Schutz vor Phishing und anderen betrügerischen Nachrichten

Initiative „IT-Sicherheit in der Wirtschaft“

Unterstützung kleiner und mittelständischer Unternehmen beim sicheren Einsatz von IKT-Systemen

Gefördert durch:

aufgrund eines Beschlusses
des Deutschen Bundestages

www.it-sicherheit-in-der-wirtschaft.de

KMU AWARE

- Verlagerung von Unternehmensabläufen ins Digitale
- Angriffe aus der digitalen Welt
- Vielfältige Konsequenzen

- Ausnutzen menschlicher Schwachstellen verhindern
- Hilfe zur Selbsthilfe
- Awareness
- Bereitstellen von benutzerfreundlichen Technologien

Modul 1: Einführung in das Thema Nachrichten mit gefährlichem Inhalt

Modul 2: Erkennung von unplausiblen Nachrichten mit gefährlichem Inhalt

Modul 3: Erkennung von plausiblen Nachrichten mit gefährlichen Links

Modul 4: Erkennung von plausiblen Nachrichten mit gefährlichen Anhängen

Gefährliche Inhalte … und Konsequenzen

- Gefährliche Datei zum Öffnen/Ausführen → Alle an Ihrem Gerät durchgeführten Aktionen *ausspähen*
  → Identitätsdiebstahl, Erpressung, …
- Gefährliche Links zum Klicken
  - (Unbemerkter) Download von Schadsoftware → Eigene Aktionen an Ihrem Gerät *durchführen* bis hin zur Blockierung der Nutzung durch Sie
    → Identitätsdiebstahl, Erpressung, …
  - Öffnen betrügerischer aber authentisch aussehender Webseite zum Einloggen → Ihre Daten/Aktionen im Account *einsehen*
    → Identitätsdiebstahl, Erpressung, …

„Phishing“

- Aufforderung sensible Daten wie Passwörter und Bankdaten zu schicken → Ihren Account nutzen und eigene Aktionen *durchführen*
  → Identitätsdiebstahl, Erpressung, …
- Aufforderung Rechnung zu begleichen durch Überweisungen oder vermeintliche Geschäftspartner anzurufen → Falsche Kontonummer bzw. kostenpflichtige Nummer
  → Geld abgreifen

Verwendete Nachrichtenformate

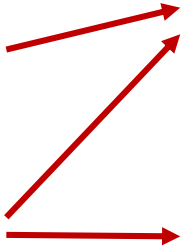
- E-Mails

  ... aber nicht nur E-Mails!

- Sondern auch
  - Messenger wie Skype, WhatsApp, Instagram und Snapchat
  - Soziale Netzwerke wie Facebook und Google+
  - Berufliche Netzwerke wie Xing und LinkedIn
  - SMS, MMS
  - ...

Vermeintlicher Absender

- Ein Ihnen bekannter und vertrauter Anbieter z.B. Ihre Bank, Amazon, PayPal
- Eine Ihnen bekannte Person z.B. Freund oder Arbeitskollege



Absender können oft *einfach* gefälscht werden

Information über Freunde/Themen aus sozialen/beruflichen Netzwerken

Account der Person nach Identitätsdiebstahl verwenden

- Unbekannte(r) Anbieter/Person…

Psychologische Tricks:
Emotionen erzeugen wie Angst, Zeitdruck, Glück oder Hilfsbereitschaft ausnutzen usw.

Jeder ist betroffen!

- Unabhängig …
  - … vom Alter
  - … vom Einkommen/Vermögen
  - … von der Position im Unternehmen
  - … von der Häufigkeit/Art der genutzten Dienste

- Warum ist jeder betroffen?
  - Angriffe werden oft automatisiert in die Masse verschickt
  - Viele kleine Beträge ergeben auch eine große Summe
  - Informationen werden zunächst für Angriff zusammengetragen

Wer glaubt nicht betroffen zu sein, kennt Schutzmaßnahmen nicht
→ Einfaches Opfer

Viele Informationen im Netz verfügbar → Einfaches Opfer für gezielte Angriffe

Warum reichen technische Schutzmaßnahmen nicht aus?

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

→ Reduzieren der Risiken durch technische Schutzmaßnamen
... aber kein vollständiger Schutz

Ziel des restlichen Vortrags:
Lernen, wie Sie betrügerische Nachrichten erkennen.

Betrügerische Nachrichten direkt löschen!

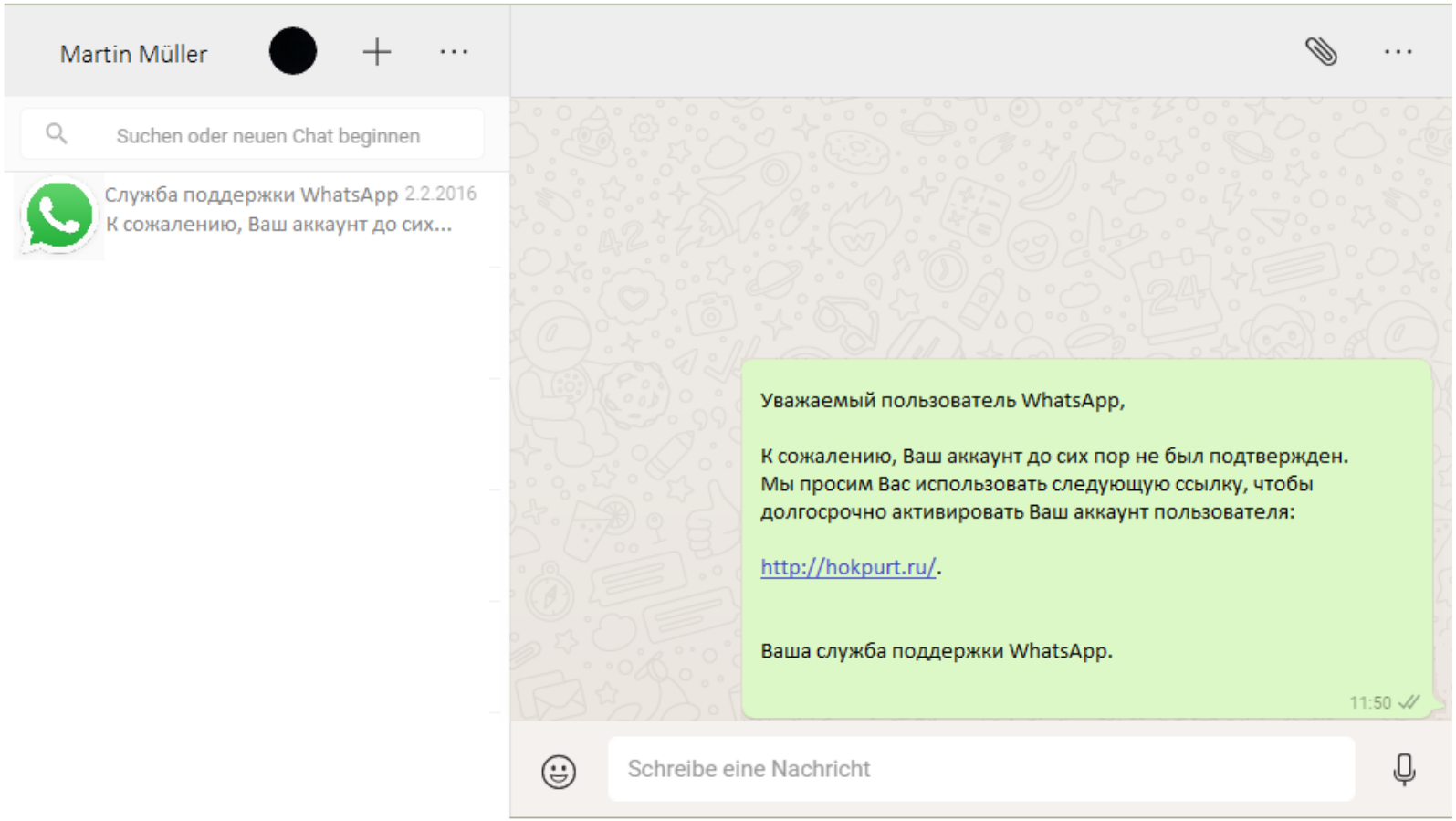
Modul 1: Einführung in das Thema Nachrichten mit gefährlichem Inhalt

