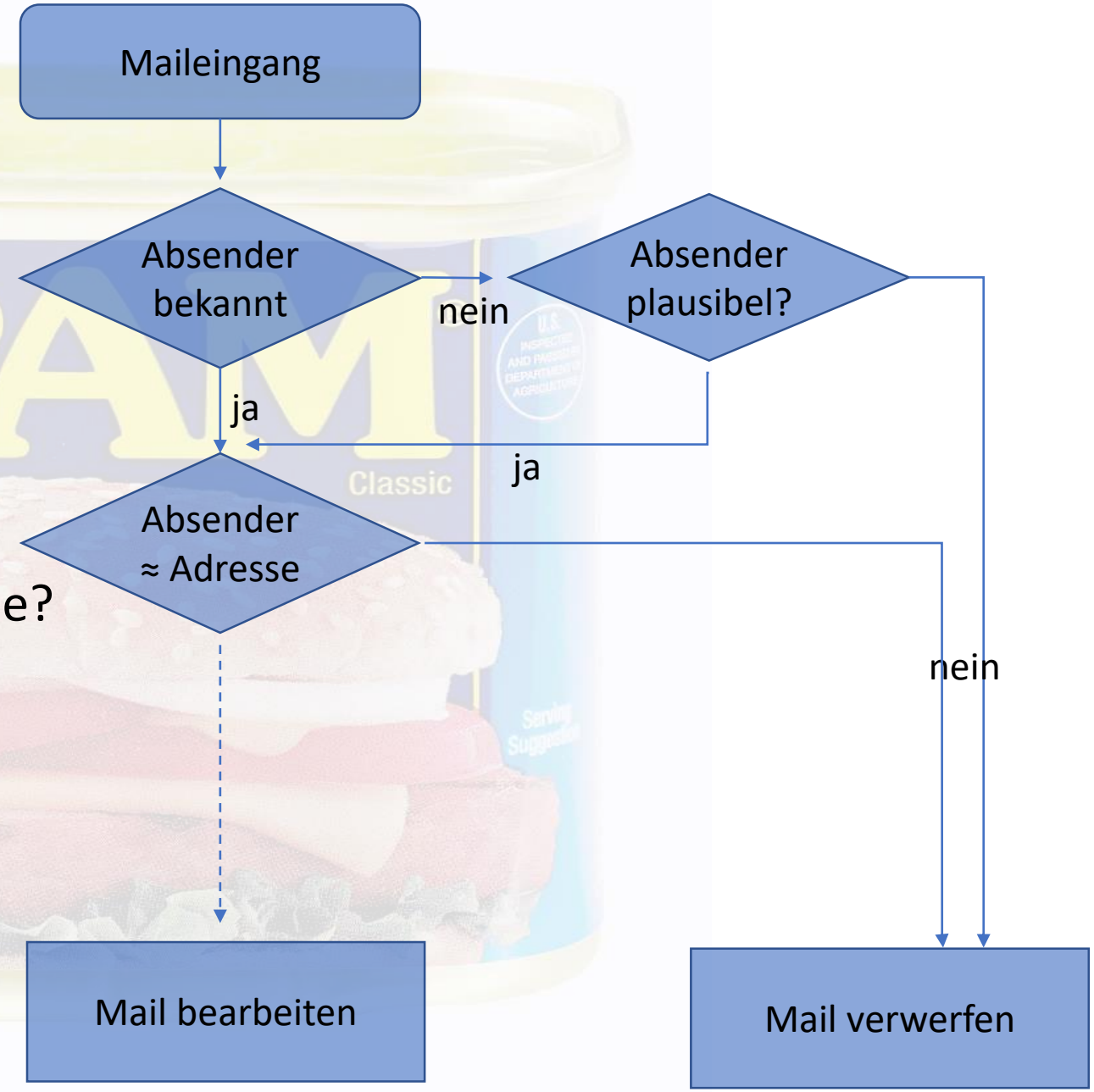
Filterung

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

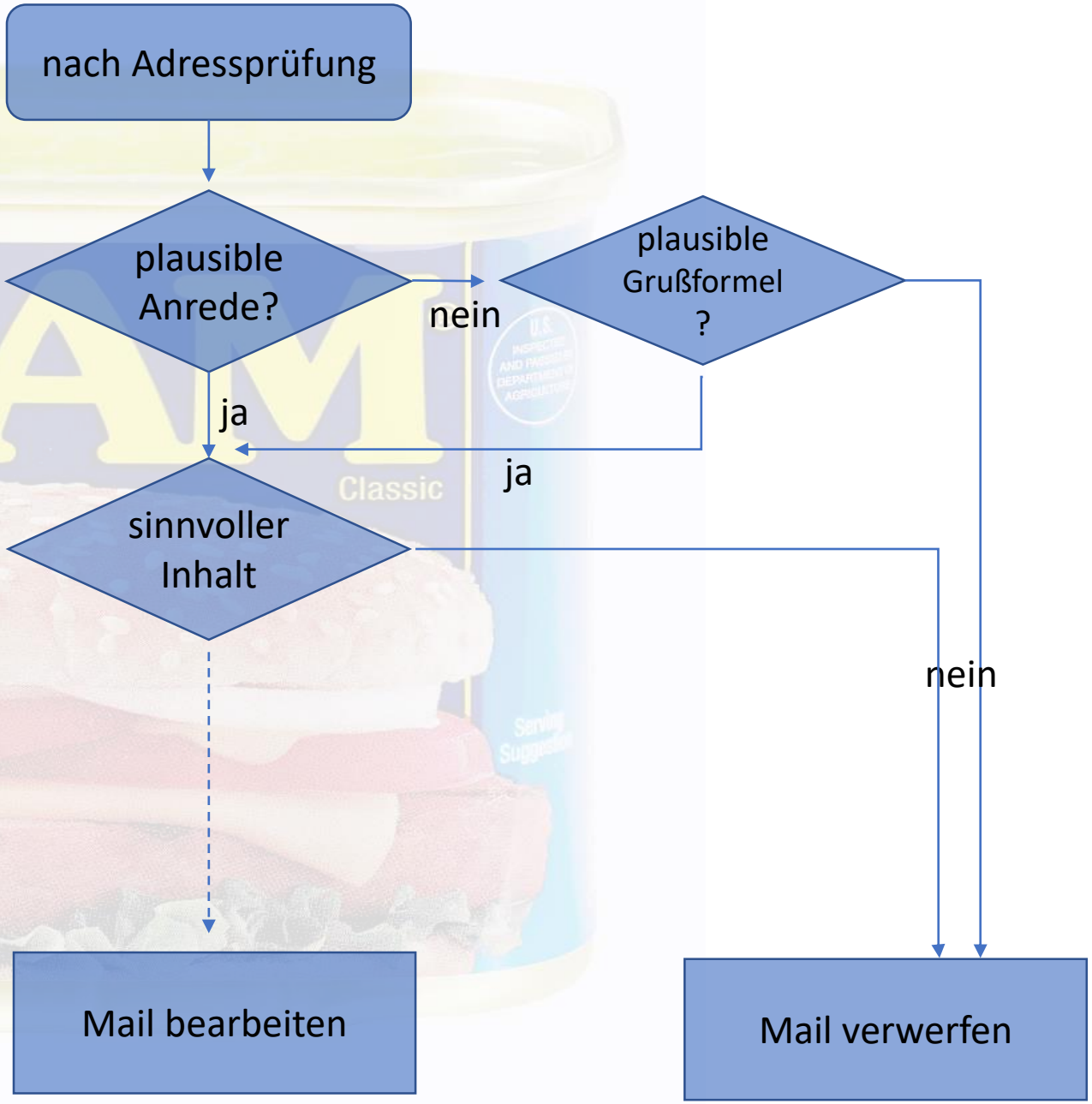
- Absender – Teil 1 (sozial)
  - Kenne ich den Absender?
  - Wenn nein, plausibel?
- Absender – Teil 2 (technisch)
  - Entspricht der Absender der Adresse?
  - Paßt die Adresse zum Versandweg?

