SECUSO
SECURITY · USABILITY · SOCIETY

Wie Sie sich gegen **Phishing und andere gefährliche Nachrichten** schützen können

01. November 2017
Sicherheitsforum "Online-Banking"

Dr. Marco Ghiglieri
Benjamin Reinheimer

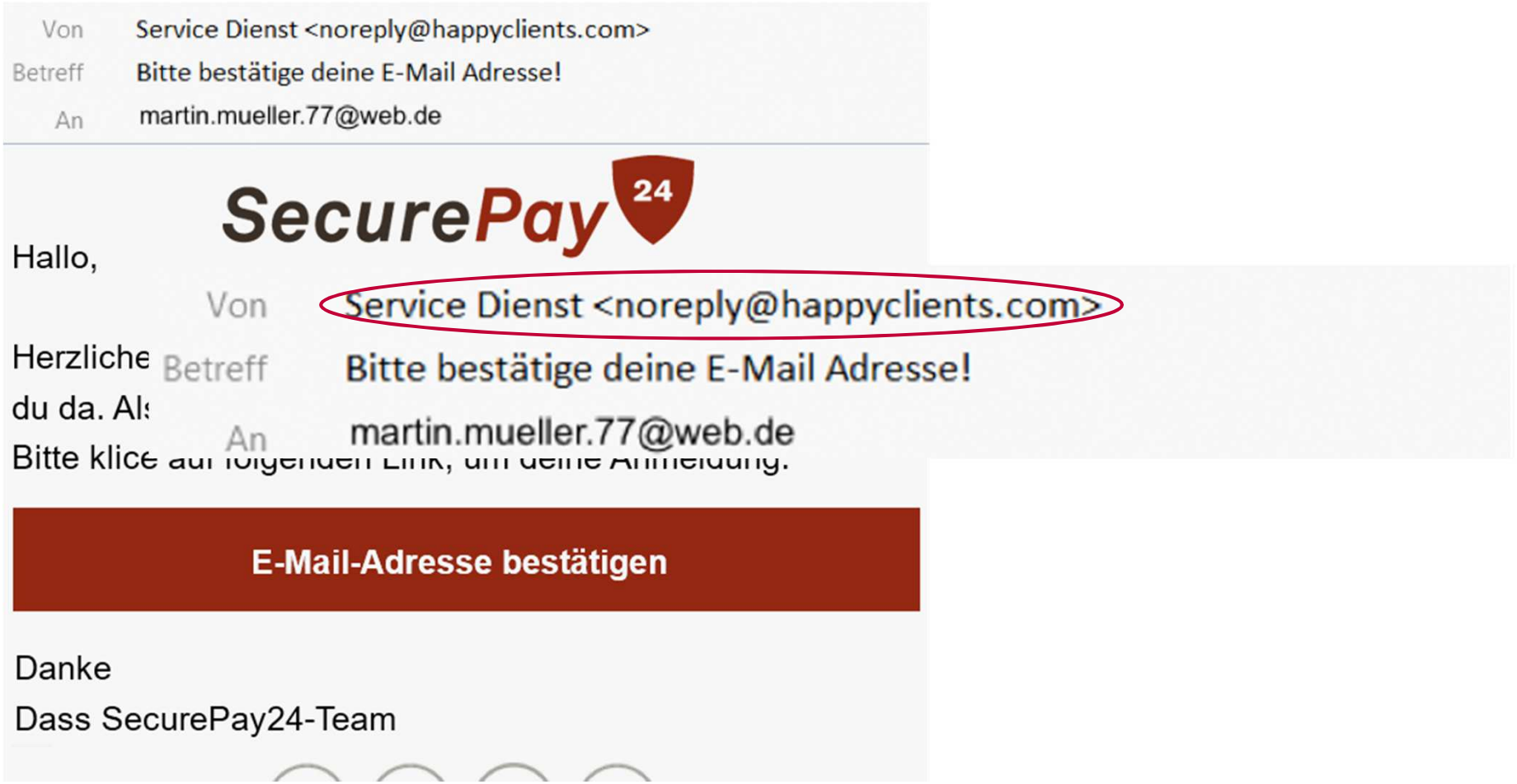
TECHNISCHE UNIVERSITÄT DARMSTADT
CYSEC

KMU AWARE

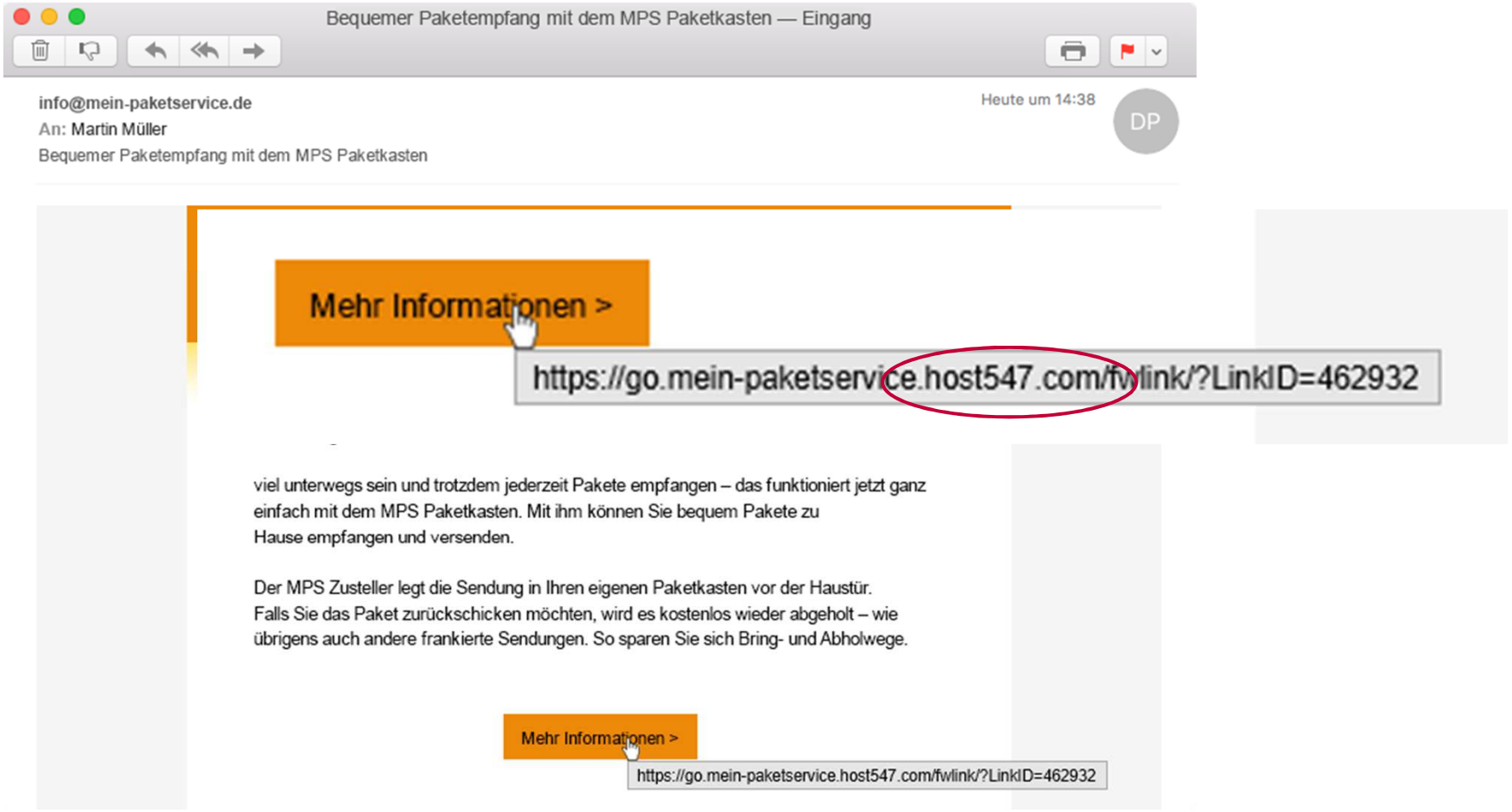
IT-Sicherheit IN DER WIRTSCHAFT

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

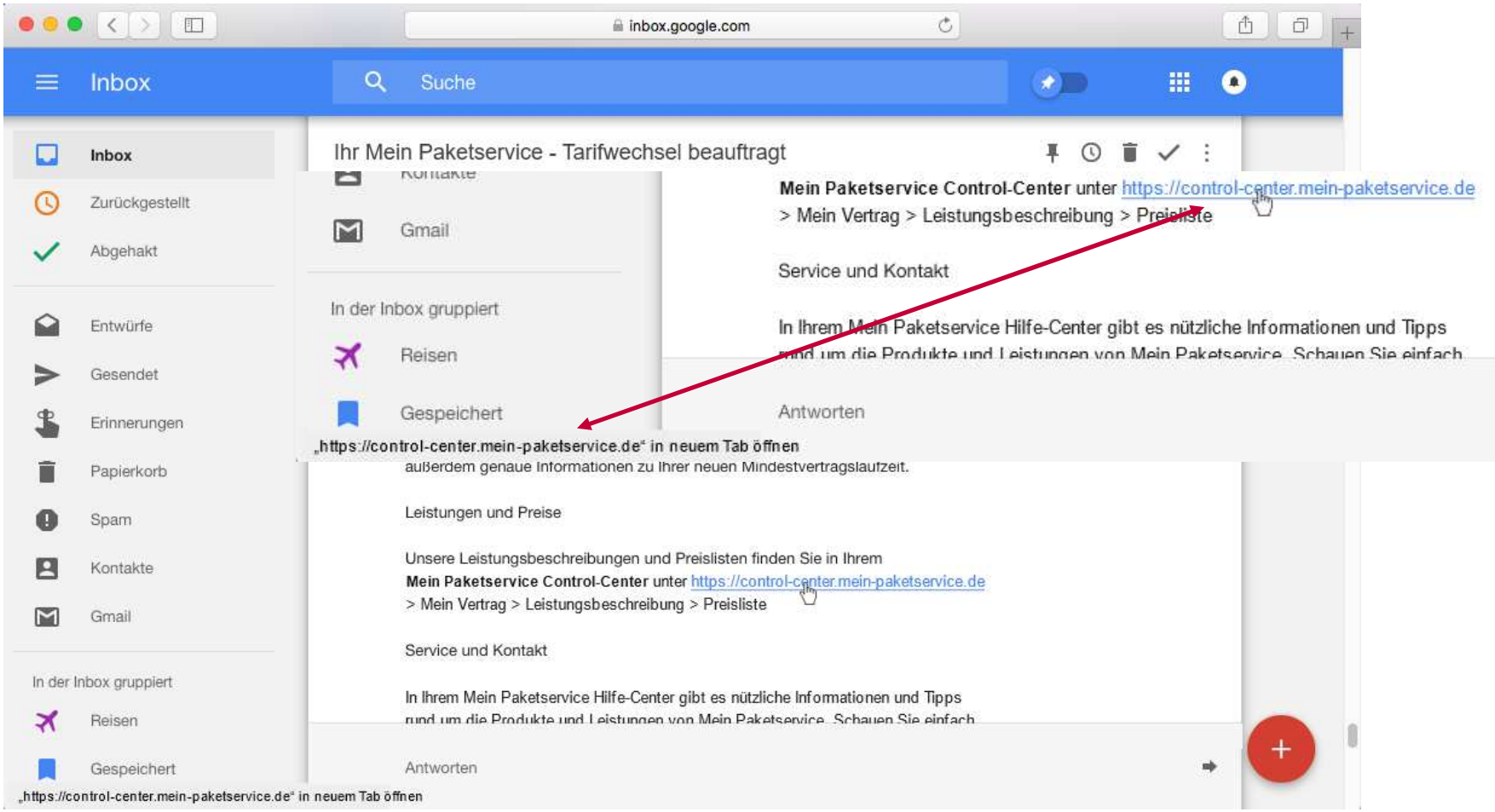
Vertrauen Sie dieser E-Mail?



Vertrauen Sie dieser E-Mail?



Vertrauen Sie dieser E-Mail?