Modul 2: Erkennung von unplausiblen Nachrichten mit gefährlichem Inhalt

Modul 3: Erkennung von plausiblen Nachrichten mit gefährlichen Links

Modul 4: Erkennung von plausiblen Nachrichten mit gefährlichen Anhängen

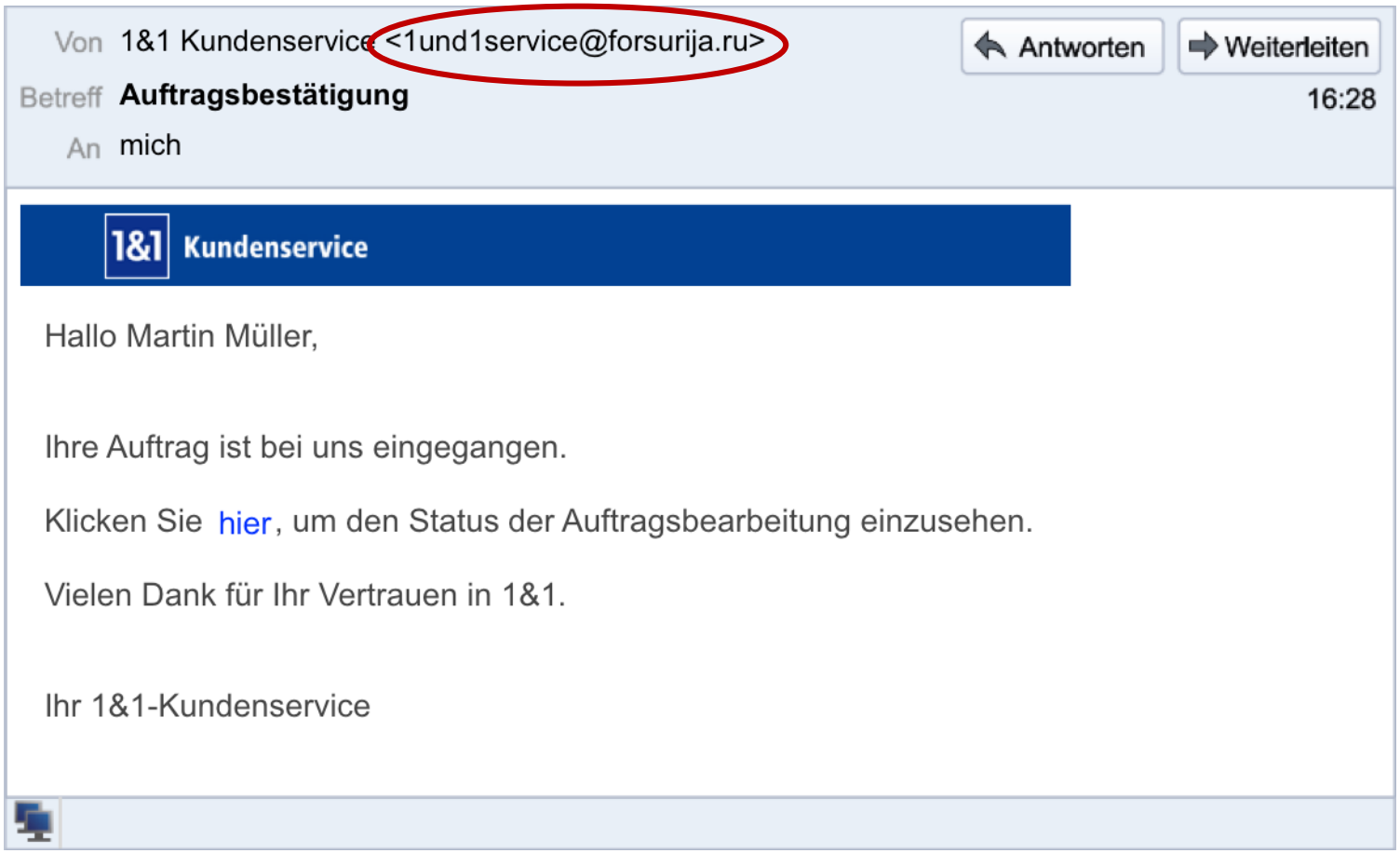
Sprechen Sie die Sprache, in der die Nachricht verfasst ist?



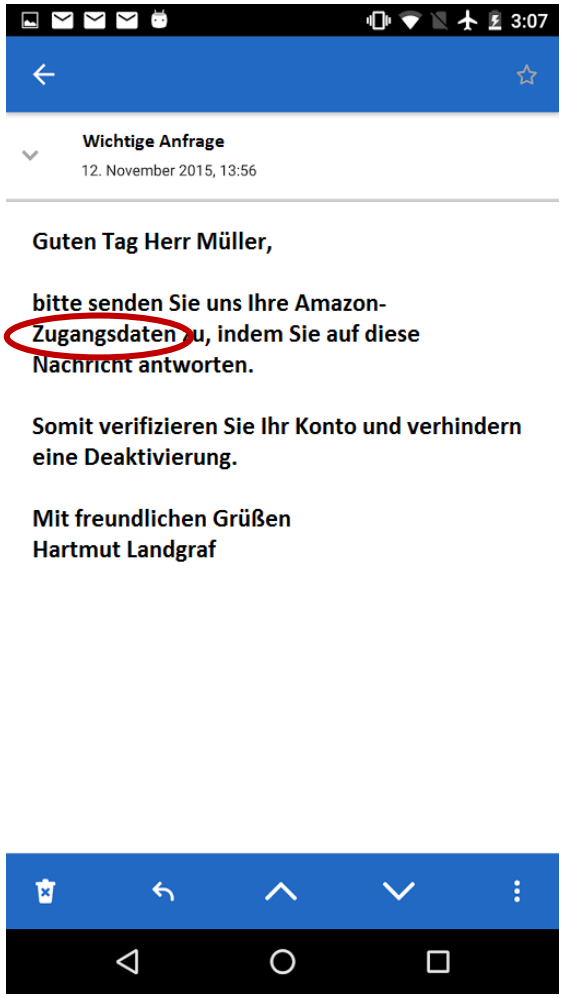
Passt das Design der Nachricht zum (vermeintlichen) Absender?

Entspricht die Sprache der Sprache des (vermeintlichen) Absenders?

Passt die Angabe des (vermeintlichen) Absenders zum Inhalt der Nachricht?



Werden Sie aufgefordert sensible Daten zu schicken?



3:07

Wichtige Anfrage

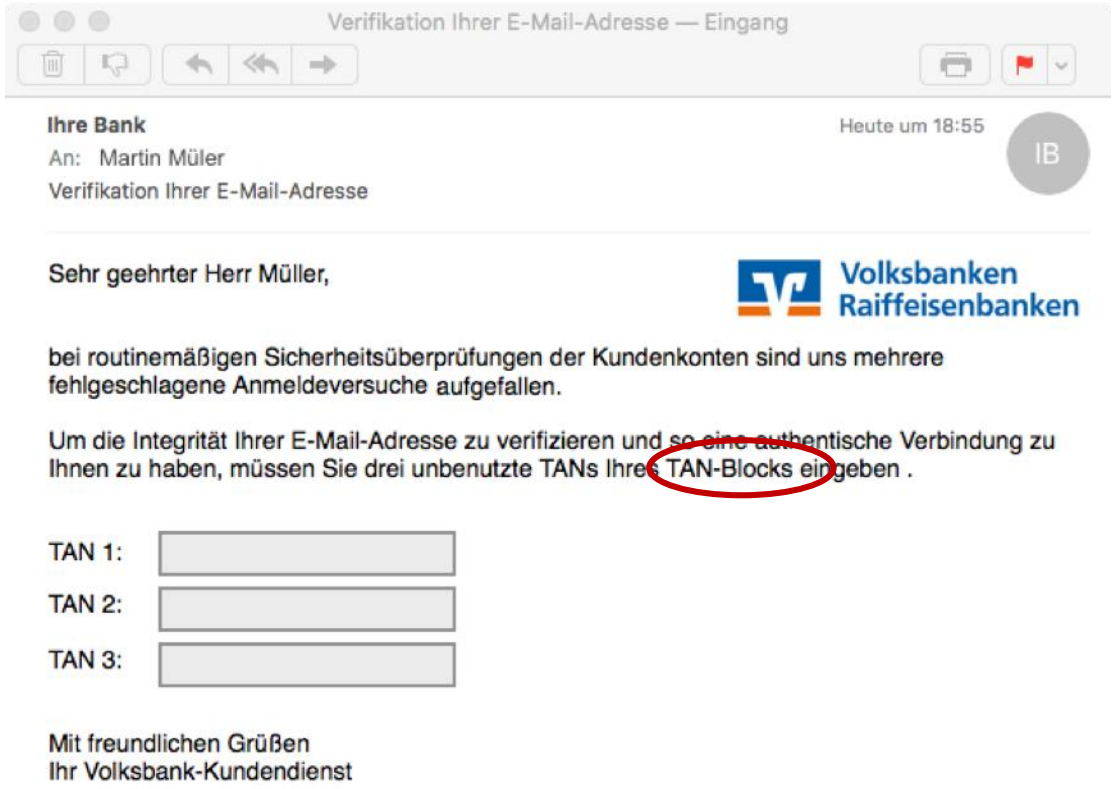
12. November 2015, 13:56

Guten Tag Herr Müller,

bitte senden Sie uns Ihre Amazon-Zugangsdaten zu, indem Sie auf diese Nachricht antworten.

Somit verifizieren Sie Ihr Konto und verhindern eine Deaktivierung.

Mit freundlichen Grüßen
Hartmut Landgraf



Verifikation Ihrer E-Mail-Adresse — Eingang

Ihre Bank
An: Martin Müler
Verifikation Ihrer E-Mail-Adresse

Heute um 18:55

IB

Sehr geehrter Herr Müller,

Volksbanken Raiffeisenbanken

bei routinemäßigen Sicherheitsüberprüfungen der Kundenkonten sind uns mehrere fehlgeschlagene Anmeldeversuche aufgefallen.