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

H

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 >>

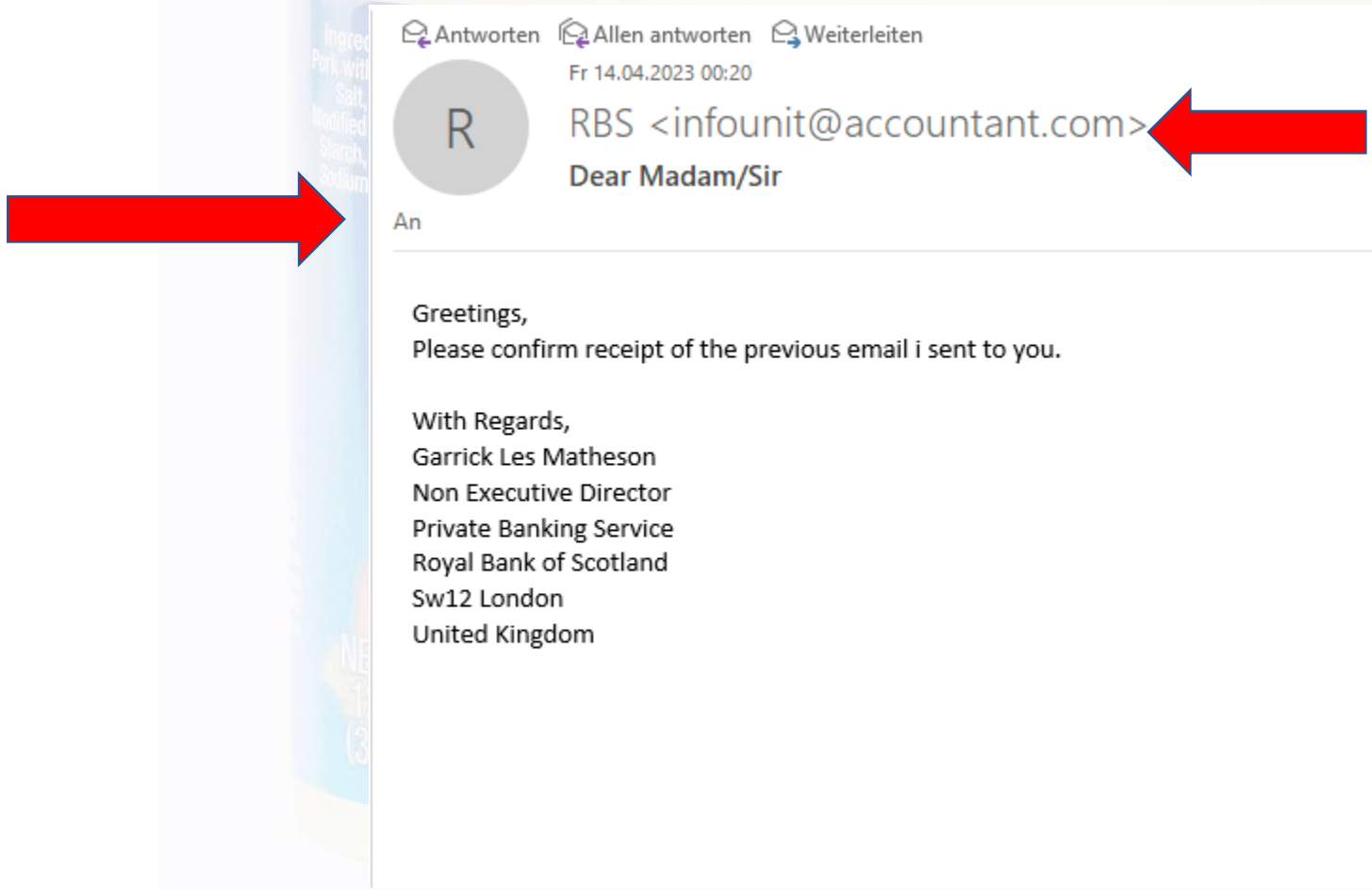
Das einzige nanotechnologische Medikament, da Gelenke auf natürliche Art und Weise wiederherstellt.
Die patentierte Formel hat keine Analoga!

Stellt in 99% der Fälle das Gewebe beschädigter Gelenkte 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!