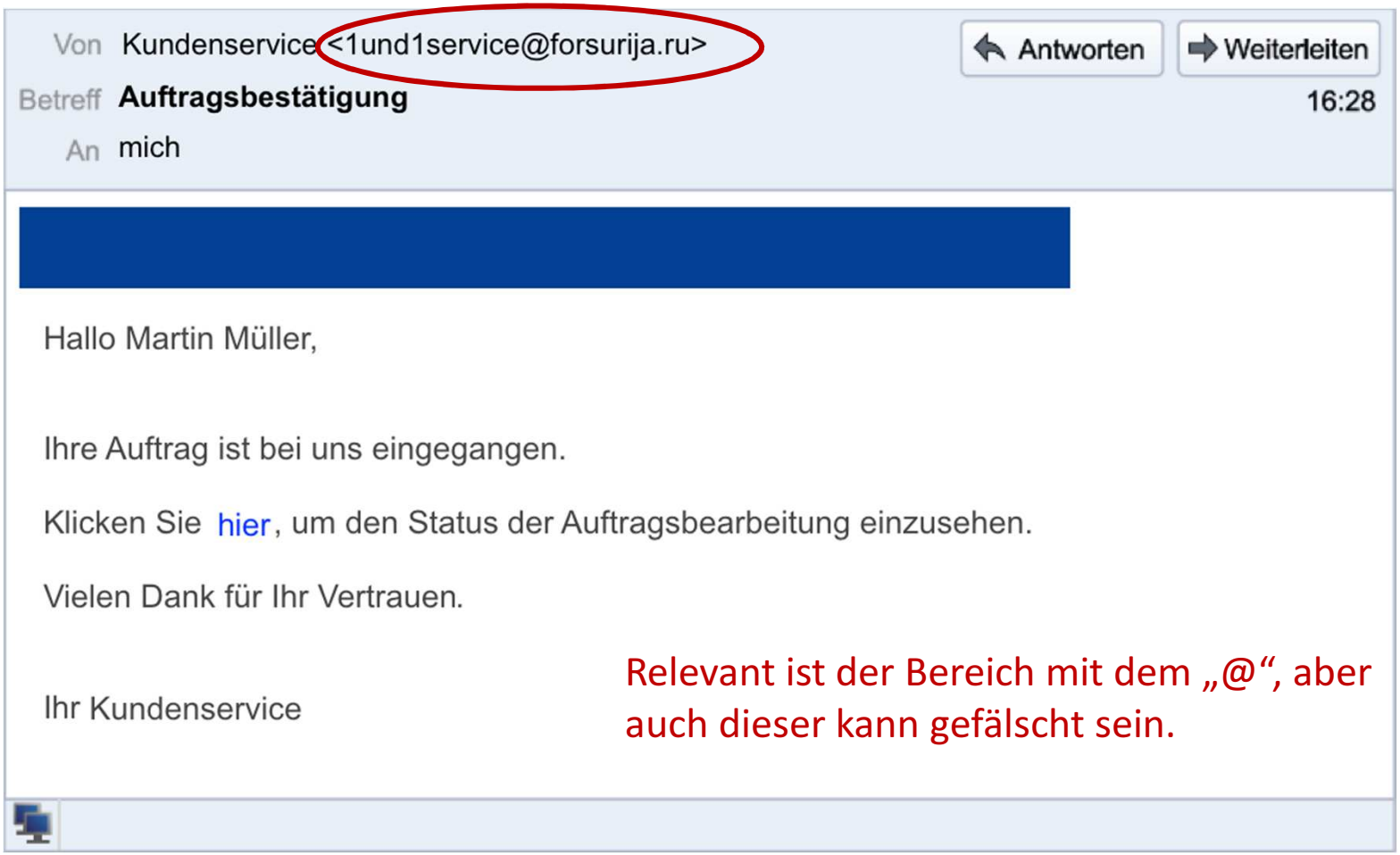
Wie erkennen Sie gefährliche Nachrichten?

Ist die Nachricht plausibel?

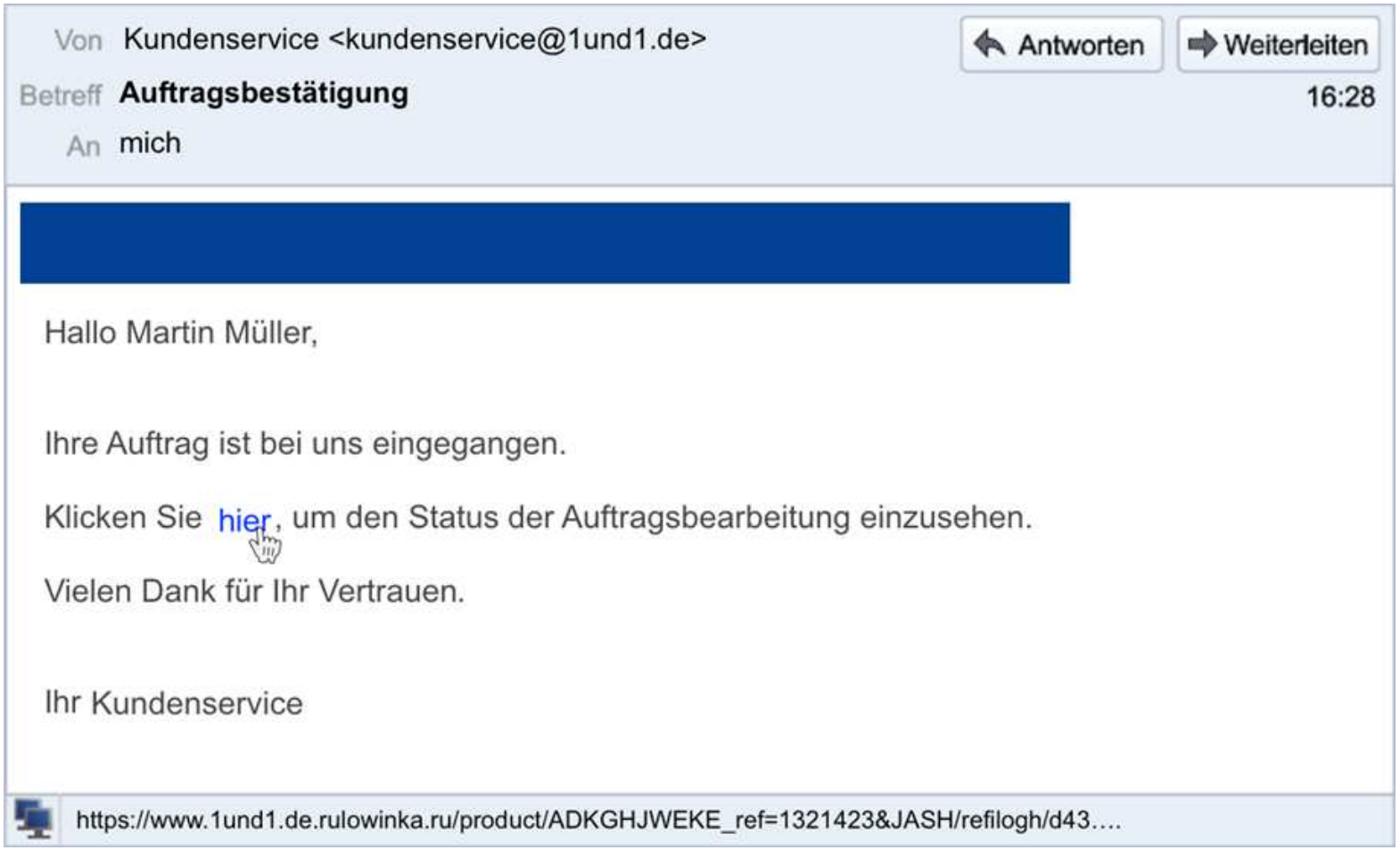
Wie?

- Absender passt zum Inhalt der Nachricht?
- Inhalt der Nachricht plausibel?

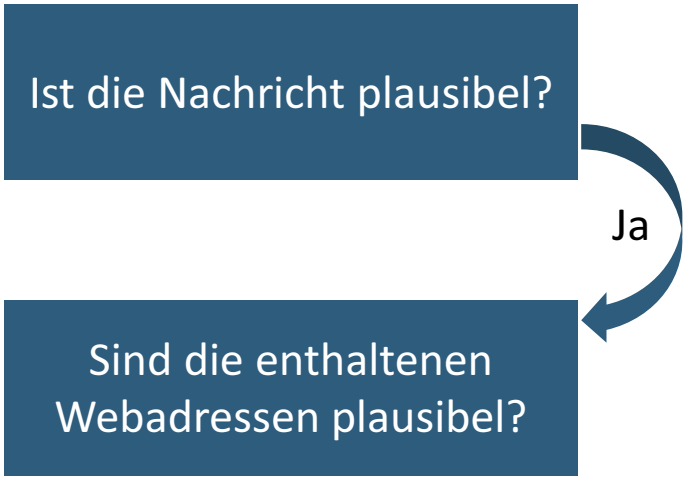
Vertrauen Sie dieser E-Mail?



Vertrauen Sie dieser E-Mail?



Wie erkennen Sie gefährliche Nachrichten?

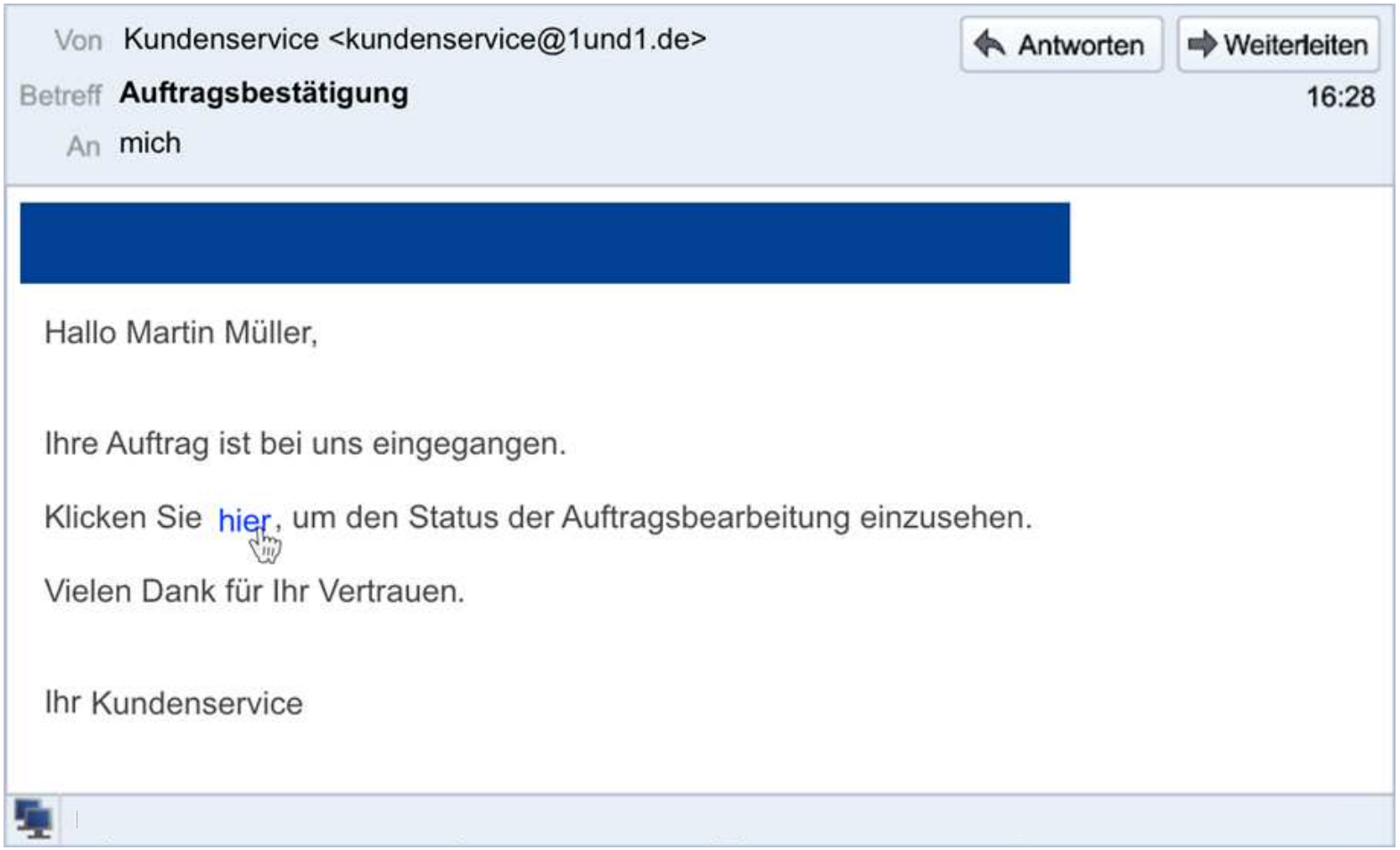


Wie?