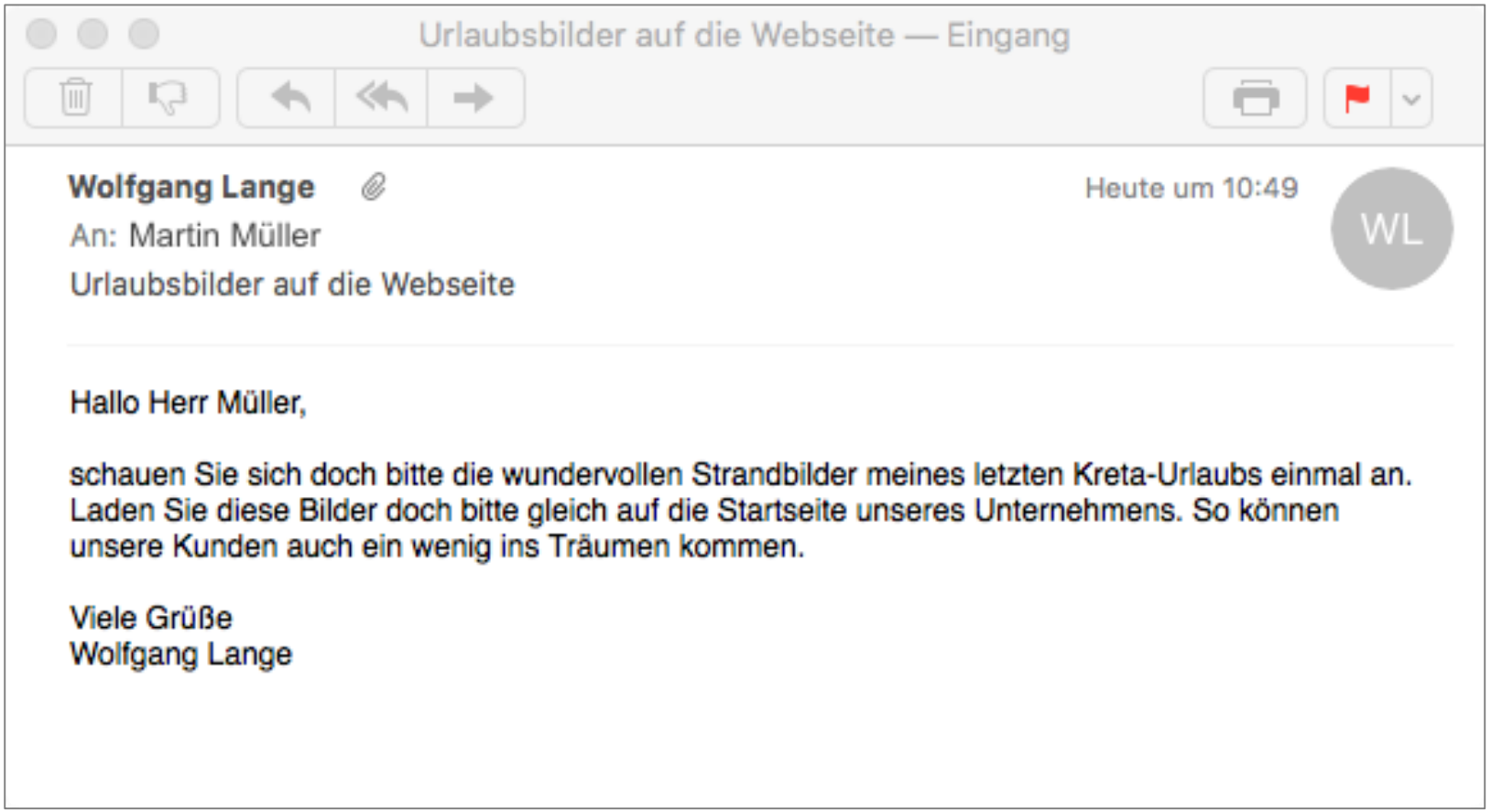
Um die Integrität Ihrer E-Mail-Adresse zu verifizieren und so eine authentische Verbindung zu Ihnen zu haben, müssen Sie drei unbenutzte TANs Ihres TAN-Blocks eingeben .

TAN 1:
TAN 2:
TAN 3:

Mit freundlichen Grüßen
Ihr Volksbank-Kundendienst

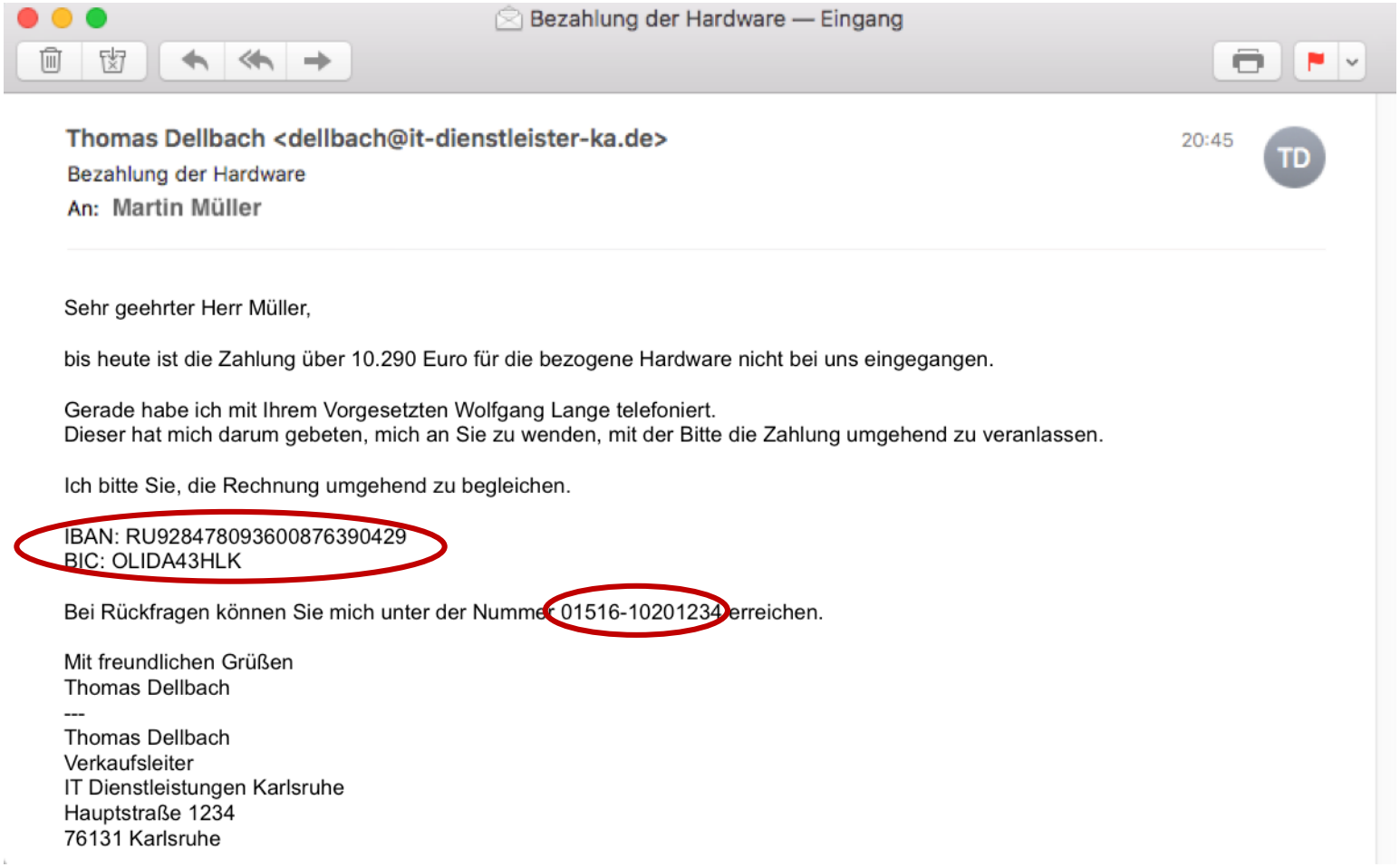
Seriöse Unternehmen werden Sie nicht zur Angabe derartiger Daten in einer Nachricht auffordern!

Passt der Inhalt der Nachricht zum (vermeintlichen) Absender?



Chef W. Lange soll diese Mail an Mitarbeiter Müller geschrieben haben.

Werden Sie aufgefordert potentiell kostenpflichtige Aktion durchzuführen?



Bezahlung der Hardware — Eingang

Thomas Dellbach <dellbach@it-dienstleister-ka.de> 20:45

Bezahlung der Hardware

An: **Martin Müller**

Sehr geehrter Herr Müller,

bis heute ist die Zahlung über 10.290 Euro für die bezogene Hardware nicht bei uns eingegangen.

Gerade habe ich mit Ihrem Vorgesetzten Wolfgang Lange telefoniert.
Dieser hat mich darum gebeten, mich an Sie zu wenden, mit der Bitte die Zahlung umgehend zu veranlassen.

Ich bitte Sie, die Rechnung umgehend zu begleichen.

IBAN: RU9284780936008763904 29
BIC: OLIDA43HLK

Bei Rückfragen können Sie mich unter der Nummer 01516-10201234 erreichen.

Mit freundlichen Grüßen
Thomas Dellbach

Thomas Dellbach
Verkaufsleiter
IT Dienstleistungen Karlsruhe
Hauptstraße 1234
76131 Karlsruhe