Beispiele – klassische SPAM-Mail



Antworten Allen antworten Weiterleiten

Fr 14.04.2023 00:20

R

RBS <infounit@accountant.com>

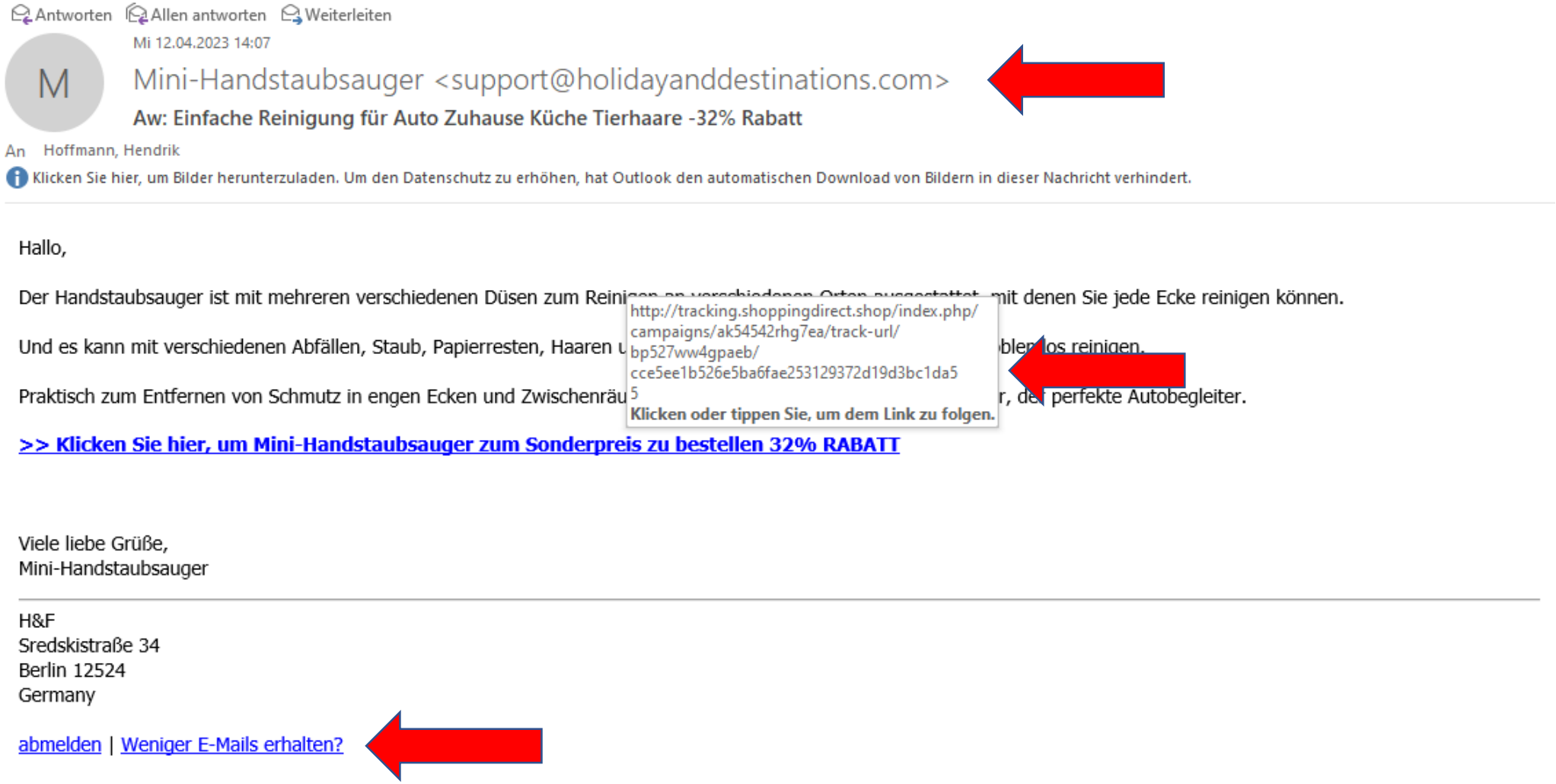
Dear Madam/Sir

An

Greetings,
Please confirm receipt of the previous email i sent to you.

With Regards,
Garrick Les Matheson
Non Executive Director
Private Banking Service
Royal Bank of Scotland
Sw12 London
United Kingdom

Beispiele – klassische SPAM-Mail



Antworten Allen antworten Weiterleiten