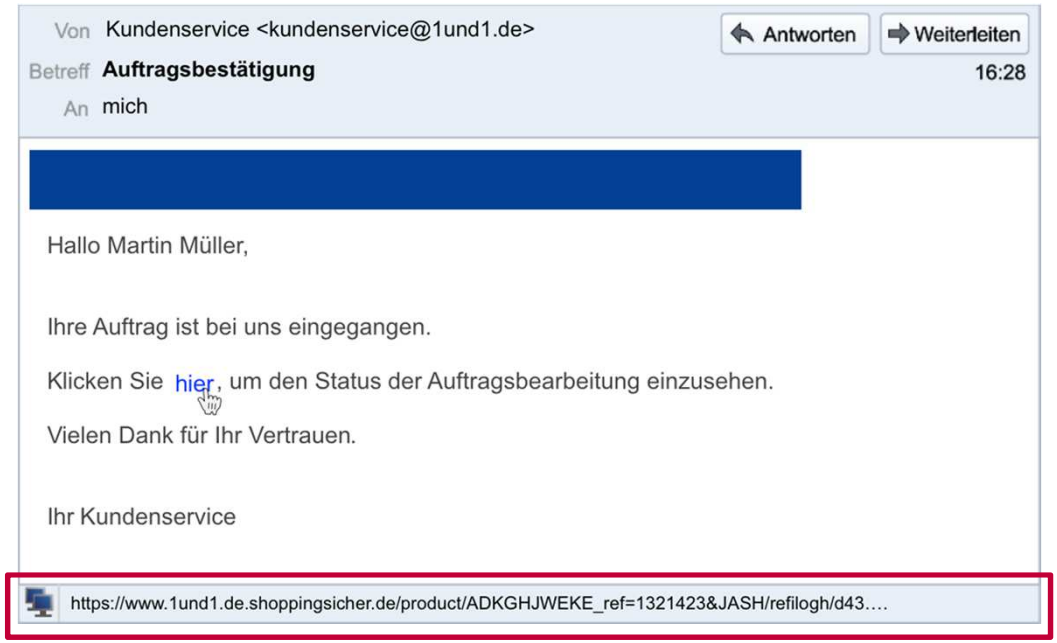
- Absender passt zum Inhalt der Nachricht?
- Inhalt der Nachricht plausibel?

- Richtige Webadresse identifizieren
- Identifizieren Sie den „Wer-Bereich“
- Hat der „Wer-Bereich“ Bezug zum Absender und Nachricht ?

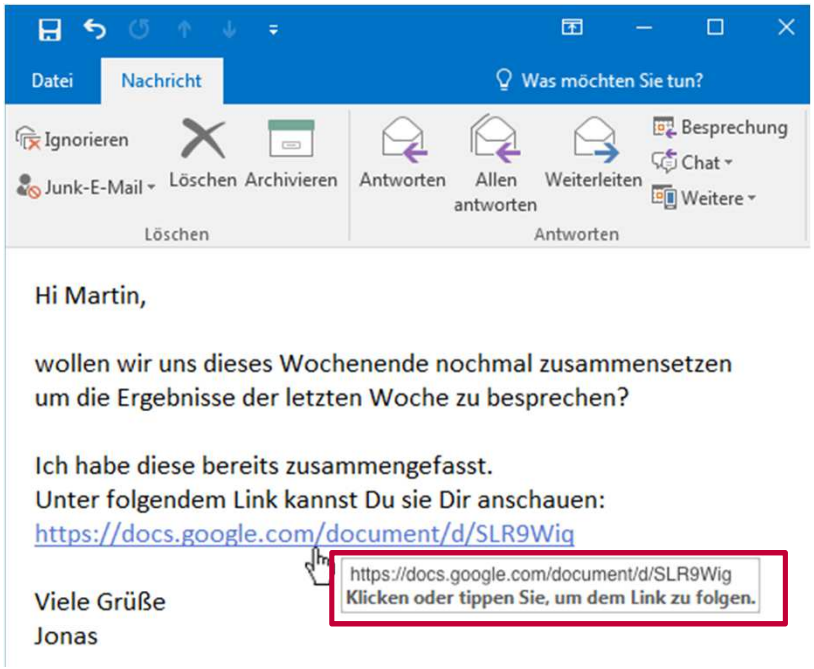
Vertrauen Sie dieser E-Mail?



Welche Webadresse steckt hinter dem Link?

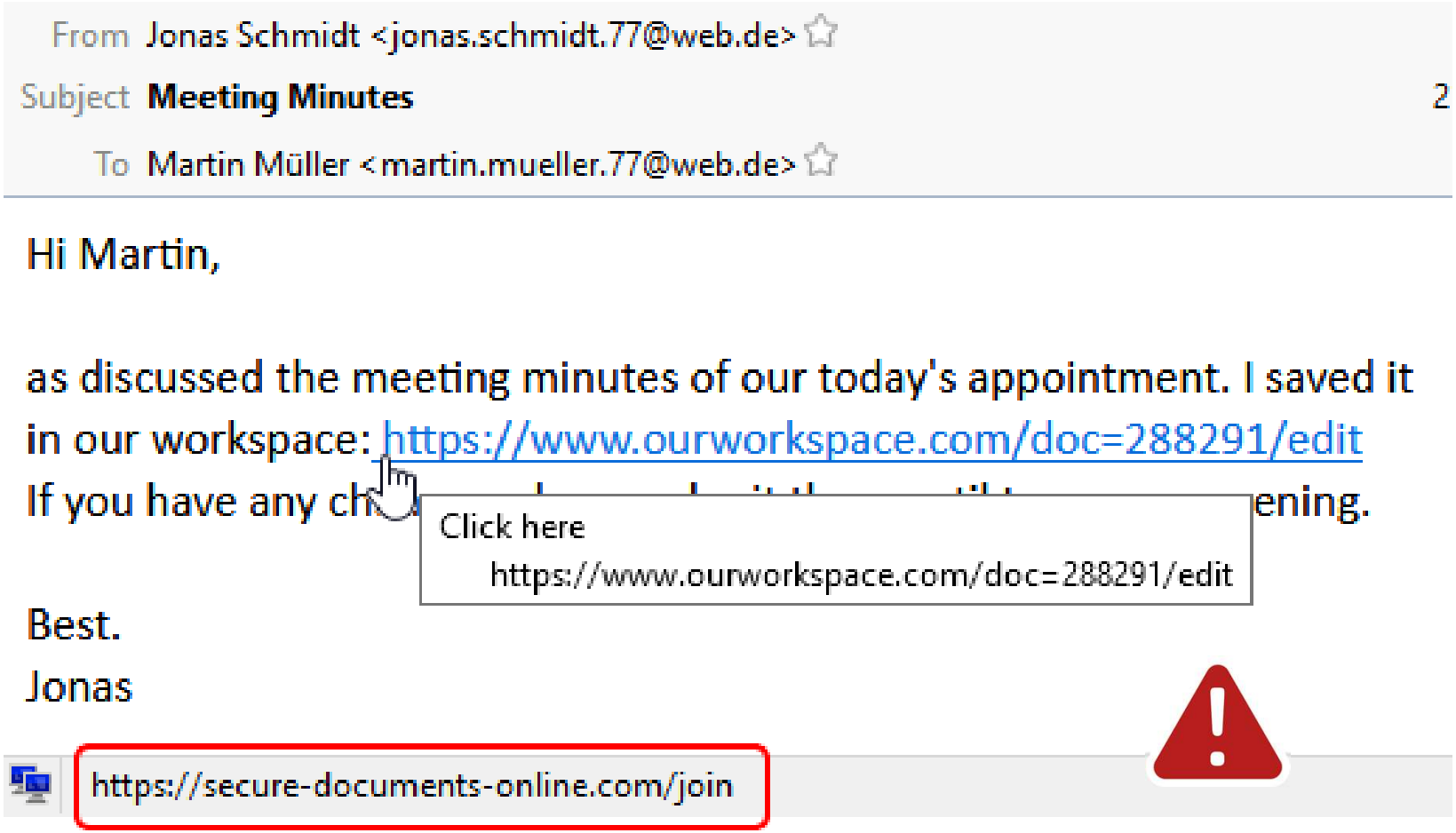


Statusleiste
(z.B. Thunderbird)

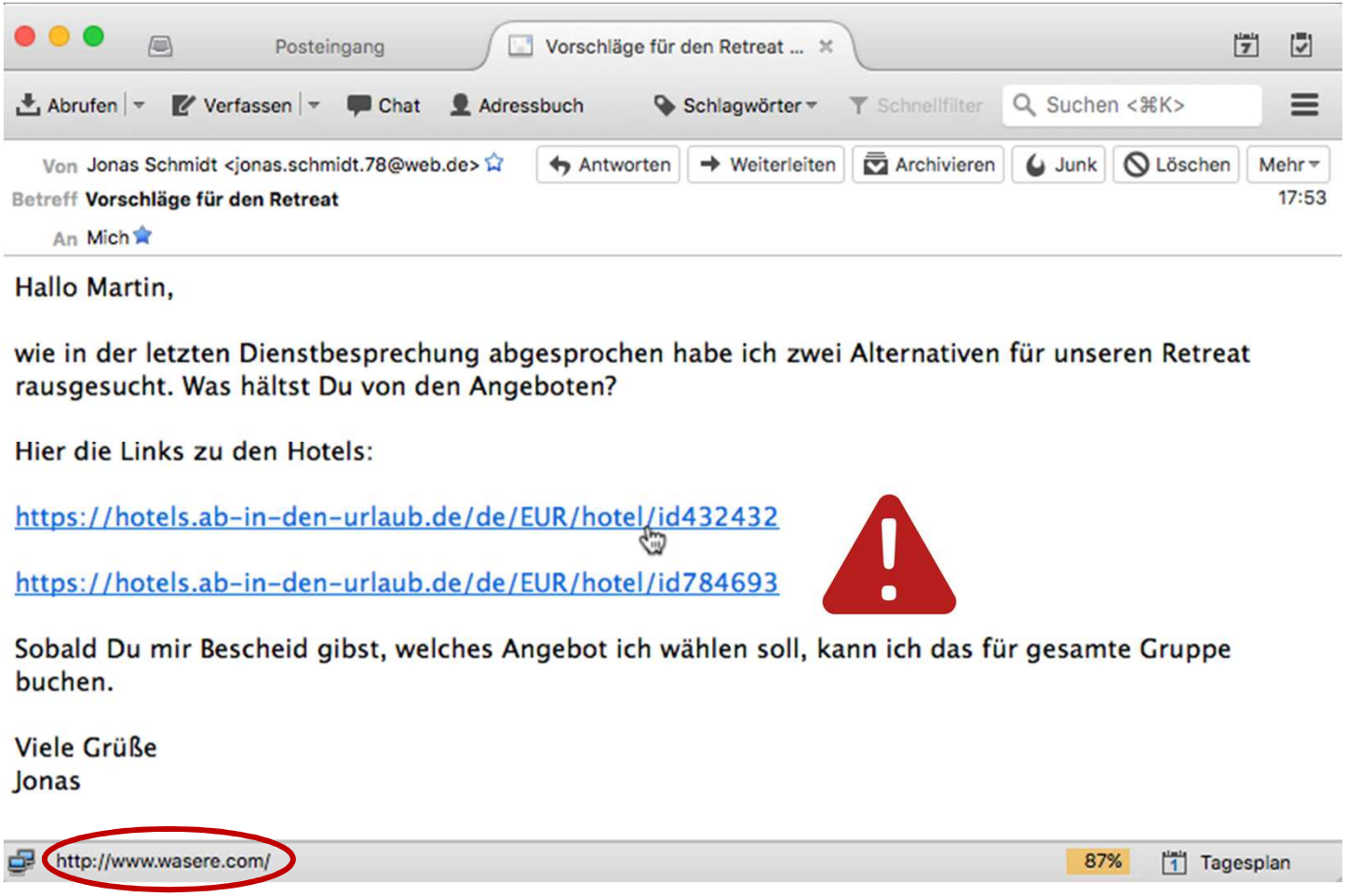


Tooltip
(z.B. Outlook)