Modul 1: Einführung in das Thema Nachrichten mit gefährlichem Inhalt

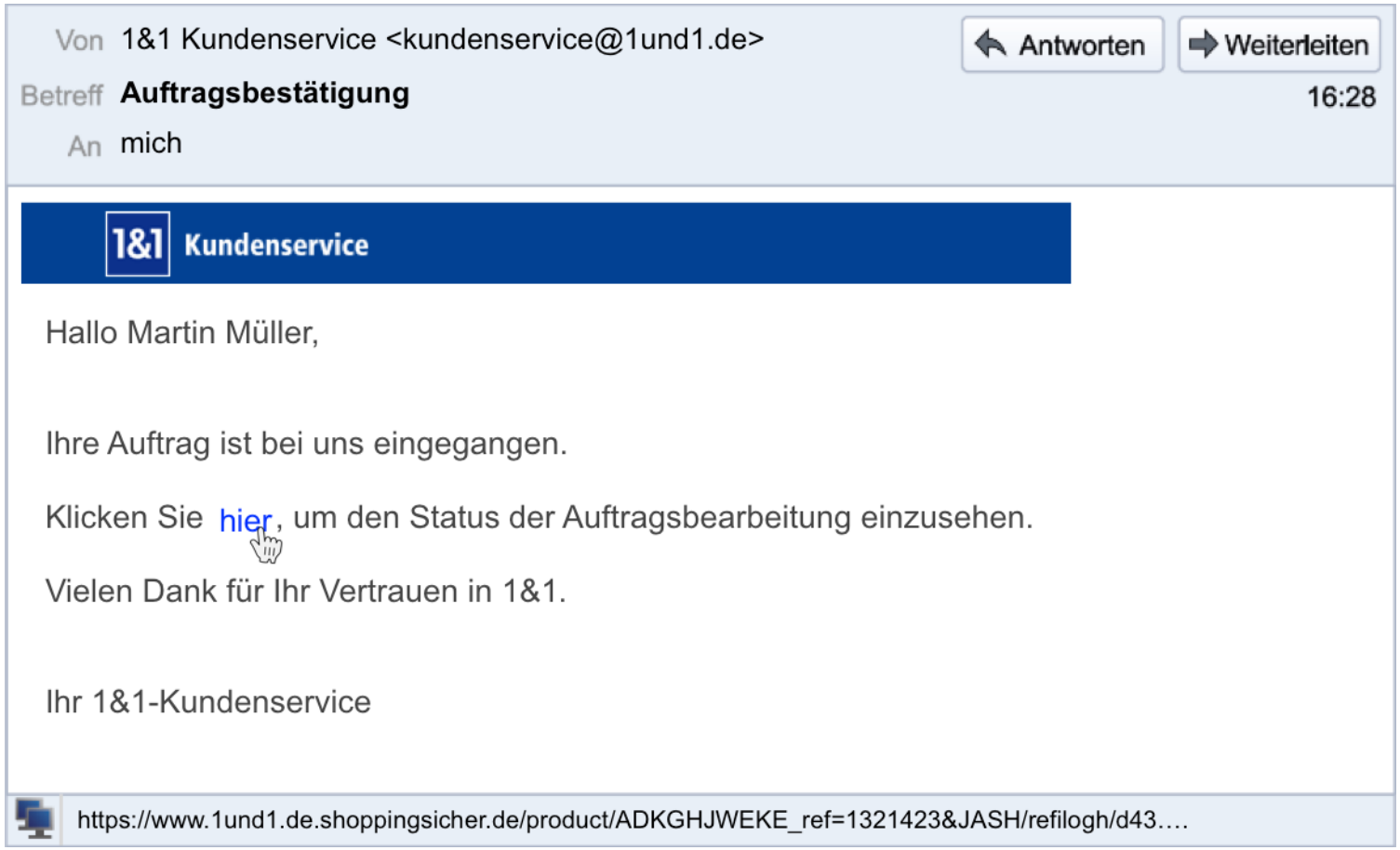
Modul 2: Erkennung von unplausiblen Nachrichten mit gefährlichem Inhalt

Modul 3: Erkennung von plausiblen Nachrichten mit gefährlichen Links

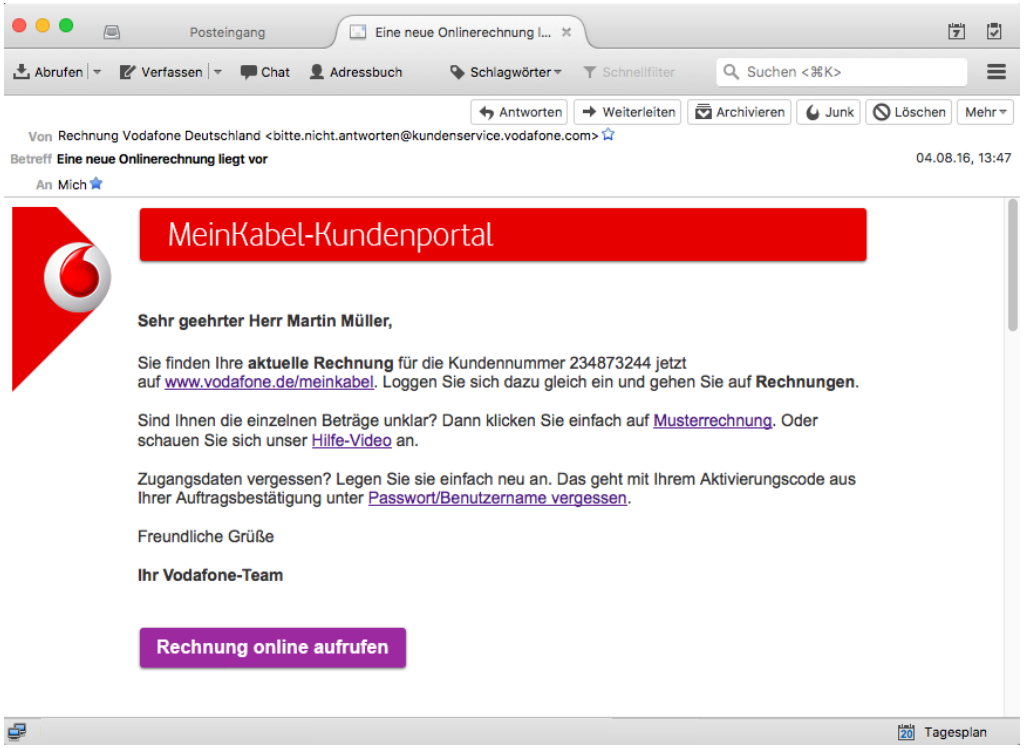
Modul 4: Erkennung von plausiblen Nachrichten mit gefährlichen Anhängen

Modul 3: Erkennung von plausiblen Nachrichten mit gefährlichen Links

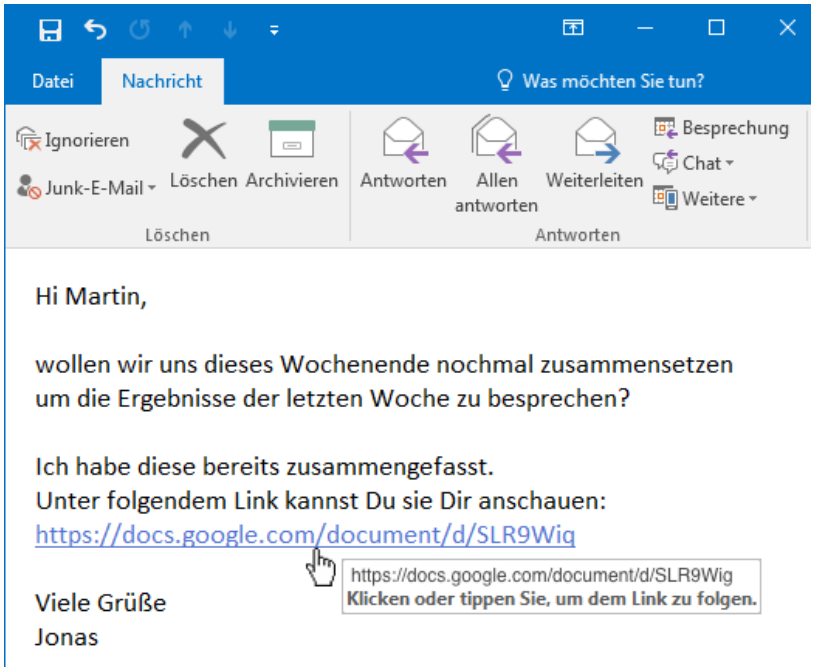
Ist dies ein gefährlicher Link?



1) Lassen Sie sich die Webadresse (URL) hinter dem Link anzeigen.