Mi 12.04.2023 14:07

M

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 u[illegible]los reinigen.

Praktisch zum Entfernen von Schmutz in engen Ecken und Zwischenräu[illegible]r, der perfekte Autobegleiter.

http://tracking.shoppingdirect.shop/index.php/campaigns/ak54542rhg7ea/track-url/bp527ww4gpaeb/cce5ee1b526e5ba6fae253129372d19d3bc1da55

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

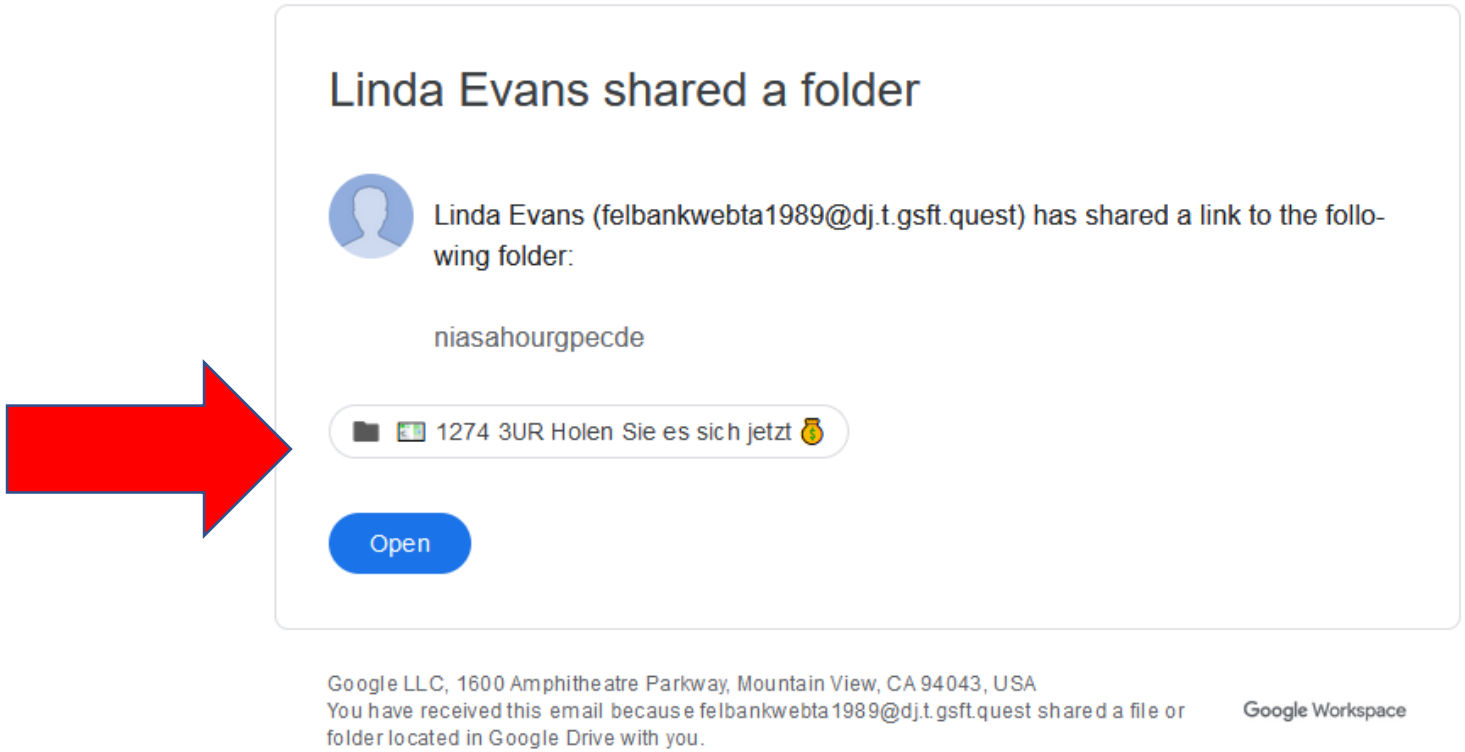
abmelden | Weniger E-Mails erhalten?