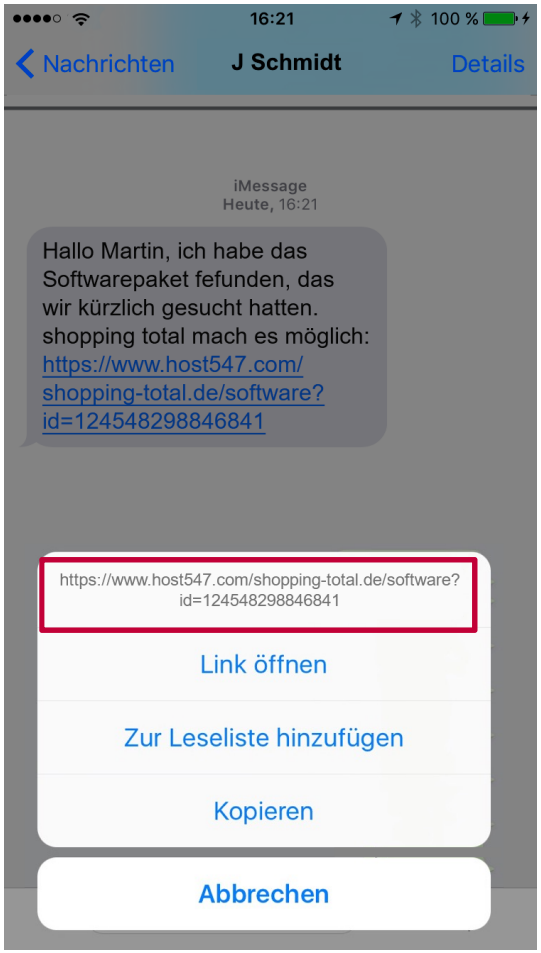
Vorsicht Falle: Falscher Tooltip



Vorsicht Falle: Webadresse bereits in Nachricht sichtbar

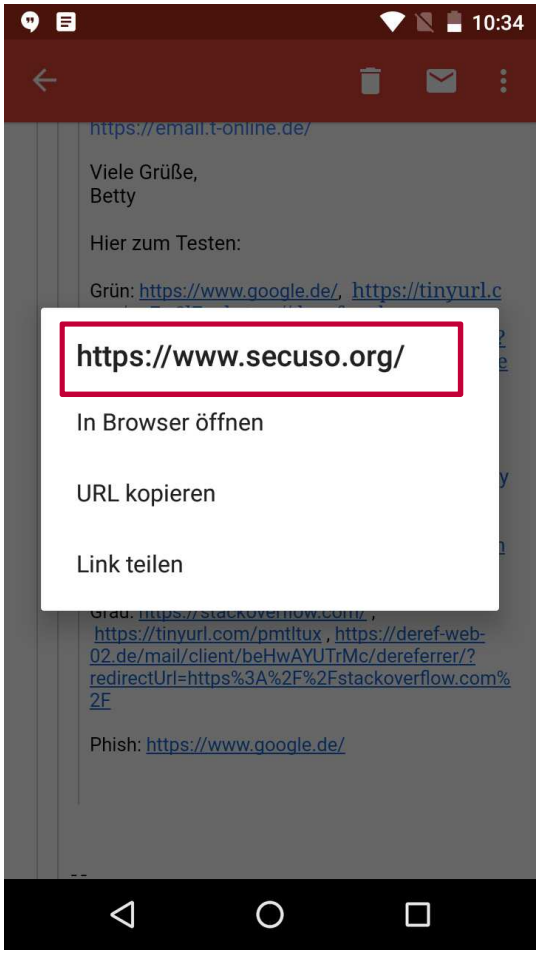


Welche Webadresse steckt hinter dem Link?

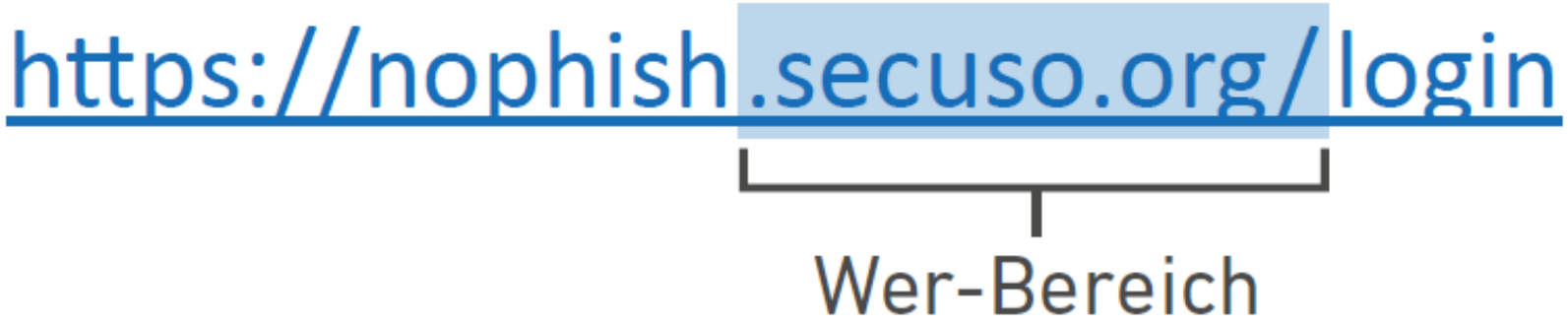


Mobile Geräte?

Mit Finger gedrückt **halten** und auf
Einblendung
warten
(z.B. iOS oder Android)



Welcher Teil der Webadresse ist für die Erkennung von gefährlichen Links wichtig?



Wer-Bereich = Zahlen → sogenannte IP Adresse → wahrscheinlich gefährlicher Link
z.B. http://192.168.11.22/login-secure

Welcher Teil der Webadresse ist für die Erkennung von gefährlichen Links wichtig?

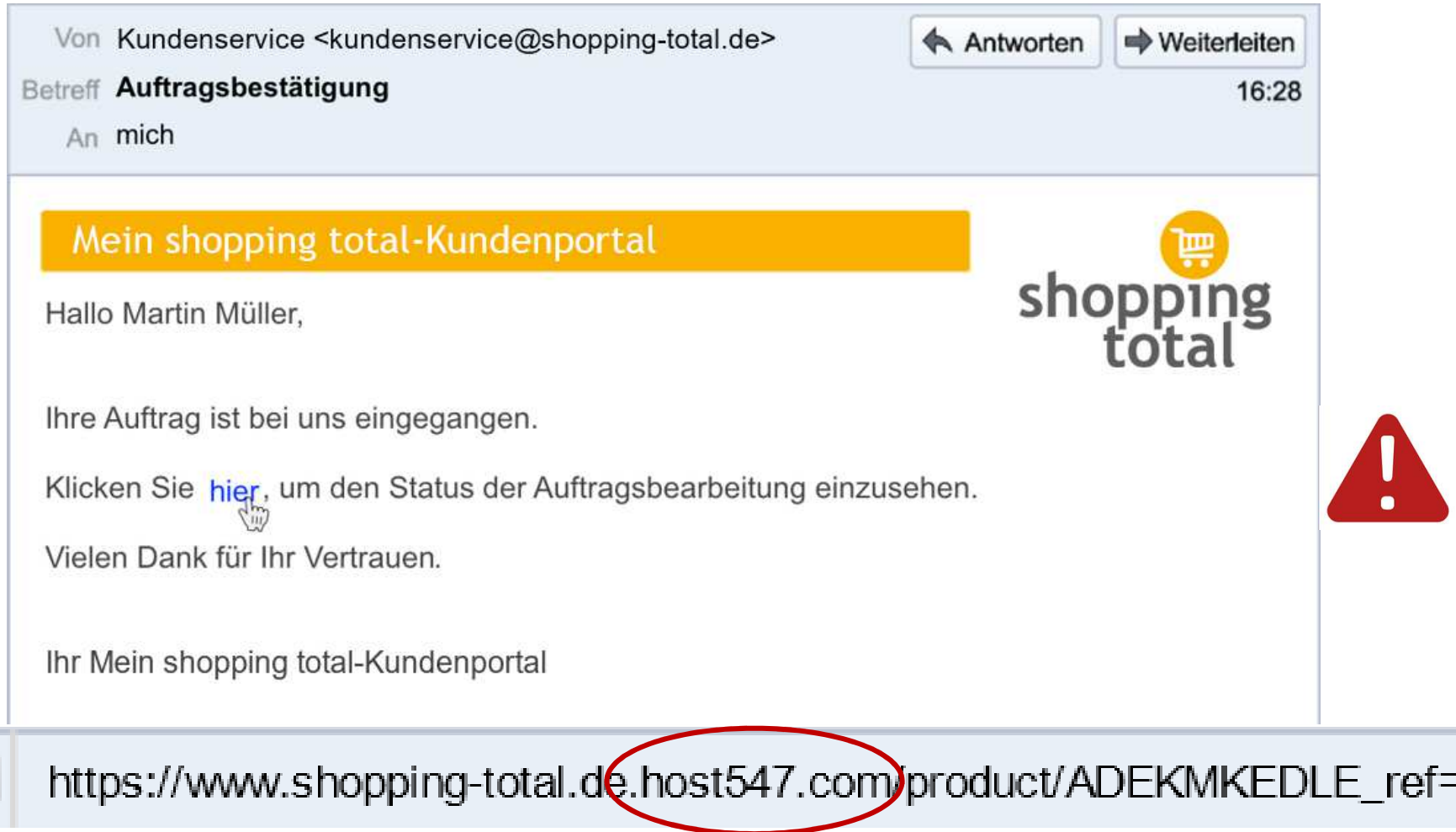
https://www.securepay24.de/login

Wer-Bereich

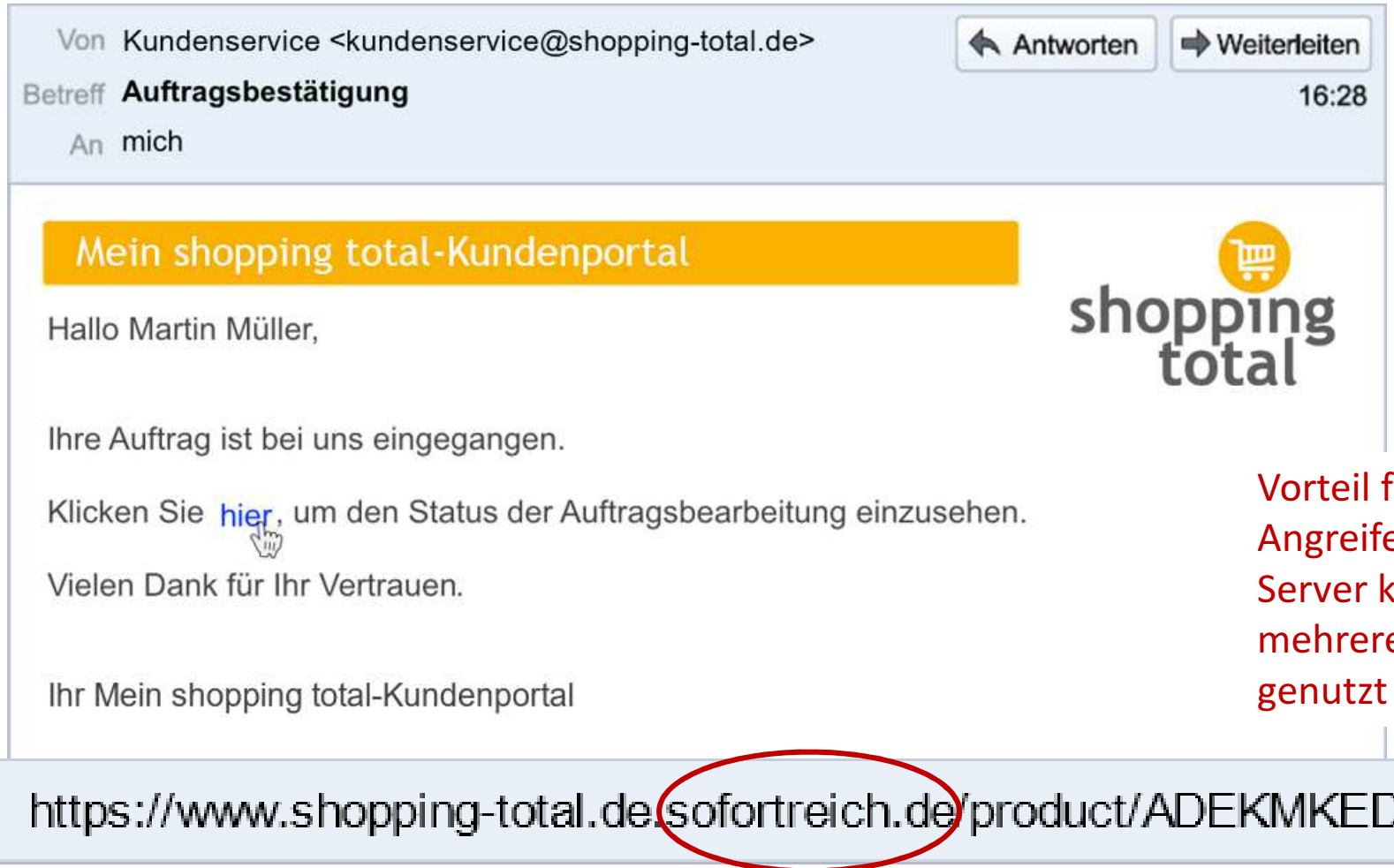
https://www.securepay24.de.secure.de.host547.com

https://host547.com/www.securepay24.de/login

Ist der Wer-Bereich plausibel?