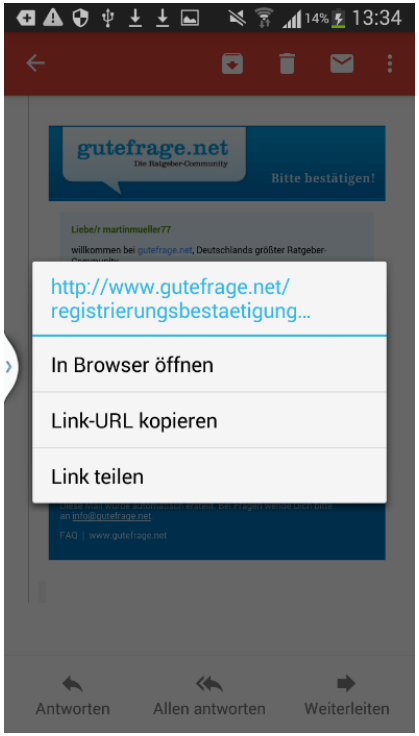
Statusleiste



Tooltip/Infofeld

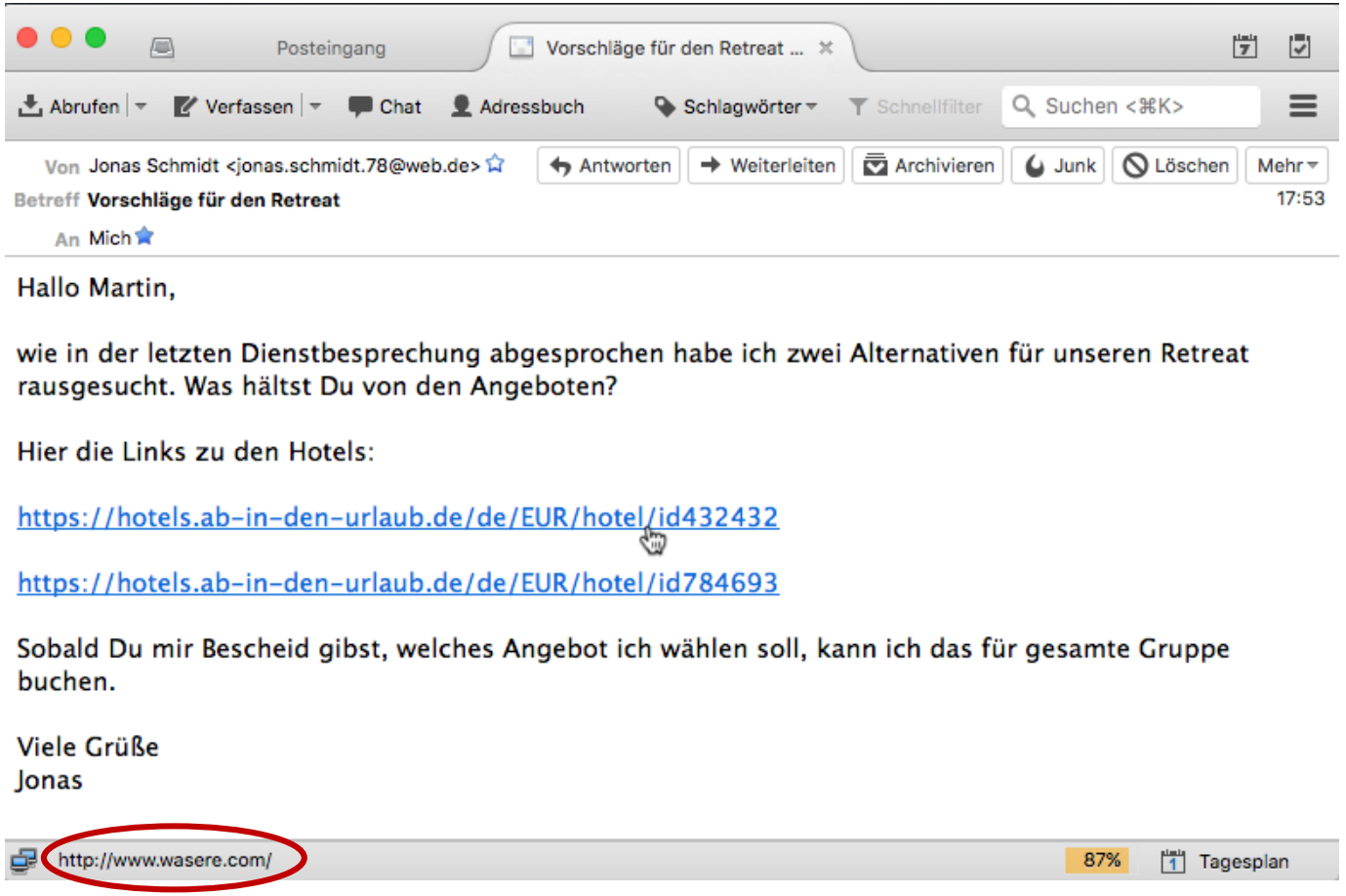
→ Ort der Anzeige hängt von Gerät, Software und Dienst ab

1) Lassen Sie sich die Webadresse (URL) hinter dem Link anzeigen.

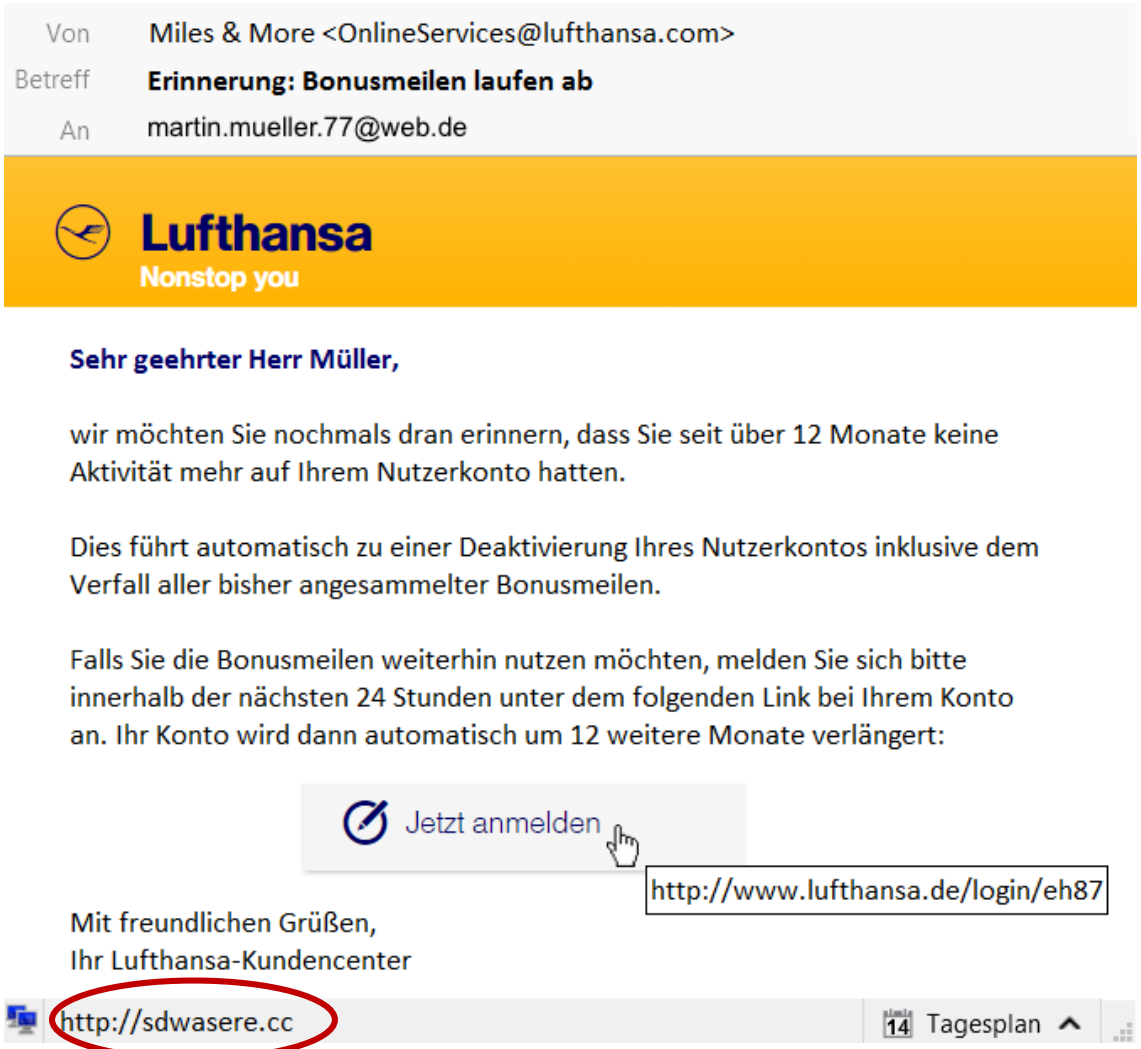


In Ausnahmefällen keine Anzeige → prüfen, ob diese aktivierbar ist oder die angezeigte URL bereits die Webadresse ist

Vorsicht Falle: Webadresse bereits in Nachricht sichtbar



Vorsicht Falle: Falscher Tooltip



2) Identifizieren Sie den sogenannten Wer-Bereich der Webadresse.