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, hedkezipzip@googlemail.com, amire_isuf@hotmail.com, weissenbacher.martina@hotmail.com

Antworten Allen antworten Weiterleiten Löschen



Beispiele – Phishing

Bitte überprüfen Sie Ihre Daten [6.4.2023]

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

6.4.2023 14:14

Antworten Allen antworten Weiterleiten Löschen

DKB

Hallo [redacted]@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.

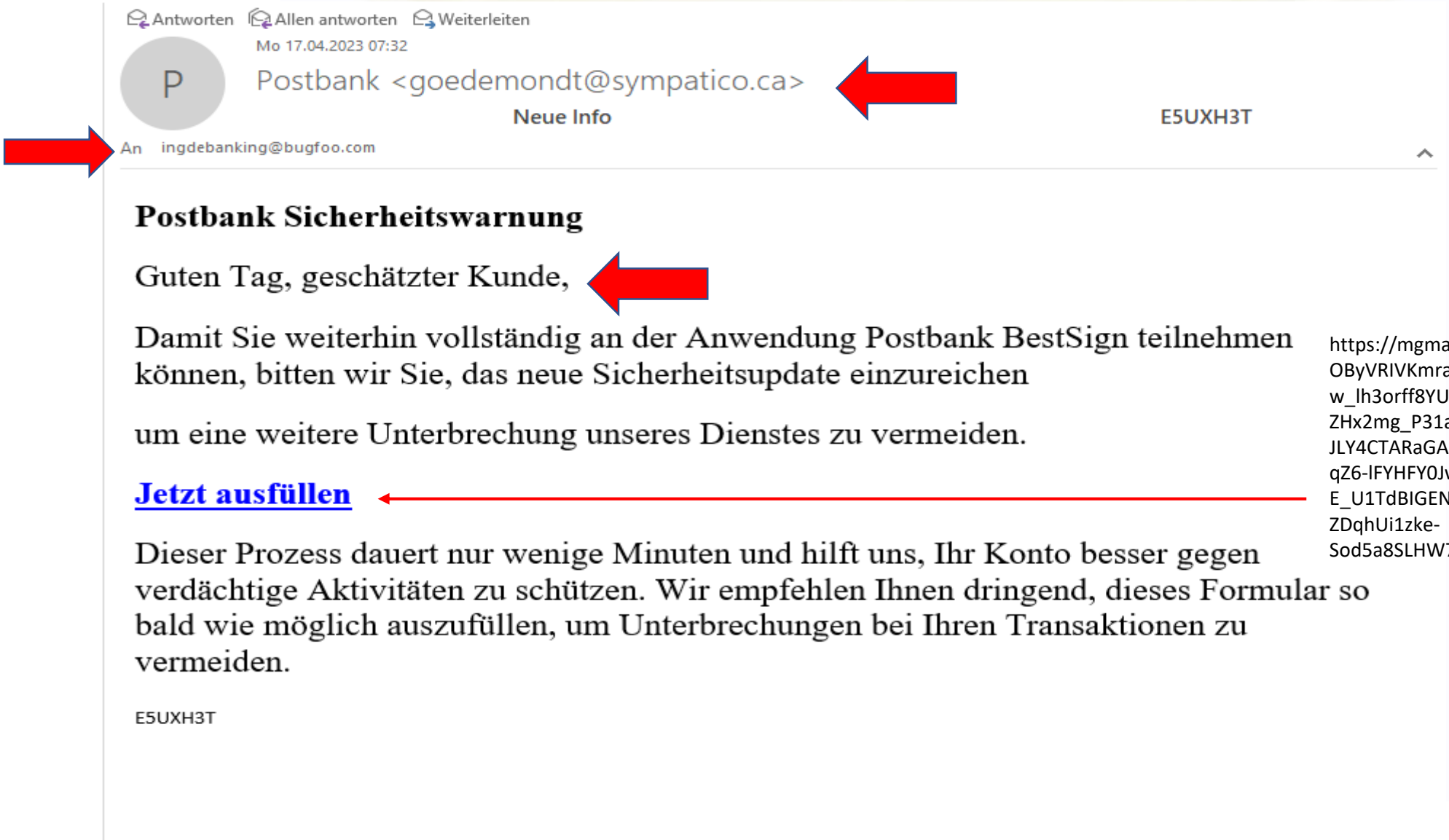
Kunden-ePortal

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

P

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/eJxczr1uhyAUQPGnk
OByVRIVKmrat28cunQ-
w_lh3orff8YUHddcW25YdHoAlAMjx8Fy01vQltHm0-re1
ZHx2mg_P31a6ejSfueENG5Uq5-
JLY4CTARaGA4BJgETYsRgxcCjhElJlhwoiREMHwzGfuRCC
qZ6-lFYHFY0Jw2RatSzBdo-