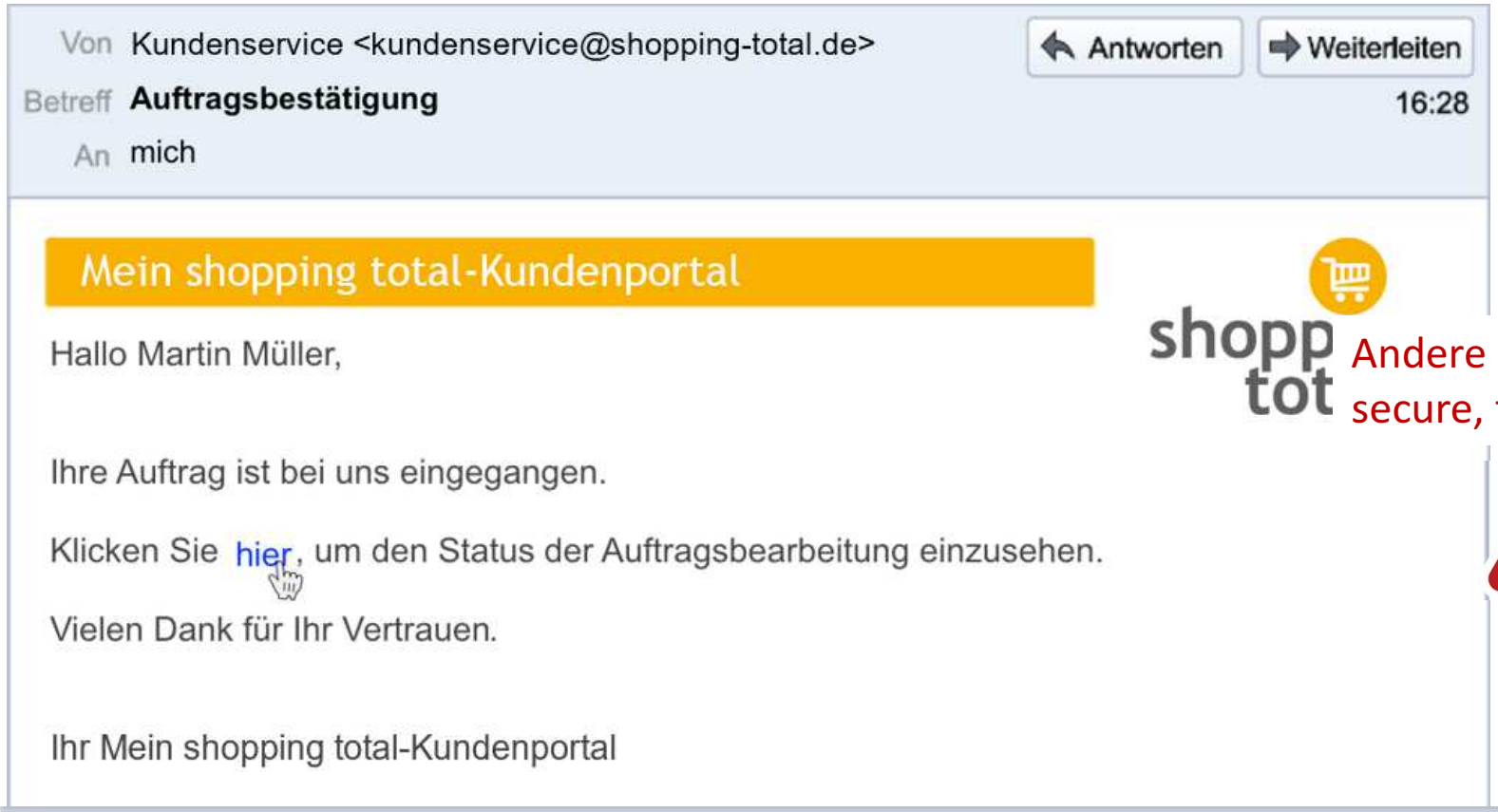


Ist der Wer-Bereich plausibel?



Vorteil für den Angreifer: Der selbe Server kann für mehrere Anbieter genutzt werden.

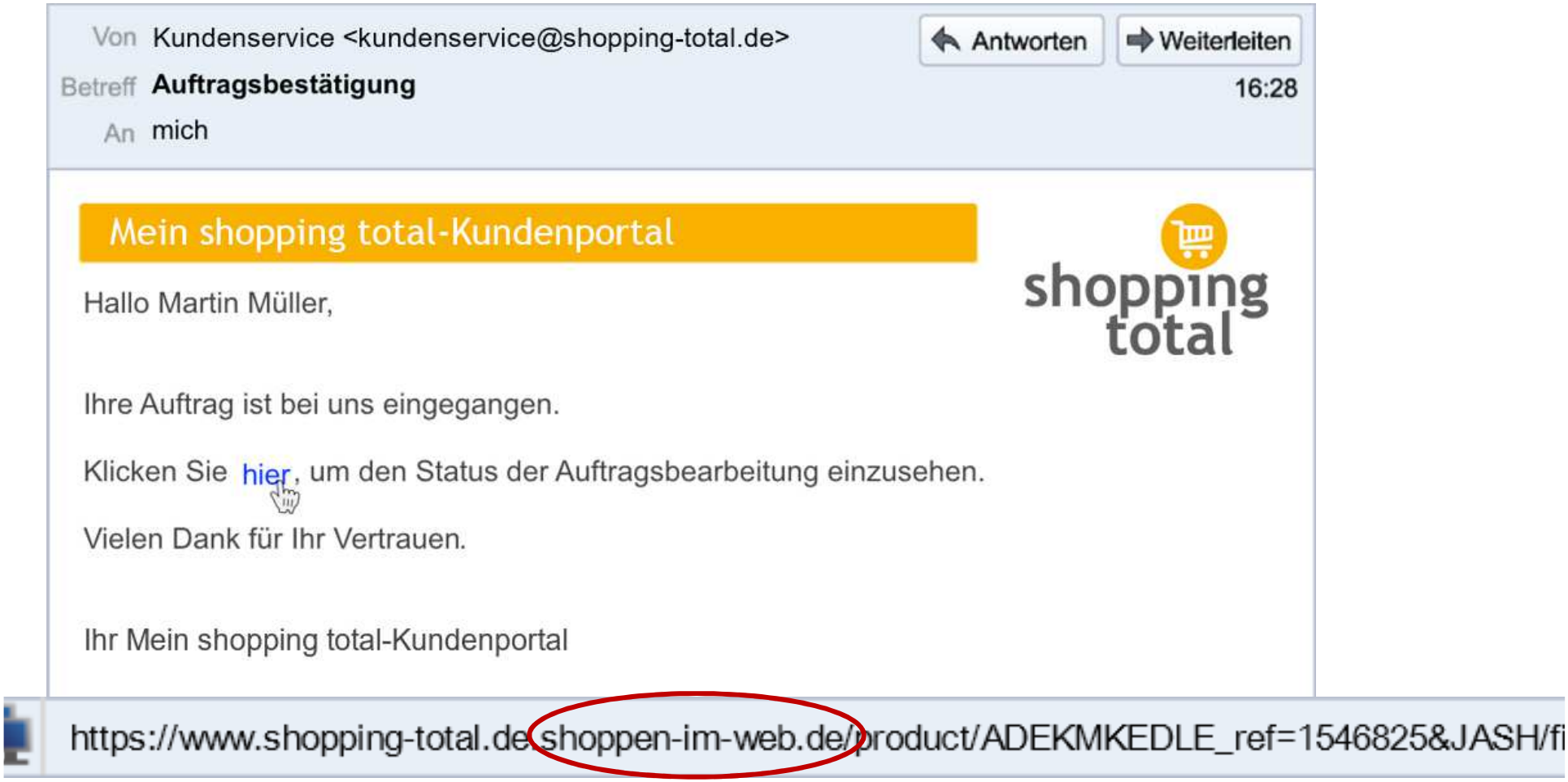
Ist der Wer-Bereich plausibel?



shopp tot

Andere Beispiele:
secure, trust, usw.

Ist der Wer-Bereich plausibel?



Vorsicht Falle: Wer-Bereich ist leicht verändert durch andere Zeichen

- 1inkedin.com statt linkedin.com
- tvvitter.com statt twitter.com
- media-rnarkt.de statt media-markt.de
- eurovvings.de statt eurowings.de
- sparkasse-duesselclorf.de statt sparkasse-duesseldorf.de
- 0tto.de statt otto.de

Wie soll ich damit umgehen?

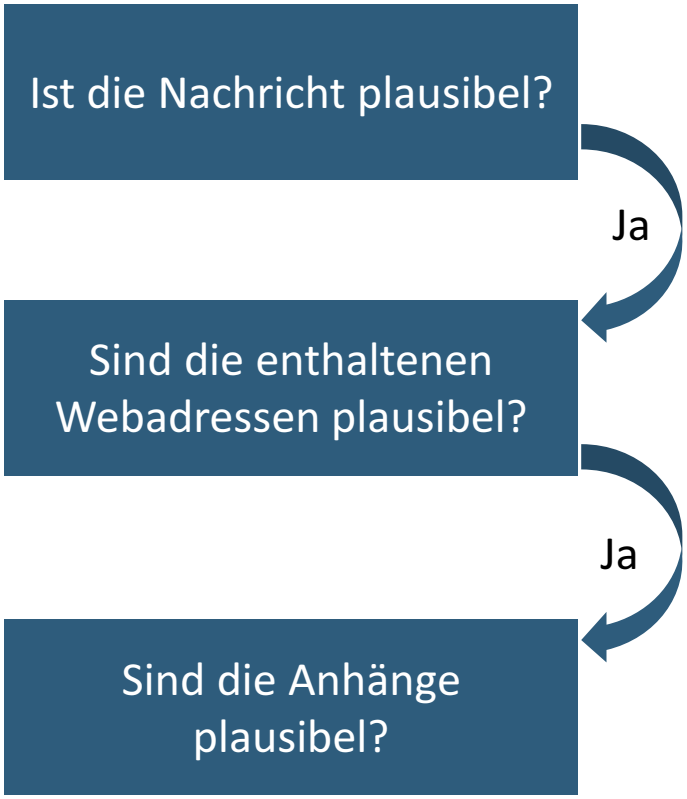
- Holen Sie weitere Informationen ein
  - Geben Sie den Ihnen bekannten **Wer-Bereich im Web-Browser** ein
  - Prüfen Sie, ob bei einer Suche nach dem Wer-Bereich in einer **Suchmaschine** einer der ersten Einträge auch diesen Wer-Bereich hat

- **Vergleichen Sie den Wer-Bereich mit dem aus Web-Adressen aus früheren Nachrichten**

- **Kontaktieren Sie den Anbieter bzw. die Person über die Ihnen bekannten Kontaktmöglichkeiten**

Unplausible Nachrichten direkt löschen!

Wie erkennen Sie gefährliche Nachrichten?



Wie?