https://www.secuso.informatik.tu-darmstadt.de/de/secuso/neuigkeiten/

Wer-Bereich

https://www.secuso.informatik.tu-darmstadt.de

Wer-Bereich

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

Vorsicht Falle: Bekannte Wer-Bereiche an anderer Stelle

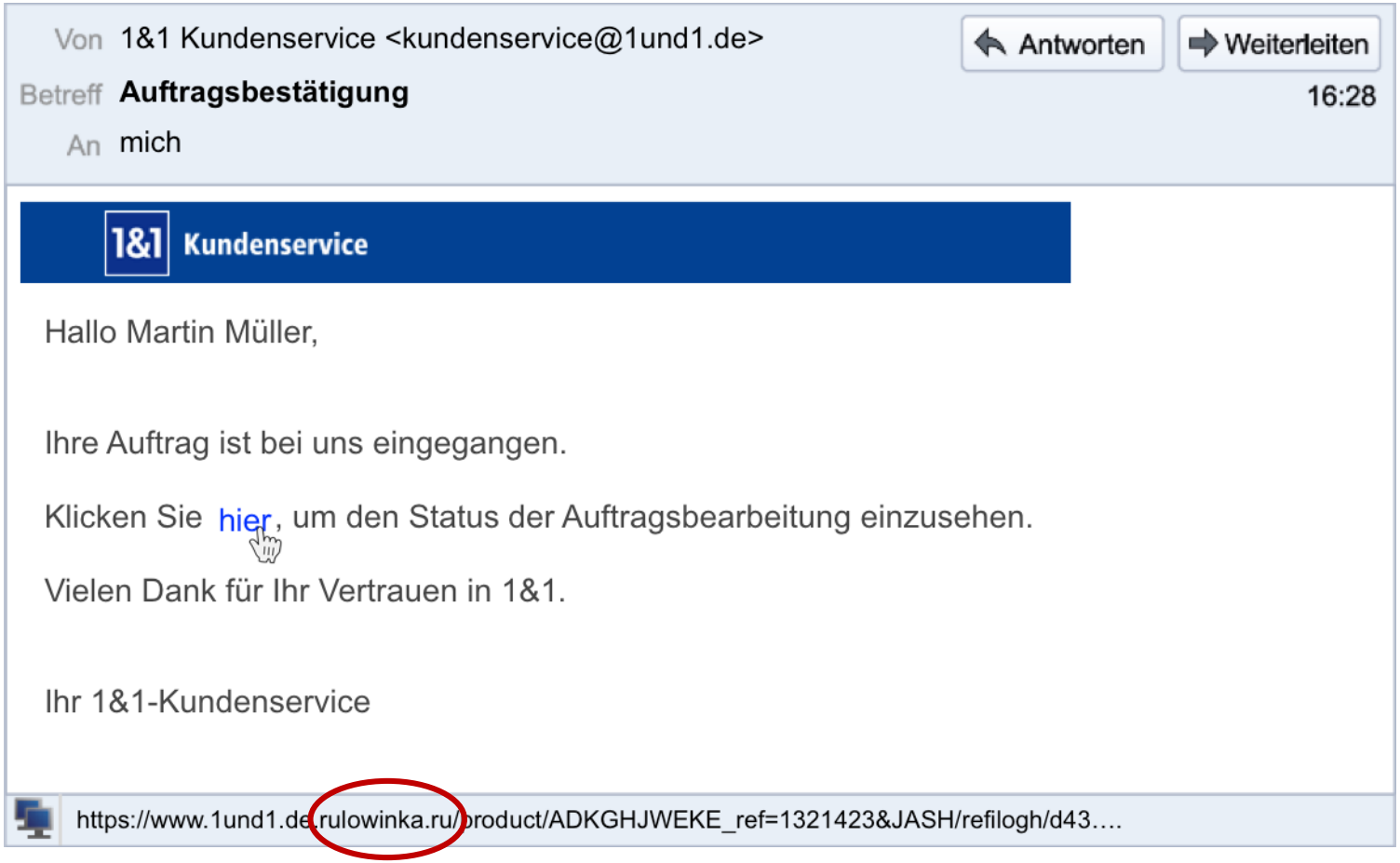
http://amazon.de.sdwasere.cc

http://sdwas.de/www.facebook.com/login

Vorsicht Falle: falsches Gefühl von Sicherheit durch „https://“

https://amazon.de.sdwasere.cc

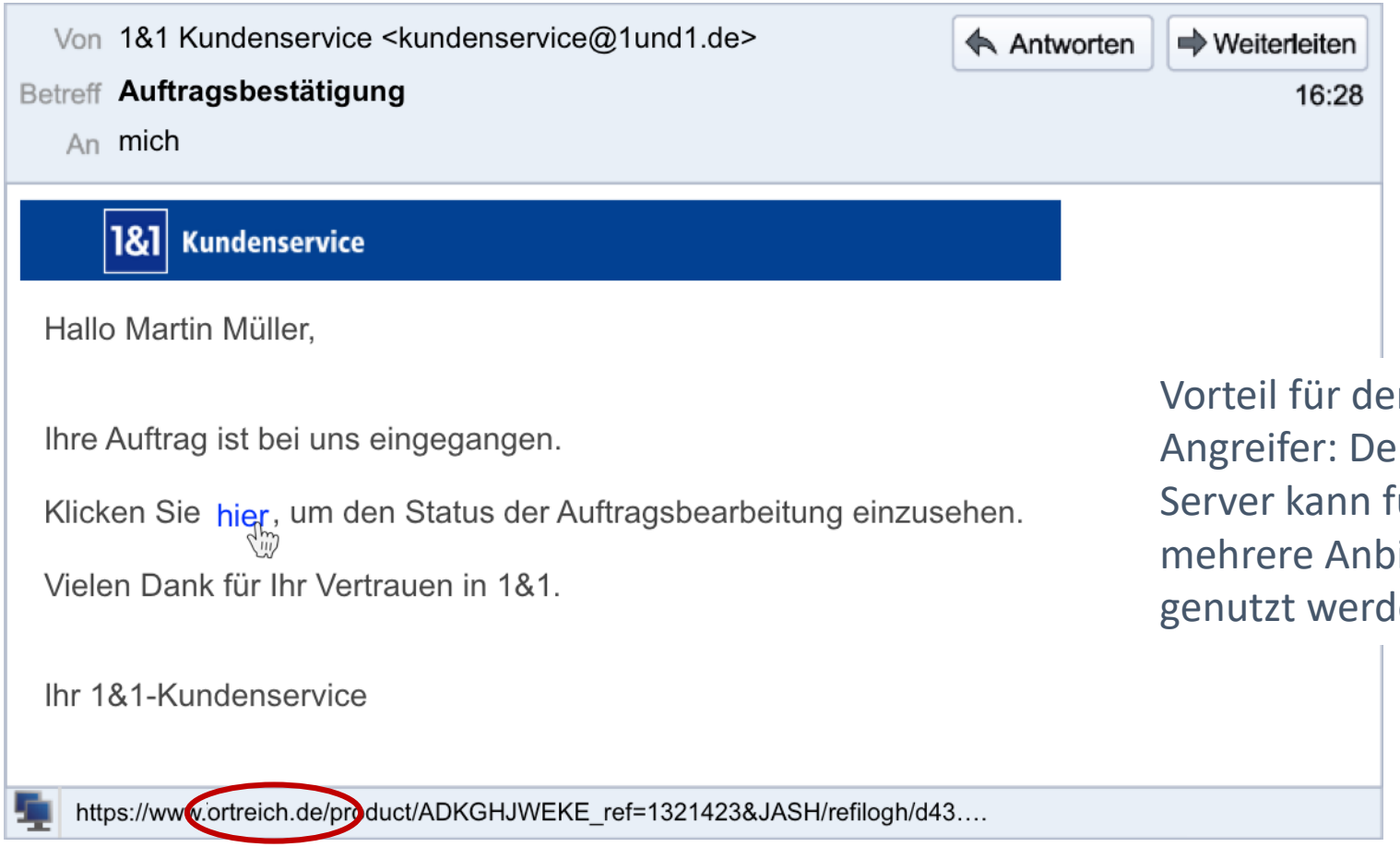
Vorsicht Falle: 99% sieht plausibel aus



Übung: Was ist der Wer-Bereich?

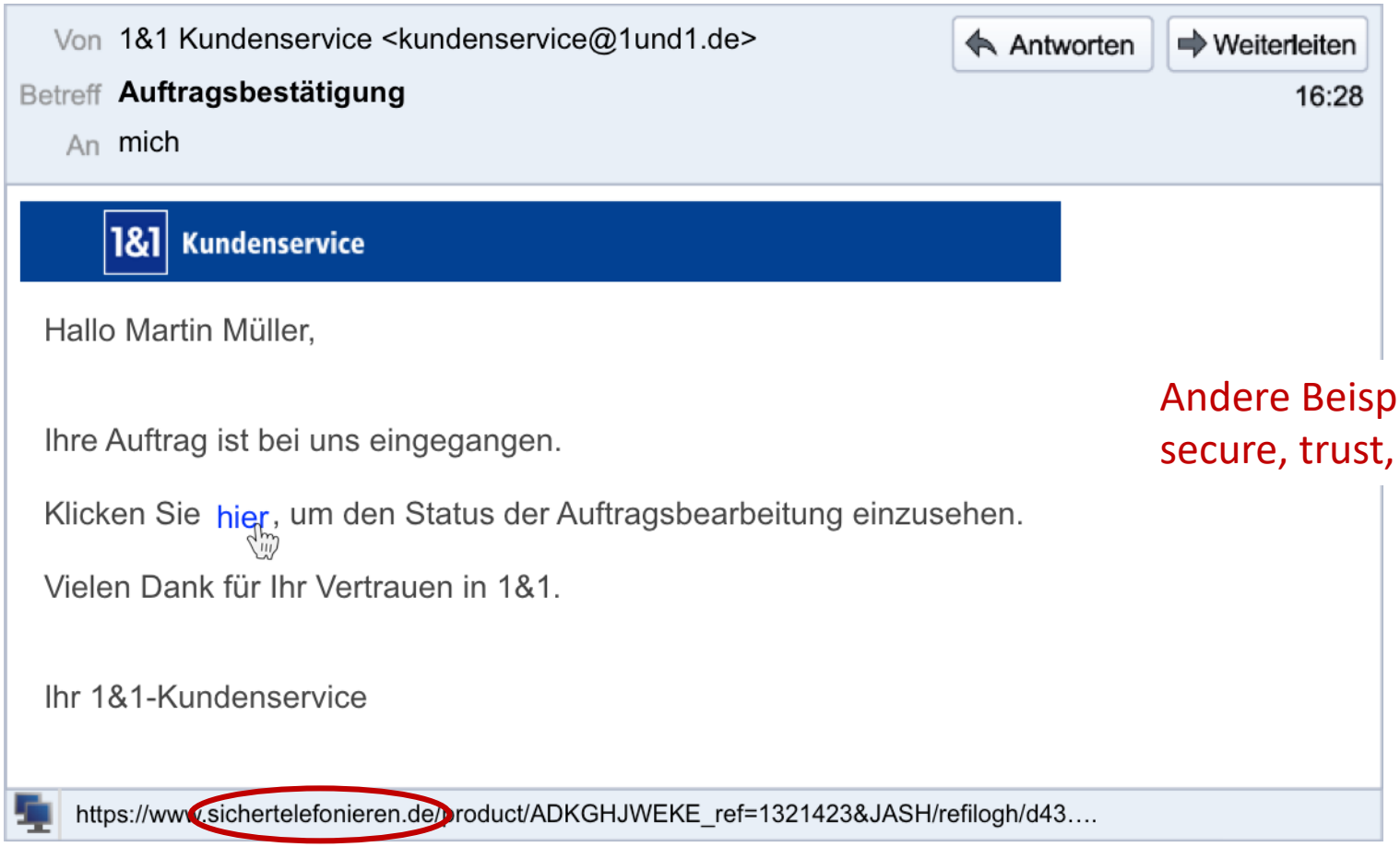
- http://www.nachrichten.spiegel.de
- http://www.computer.chip.de/testberichte
- http://www.suche.bild.de/bildersuche
- http://account.twitter.com/paypal.com
- http://www.msn.de.gutefrage.de/wetter.com
- https://www.billing.netflix.com/overview
- https://account.linkedin.com/personal
- https://finanzen.postbank.de/konto

3) Prüfe, ob der Wer-Bereich einen Bezug zum (vermeintl.) Absender/Inhalt hat.



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

Vorsicht Falle: Verwendung von vertrauensweckenden Begriffen



Andere Beispiele:
secure, trust, usw.