E_U1TdBIGENpo9g_yNKMV9NIqtrrlPEtt5FsjXo14bZT2N
ZDqhUi1zke-
Sod5a8SLHW72c8pf9zctd2xUH655yvnJ7Kp0PCsLvRBS2

Beispiele – Phishing (Header)

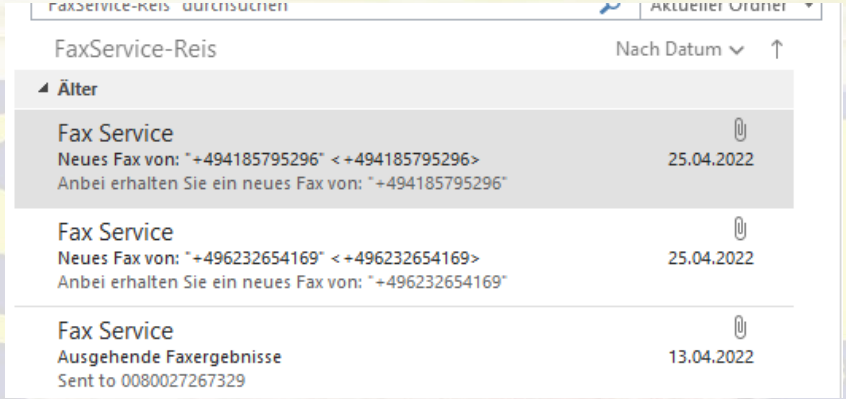
Authentication-Results: mailgate-3.zdv.net; dkim=none (message not signed) header.i=none; spf=Pass smtp.mailfrom=goedemondt@sympatico.ca; spf=Pass smtp.helo=postmaster@cmx-torrgo001.bell.net

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"

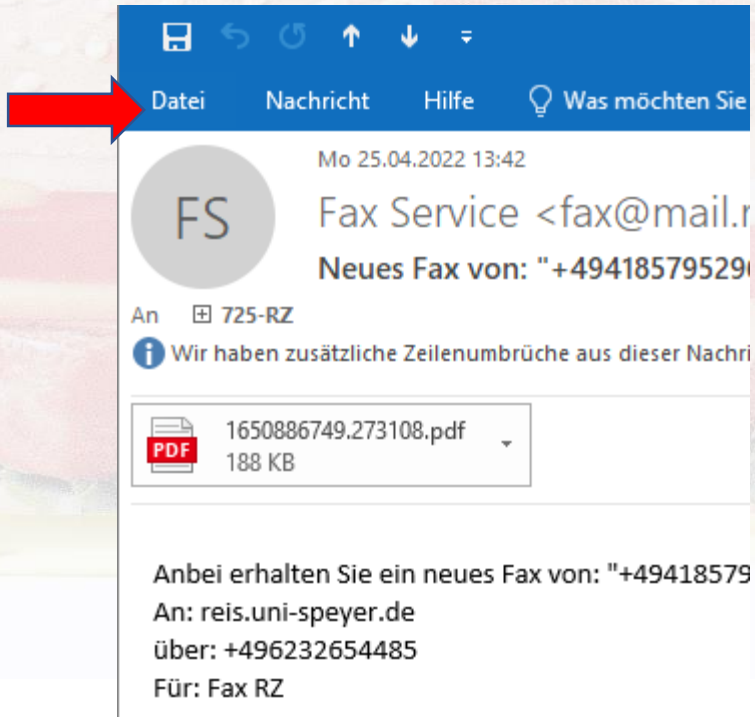
Received-SPF: Pass (mailgate-3.zdv.net: domain of postmaster@cmx-torrgo001.bell.net designates 209.71.212.29 as permitted sender) identity=helo; client-ip=209.71.212.29; receiver=mailgate-3.zdv.net; envelope-from="goedemondt@sympatico.ca"; x-sender="postmaster@cmx-torrgo001.bell.net"; x-conformance=spf_only; 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