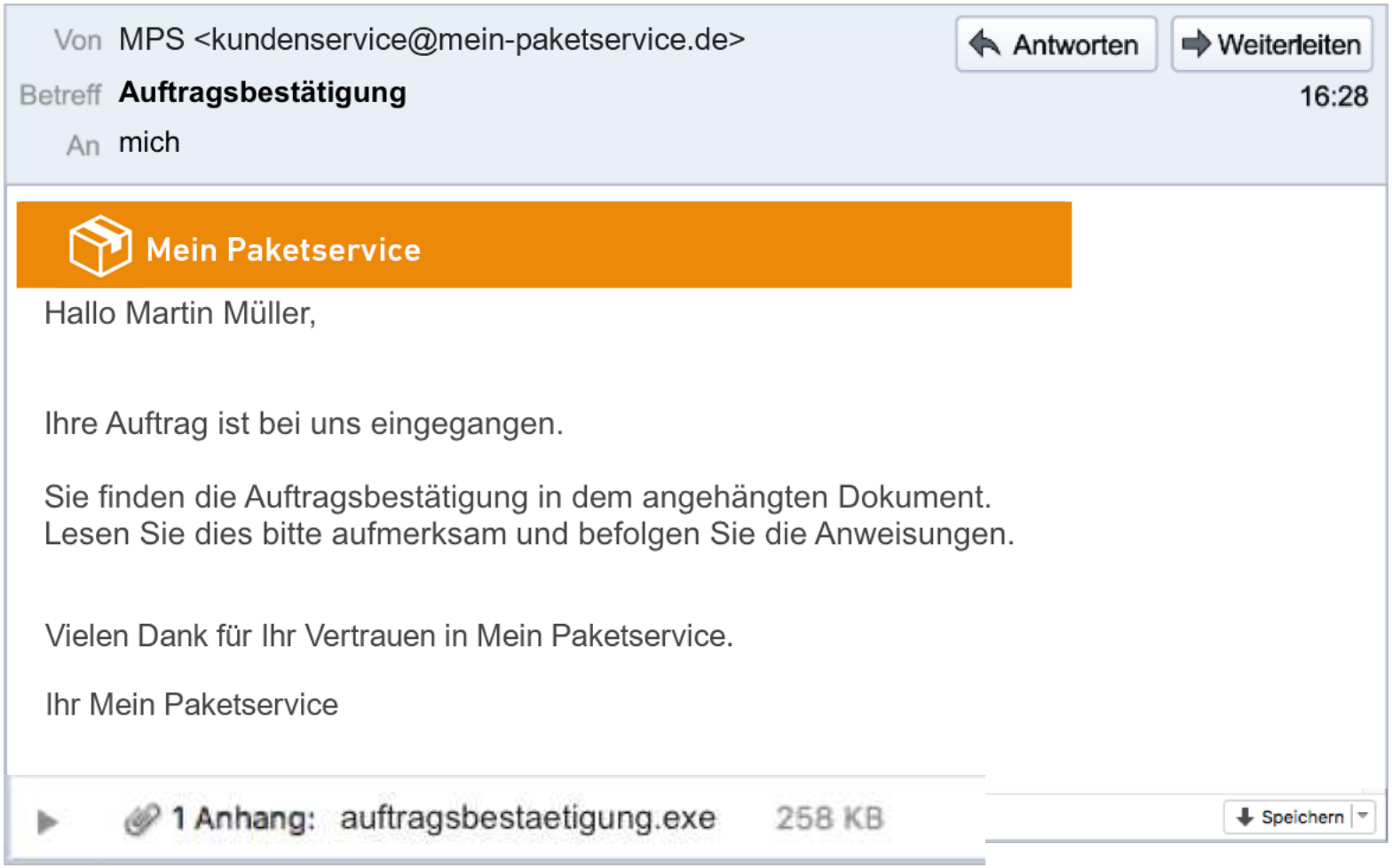
- Absender passt zum Inhalt der Nachricht?
- Inhalt der Nachricht plausibel?

- Richtige Webadresse identifizieren
- Identifizieren Sie den „Wer-Bereich“
- Hat der „Wer-Bereich“ Bezug zum Absender und Nachricht ?

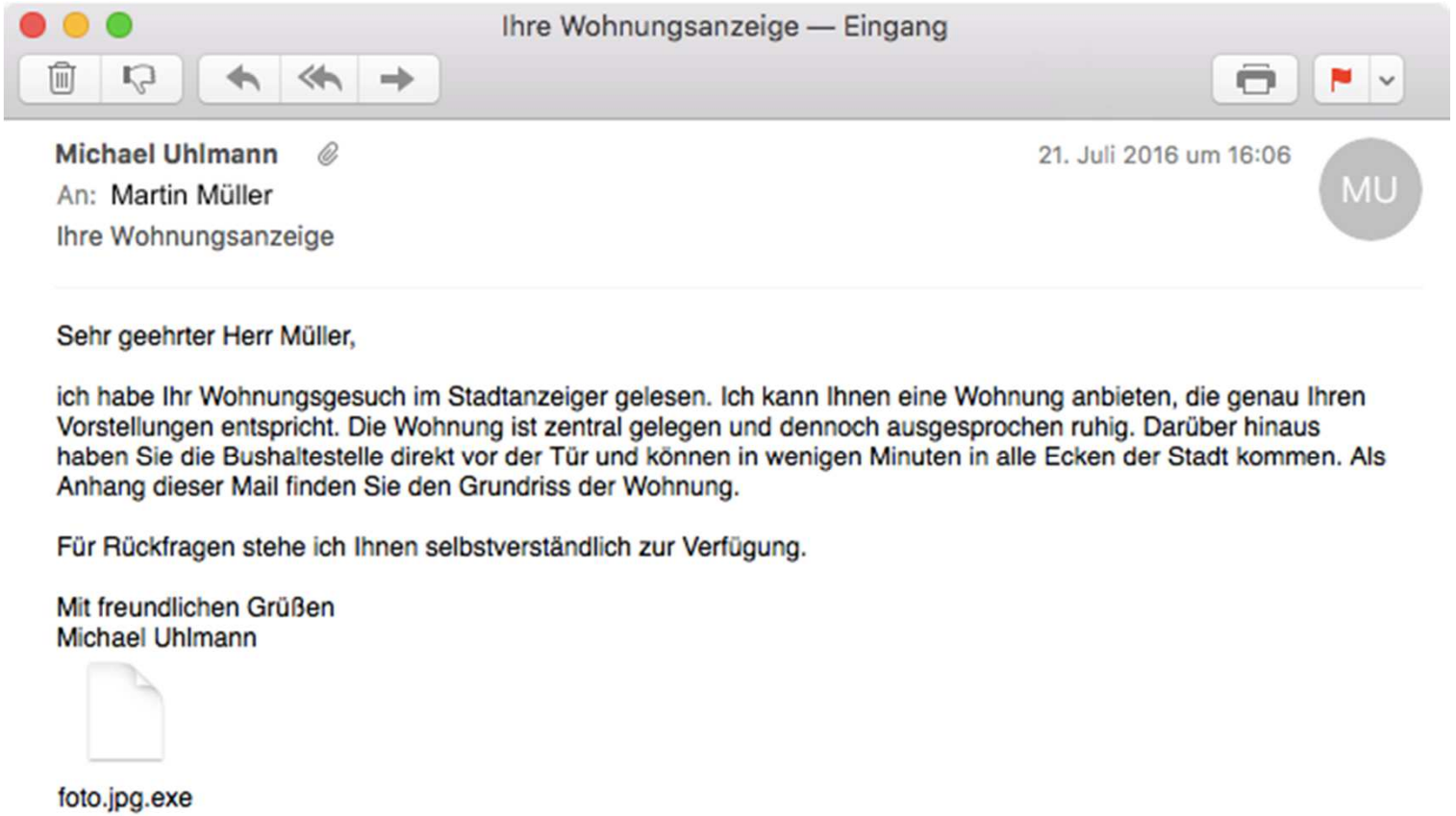
- Anhang identifizieren
- Identifizieren Sie das Dateiformat
- Erwarten Sie den Anhang vom Absender?

Wenn Sie eine der Fragen mit **Nein** beantworten, **löschen Sie die Nachricht**.
Wenn Sie sich nicht sicher sind, informieren Sie sich auf anderem Weg.

Vertrauen Sie dieser E-Mail?



Vertrauen Sie dieser E-Mail?

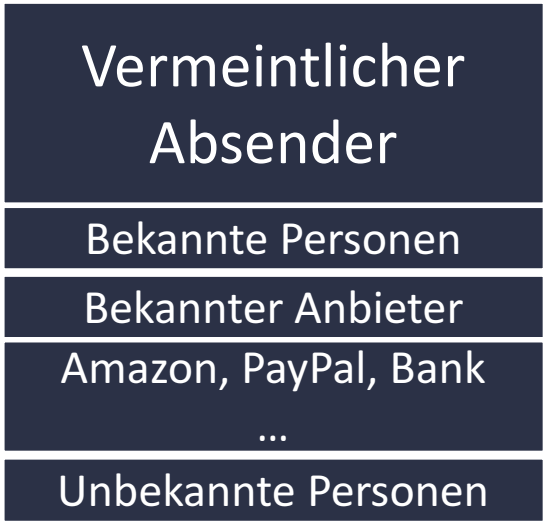


Woran erkennen Sie gefährliche Anhänge?

- Beachten Sie das Format des Anhangs:
  - Potentiell gefährlich: direkt ausführbaren Anhang (z.B. Formate .exe, .bat, .com, .cmd, .scr, .pif) oder
  - Potentiell gefährlich: Anhang, der möglicherweise Makros ausführen kann (z.B. Microsoft Office Dateien wie z.B. Formate .doc, .docx, .ppt, .pptx, .xls, .xlsx)

  - Ist Ihnen das Format eines Anhangs gänzlich unbekannt?
    - Nicht öffnen!
    - Bei bekannten Absendern, fragen Sie nach.

Was haben wir bisher gelernt?



Warum geht das so einfach?

Absender können oft *einfach* gefälscht werden

Information über Freunde/ Themen aus sozialen/ beruflichen Netzwerken

Account der Person nach Identitätsdiebstahl verwenden

Was haben wir noch gelernt?

Jeder ist betroffen Unabhängig von…			
Alter	Einkommen / Vermögen	Jobposition	…

Warum ist jeder betroffen?	
Automatisierte Angriffe	Informationen zusammentragen

Wer glaubt nicht betroffen zu sein, kennt Schutzmaßnahmen häufig nicht
➔ Einfaches Opfer

Viele Informationen über Sie im Netz verfügbar?
➔ Einfaches Opfer für gezielte Angriffe

Warum reichen heutige technische Schutzmaßnahmen nicht aus?

- Betrüger passen Strategien an verfügbare technische Schutzmaßnahmen an
- Anpassung technischer Schutzmaßnahmen braucht Zeit

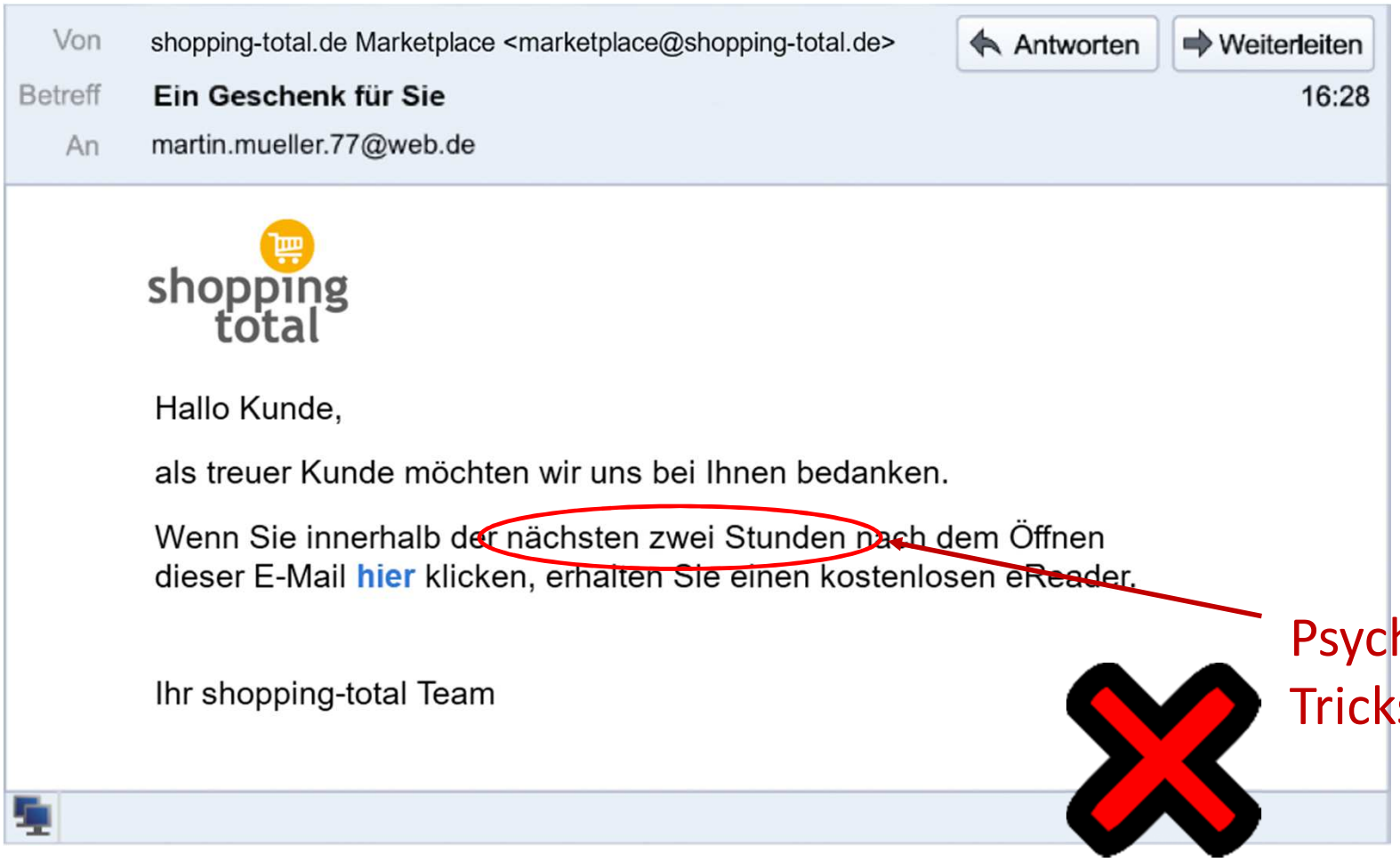
Es gibt keinen 100% Schutz!
Reduktion der Risiken möglich

Gefährliche Nachrichten direkt löschen!