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

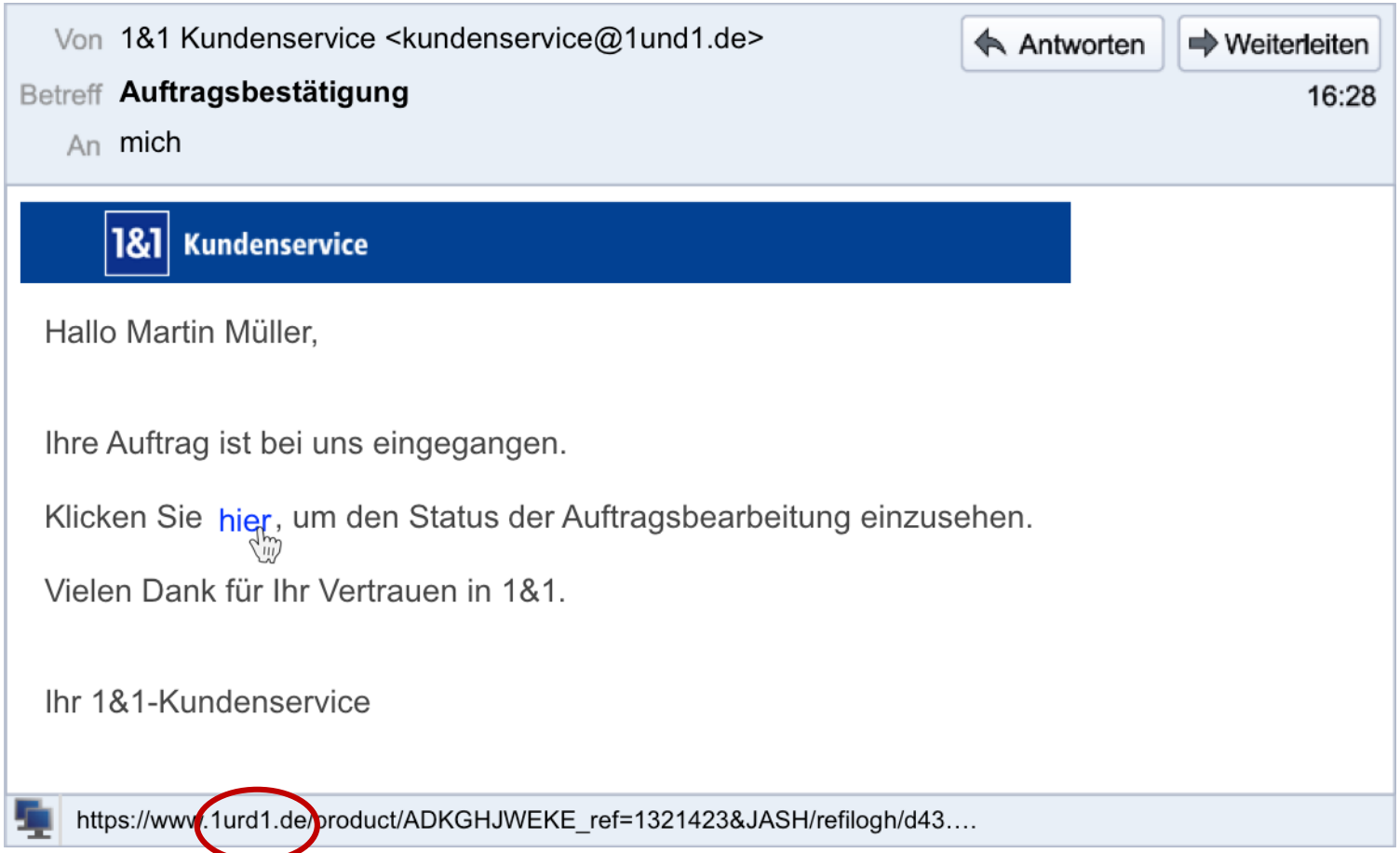
Es werden nur Kleinbuchstaben verwendet in der Webadresse

Vorsicht Falle: Wer-Bereich ist leicht verändert durch „Tippfehler“

- sprakasse.de statt sparkasse.de
- paketsrevice.de statt paketservice.de
- microsfot.de statt microsoft.de
- lufthanser.com statt lufthansa.de
- zallando.de statt zalando.de
- goo**gel**.de statt google.de

Vorsicht mit Aussprache im Englischen

Vorsicht Falle: 99,9% sieht plausibel aus



Übung: Ist der Wer-Bereich plausibel?

Sie möchten die Webseite von

Postbank

besuchen. Ist in diesem Fall der Wer-Bereich im folgenden Link plausibel:

http://www.banking.postbank.de/account

Übung: Ist der Wer-Bereich plausibel?

Sie möchten die Webseite von

LinkedIn

besuchen. Ist in diesem Fall der Wer-Bereich im folgenden Link plausibel:

https://register.herose.com/new 

Übung: Ist der Wer-Bereich plausibel?

Sie möchten die Webseite von

Bild

besuchen. Ist in diesem Fall der Wer-Bereich im folgenden Link plausibel:

http://www.suche.bild.de/bildersuche 

Übung: Ist der Wer-Bereich plausibel?

Sie möchten die Webseite von

Apple

besuchen. Ist in diesem Fall der Wer-Bereich im folgenden Link plausibel:

http://www.apple.com/de/iphone-6s/ 

Übung: Ist der Wer-Bereich plausibel?

Sie möchten die Webseite von

Arbeitsagentur

besuchen. Ist in diesem Fall der Wer-Bereich im folgenden Link plausibel:

http://www.jobsuche24.arbeitasgentur.de/überblick ✗

Übung: Ist der Wer-Bereich plausibel?

Sie möchten die Webseite von

Deezer

besuchen. Ist in diesem Fall der Wer-Bereich im folgenden Link plausibel:

http://deezer.com.uhrpav.com/bestmusic 

Übung: Ist der Wer-Bereich plausibel?

Sie möchten die Webseite von

T-Online

besuchen. Ist in diesem Fall der Wer-Bereich im folgenden Link plausibel:

http://tarife-und-produkte.t-online.de/internet-telefonie-telekom-tarife-mit-dsl-und-telefon-flatrate 

Übung: Ist der Wer-Bereich plausibel?

Sie möchten die Webseite von

eBay

besuchen. Ist in diesem Fall der Wer-Bereich im folgenden Link plausibel:

http://www.sicheres-shoppen24.de/ebay.de/einkaufen/32345 

Übung: Ist der Wer-Bereich plausibel?

Sie möchten die Webseite von

Google

besuchen. Ist in diesem Fall der Wer-Bereich im folgenden Link plausibel:

http://login.goog1e.com/myaccount ✗

Übung: Ist der Wer-Bereich plausibel?

Sie möchten die Webseite von

Leo Wörterbuch

besuchen. Ist in diesem Fall der Wer-Bereich im folgenden Link plausibel:

http://dict.leo.org/esde/index_de.html#/search=Hallo 

Übung: Ist der Wer-Bereich plausibel?

Sie möchten die Webseite von

Stackoverflow

besuchen. Ist in diesem Fall der Wer-Bereich im folgenden Link plausibel:

http://www.stackoverflovv.com/discussion32121 ✗

Was, wenn Sie sich nicht sicher sind, ob der Wer-Bereich korrekt ist?

- Beispiele
  - amazononline.de oder amazon-bestellen.de
  - amazon.at oder amazon.cw
- Problem
  - Anbieter nutzen verschiedene Wer-Bereiche
  - Unmöglich alle Wer-Bereiche zu kennen

→ Holen Sie weitere Informationen ein

- Bekannte Webadresse im Web-Browser eingeben
- Nach Wer-Bereich in einer Suchmaschine suchen (eines der ersten Ergebnisse?)
- Vergleich mit früheren Nachrichten
- Kontakt aufnehmen über bereits bekannte Kontaktmöglichkeiten

Vorsicht Fallen

- Verwendung von Bindestrichen: g-mail.com statt gmail.com
- Ergänzungen: amazon-sicher.com statt amazon.com
- Andere Endung: amazon.cw statt amazon.com