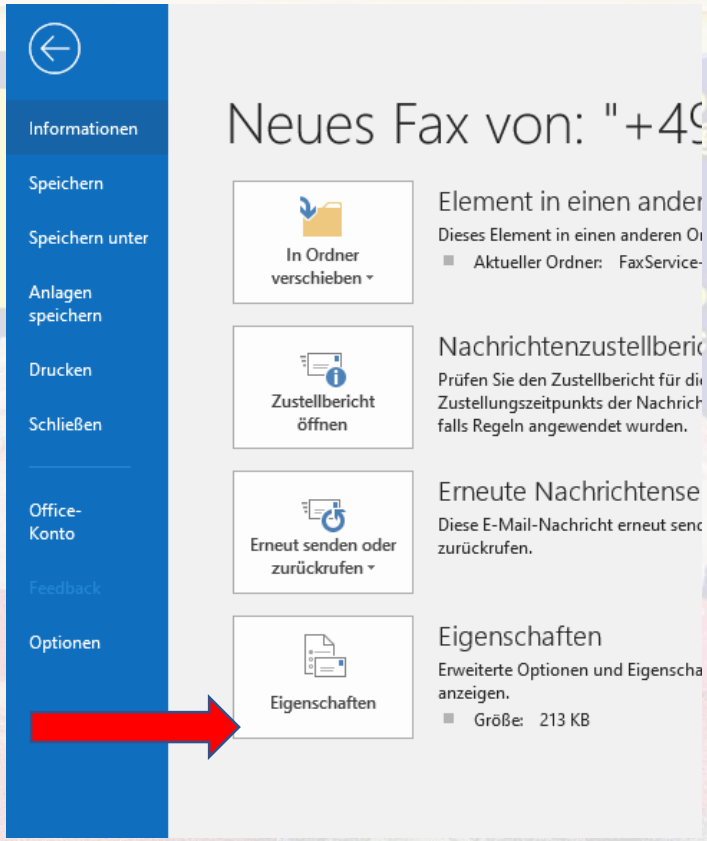
Doppelklick auf eine Mail in der Übersicht:



Klick auf Datei

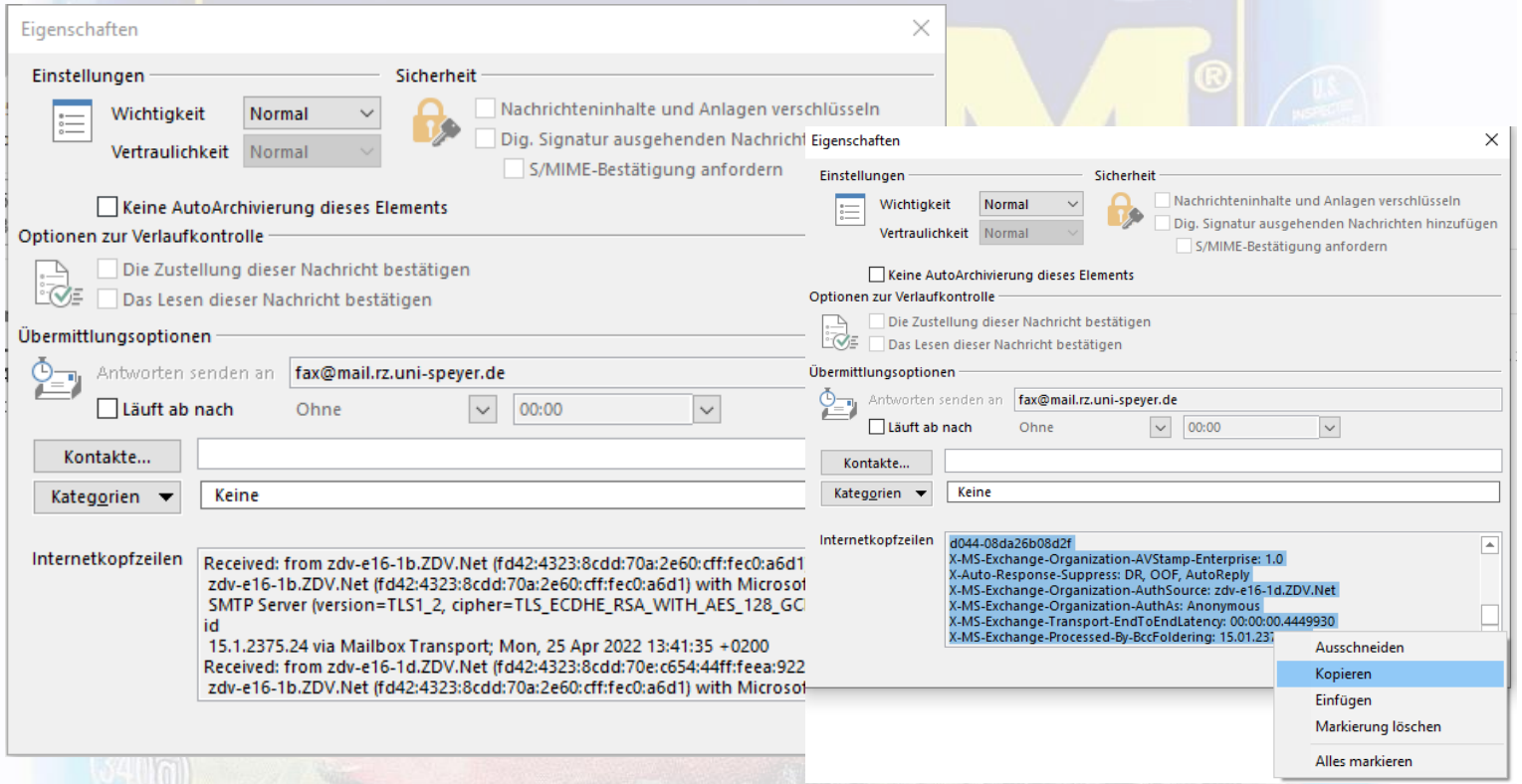


Praxistip – Mailheader II



Klick auf Eigenschaften

Praxistip – Mailheader III

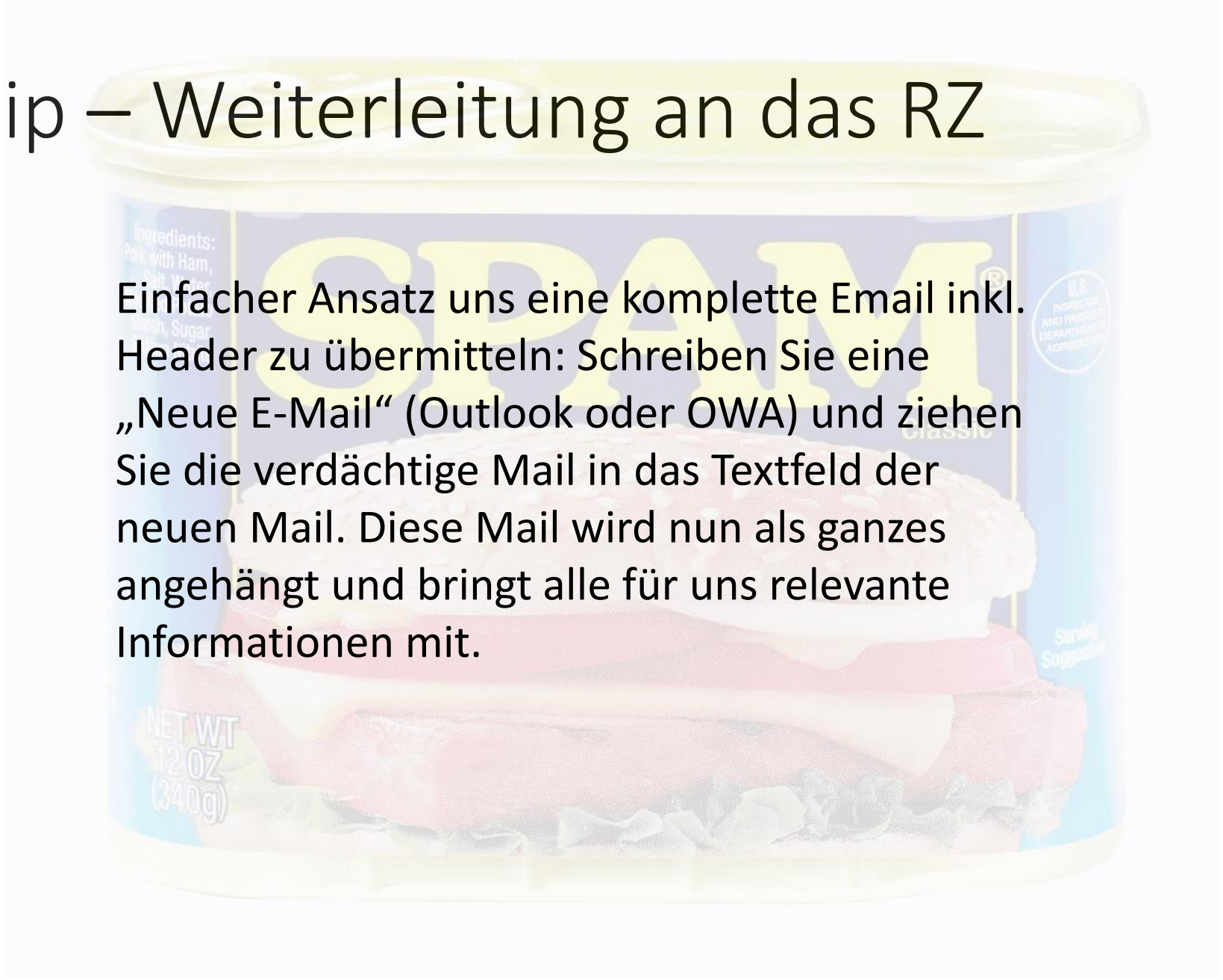


Praxistip – Mailheader IV

```
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.