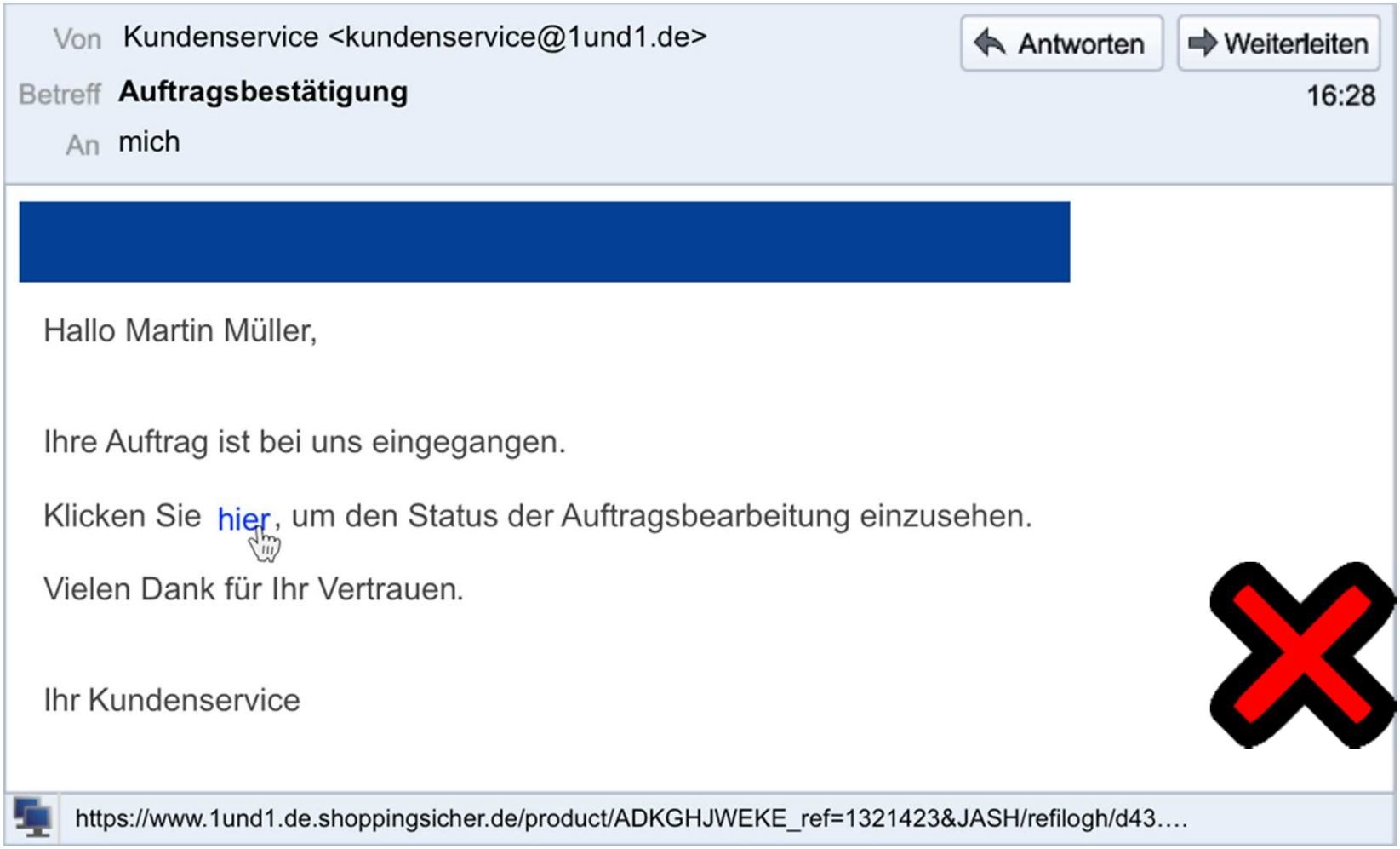
Video

Link zum Video
https://secuso.org/video

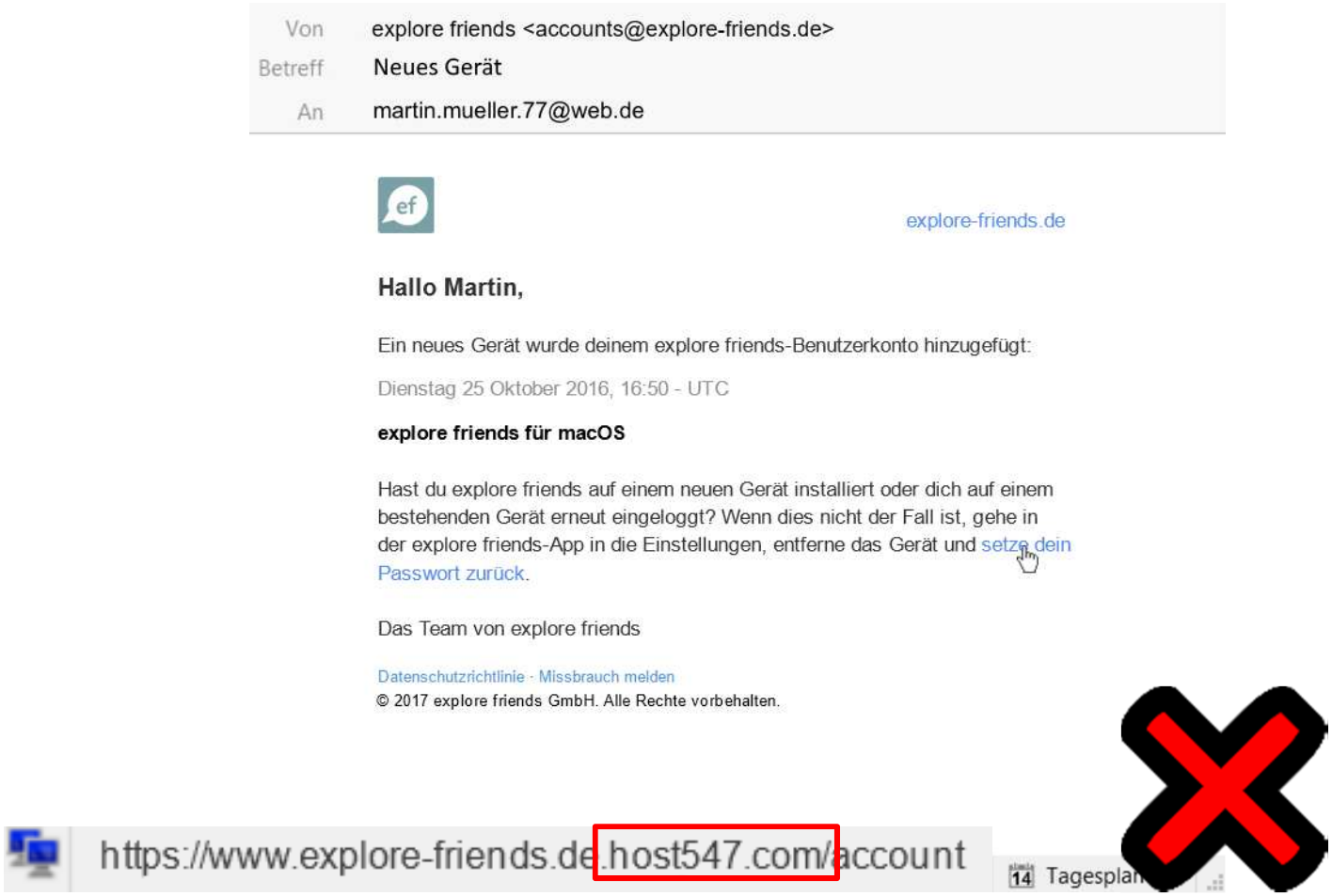
Vertrauen Sie dieser E-Mail?



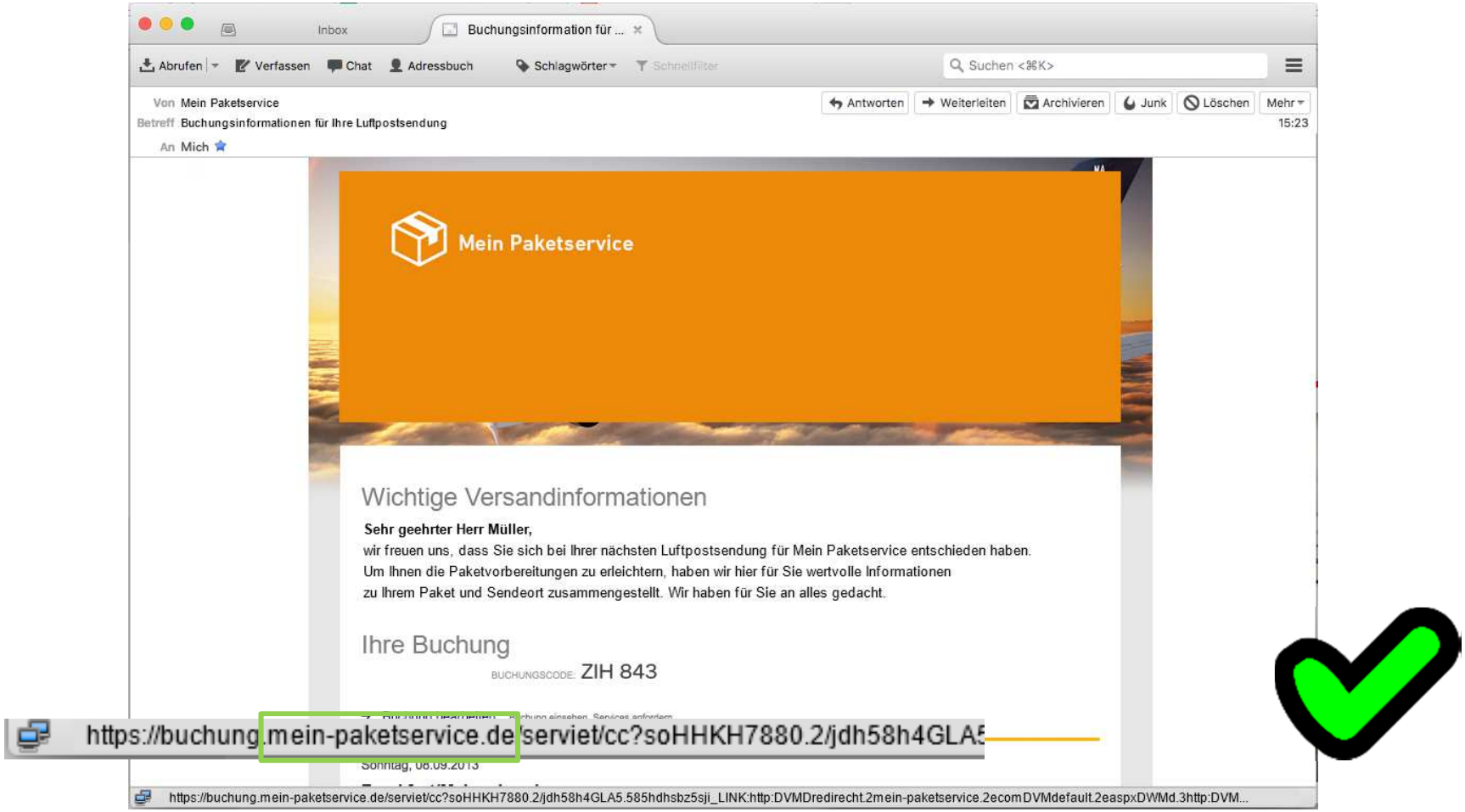
Vertrauen Sie dieser E-Mail?



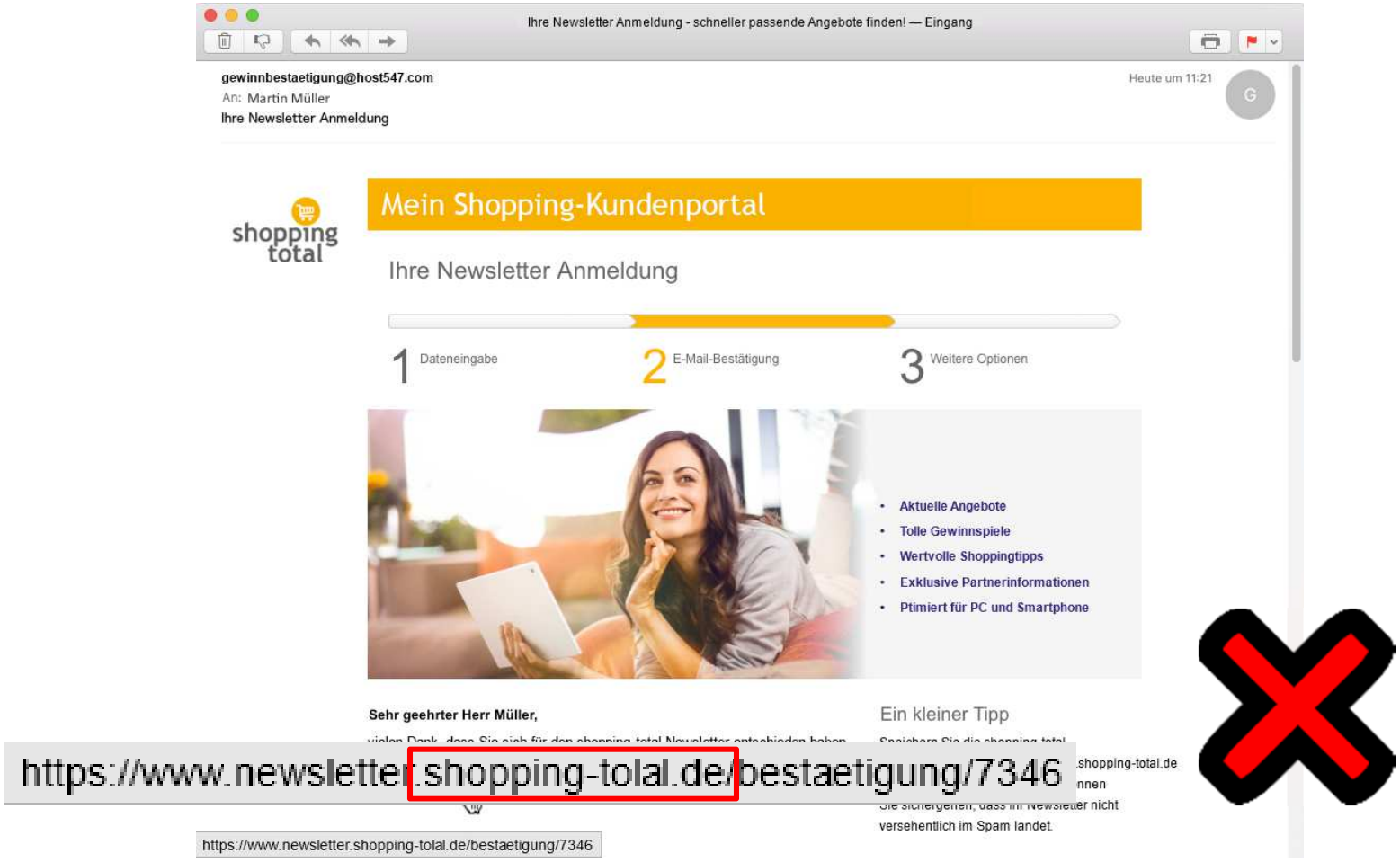
Vertrauen Sie dieser E-Mail?



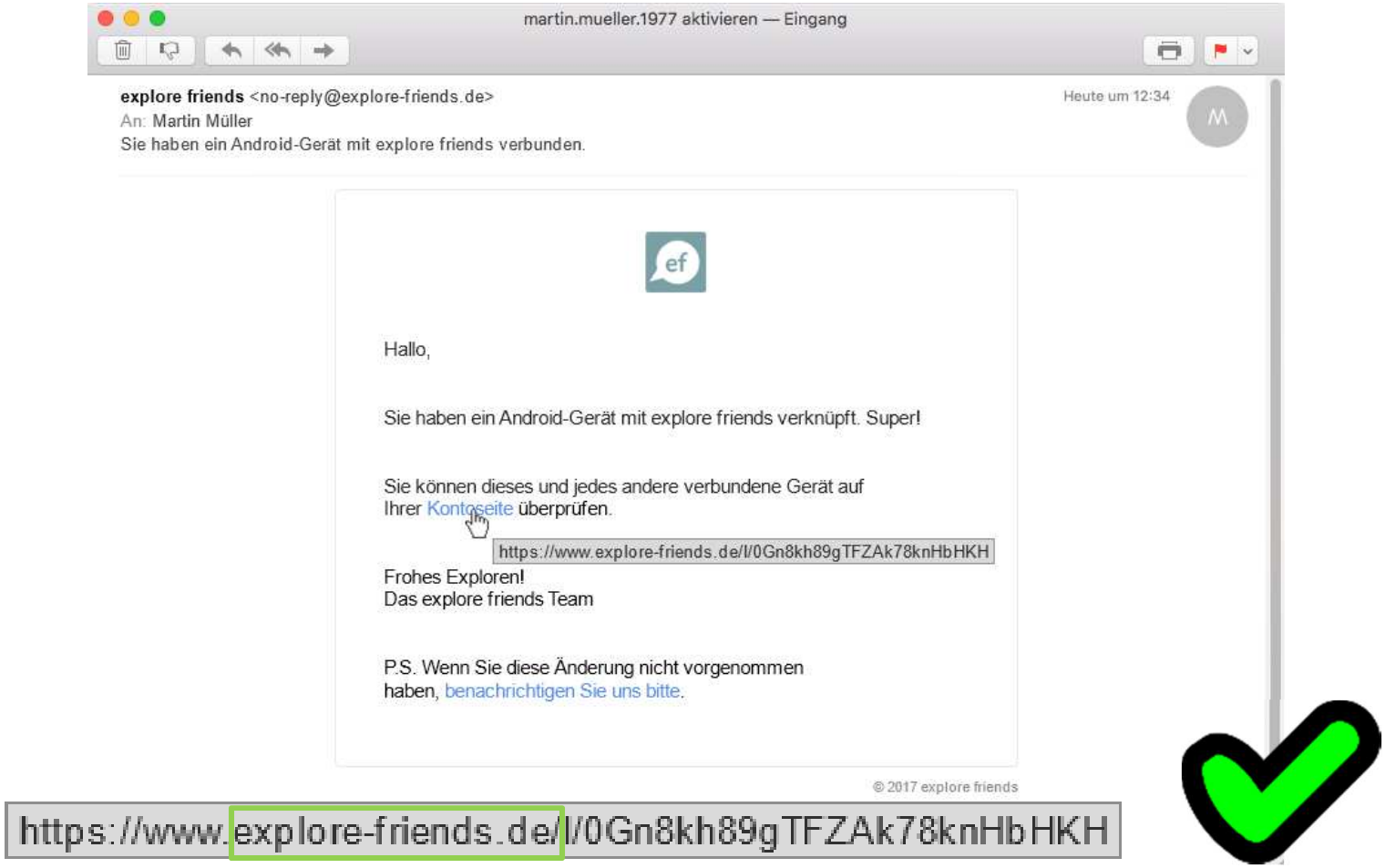
Vertrauen Sie dieser E-Mail?



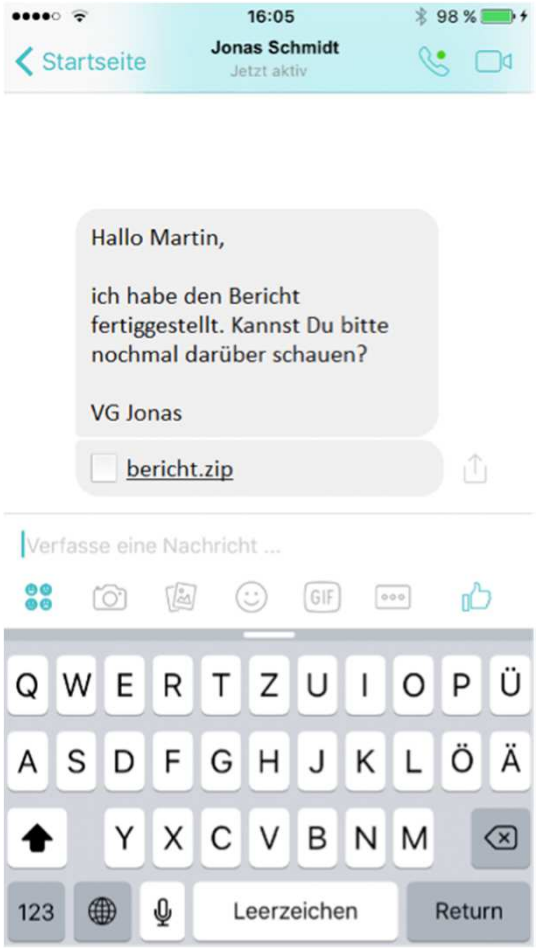
Vertrauen Sie dieser E-Mail?



Vertrauen Sie dieser E-Mail?



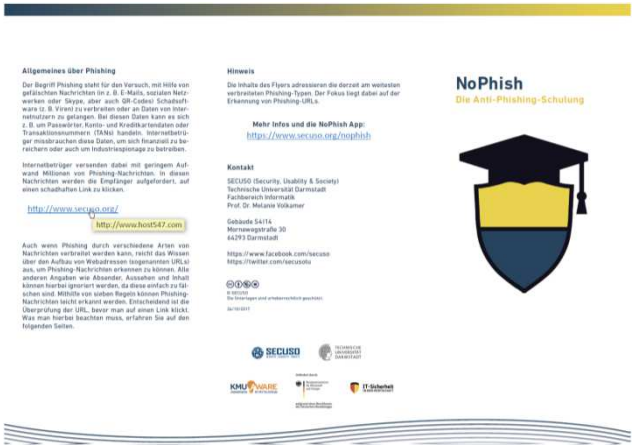
Vertrauen Sie dieser Nachricht?

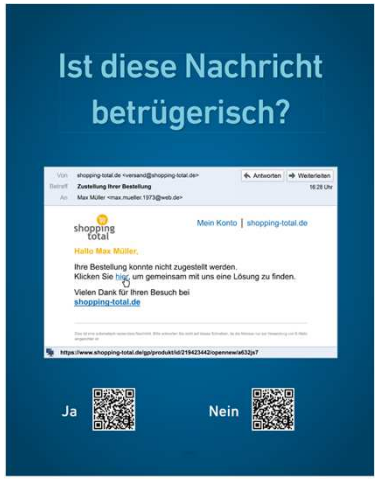


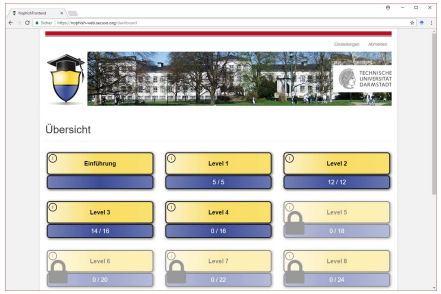
Wenn Nachricht für Sie plausibel, dann

Wenn Nachricht für Sie NICHT plausibel, dann

Materialien für Sensibilisierung, Schulungen und Werkzeuge







Wenn Sie mehr Wissen möchten

Links:

Web Training
https://nophish-web.secuso.org

Android App
Erhältlich im Google Play Store

Add-On für Thunderbird, dass Sie beim Erkennen gefährlicher Links unterstützt
https://www.secuso.org/torpedo

Infos zu allen anderen Themen:

https://www.secuso.org

Aktuelle Tipps und Neuigkeiten:

https://www.facebook.com/Secuso

https://twitter.com/secusotu

Ihre Ansprechpartner

Technische Universität Darmstadt
SECUSO
Mornewegstraße 30
64293 Darmstadt

Prof. Dr. Melanie Volkamer

Leiterin der Gruppe
melanie.volkamer@secuso.org

Dr. Marco Ghiglieri

Wissenschaftlicher Mitarbeiter
marco.ghiglieri@secuso.org

Benjamin Reinheimer

Wissenschaftlicher Mitarbeiter
benjamin.reinheimer@secuso.org