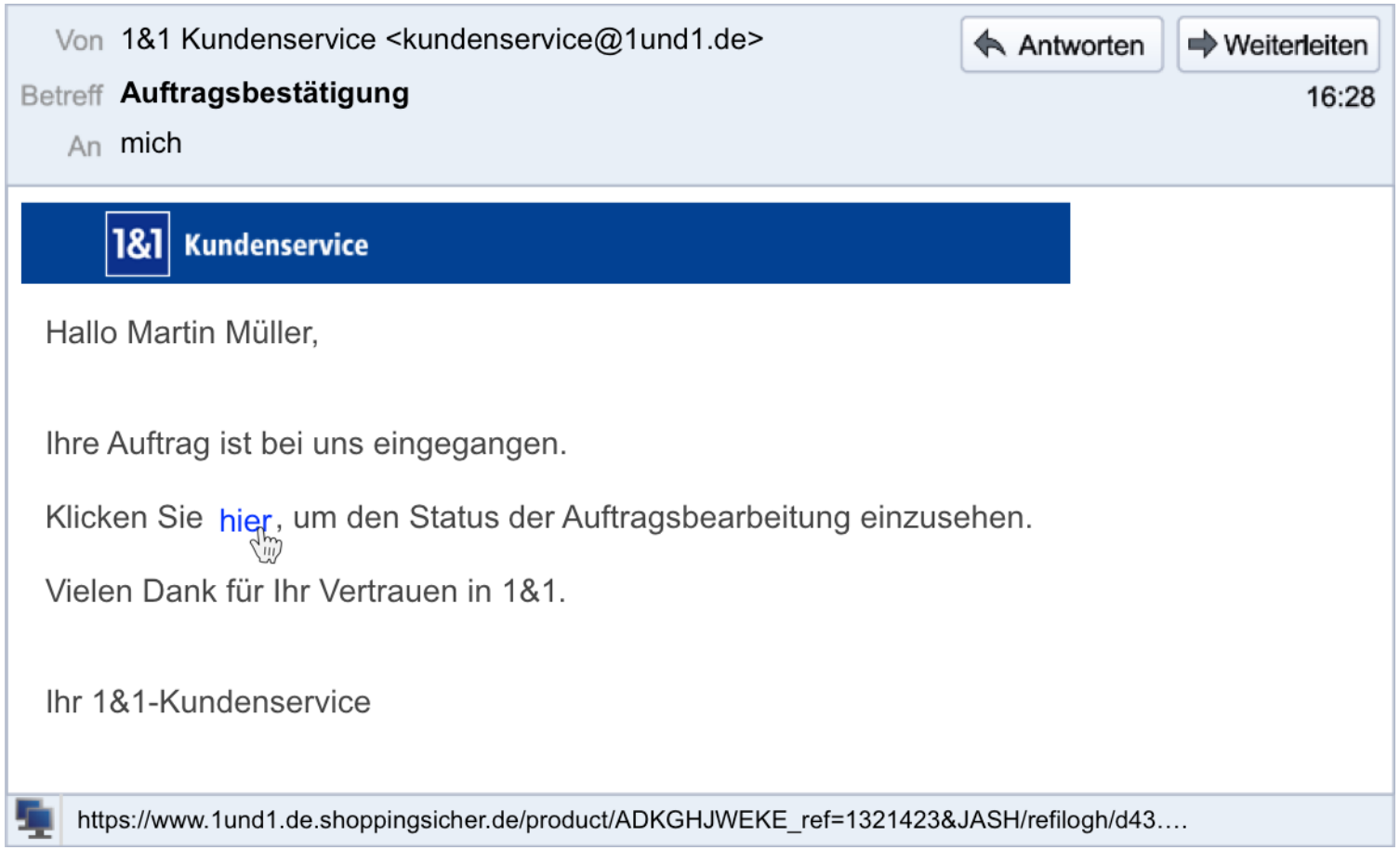
Weiterführende Informationen

https://www.secuso.org/schulung → Modul 3

- Tiny URLs und sonstige Weiterleitungen
- Tools zur Unterstützung bei der Erkennung
- …

Modul 3: Erkennung von plausiblen Nachrichten mit gefährlichen Links

Ist dies ein gefährlicher Link?



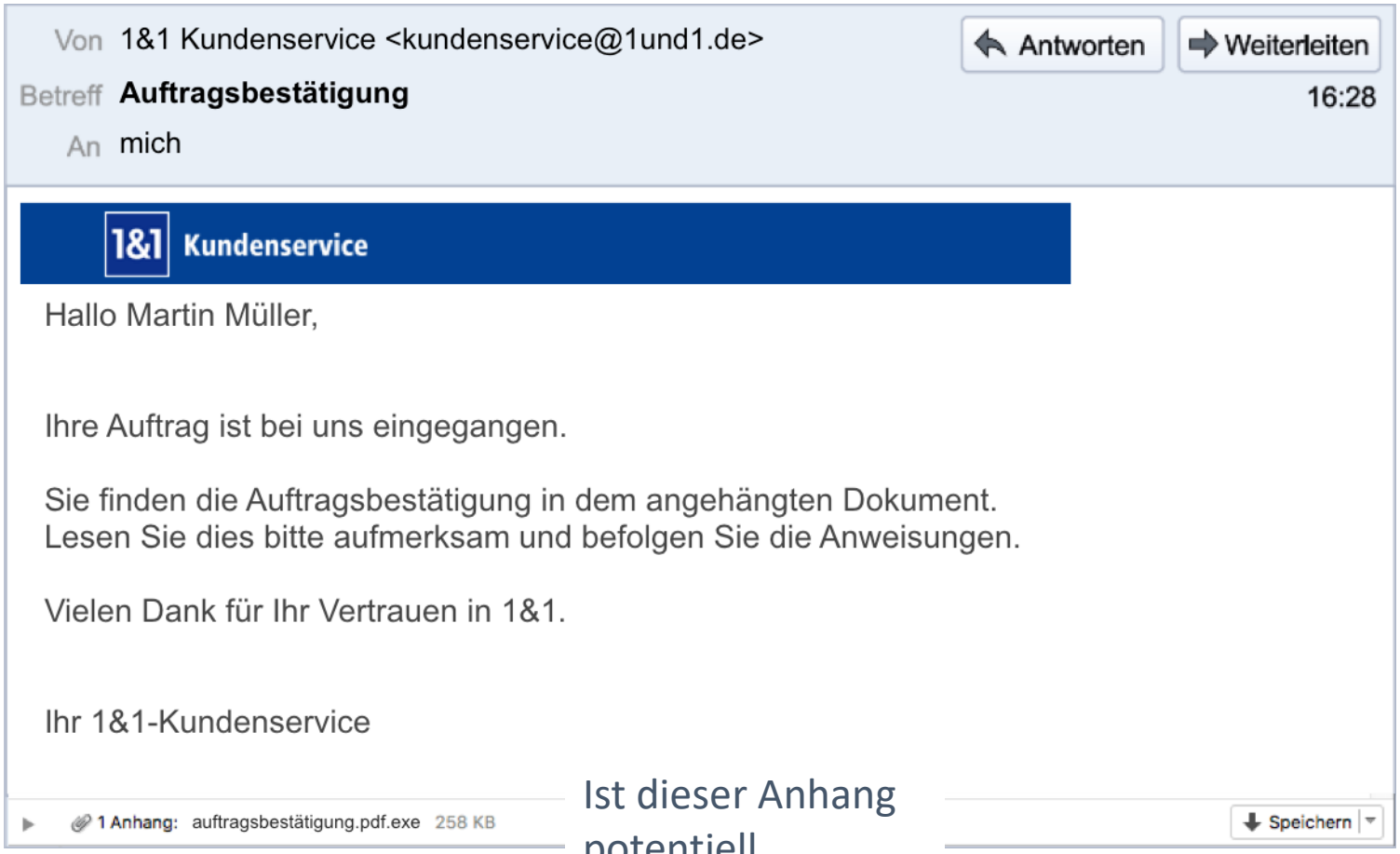
Modul 1: Einführung in das Thema Nachrichten mit gefährlichem Inhalt

Modul 2: Erkennung von unplausiblen Nachrichten mit gefährlichem Inhalt

Modul 3: Erkennung von plausiblen Nachrichten mit gefährlichen Links

Modul 4: Erkennung von plausiblen Nachrichten mit gefährlichen Anhängen

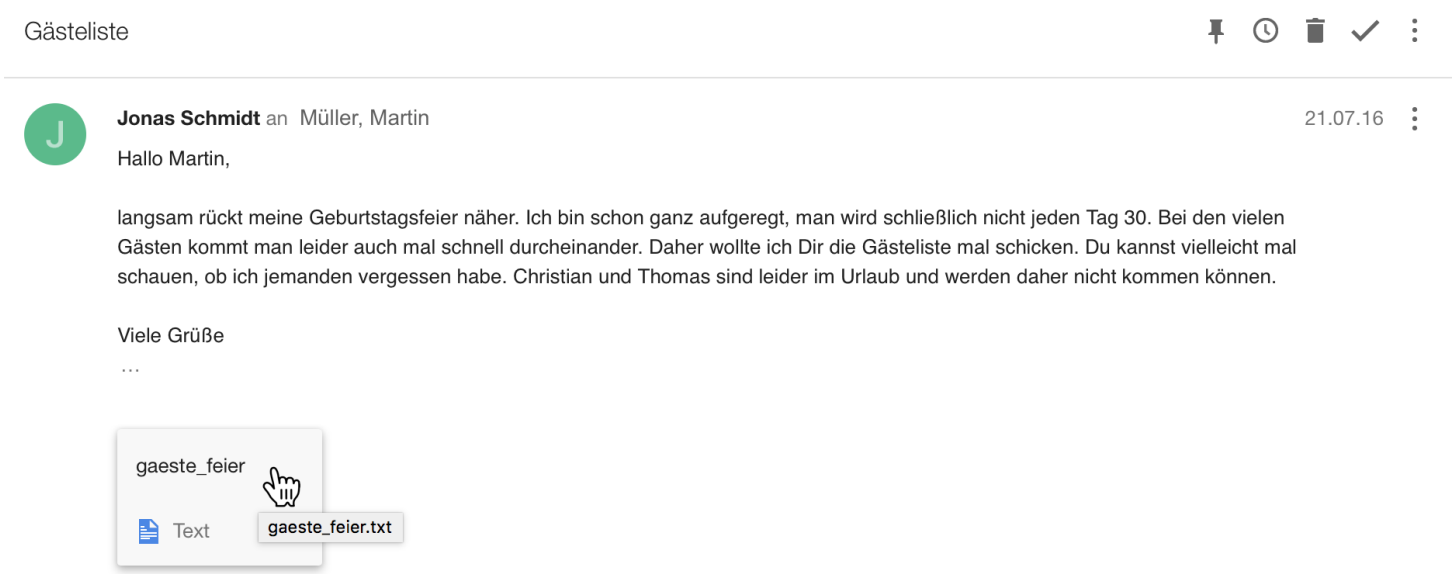
Modul 4: Erkennung von plausiblen Nachrichten mit gefährlichen Anhängen



Ist dieser Anhang potentiell gefährlich?

1) Lassen Sie sich den vollständigen Namen der Datei anzeigen.

Teilweise wird der Name nur teilweise angezeigt → Maus über Anhang bewegen



→ Ort der Anzeige hängt von Gerät, Software und Dienst ab

2) Identifizieren Sie das Format der Datei.

Bewerbung.pdf

Bewerbung.tu-darmstadt.pdf

3) Prüfen Sie, ob das Format auf einen potentiell gefährlichen Inhalt hinweist.

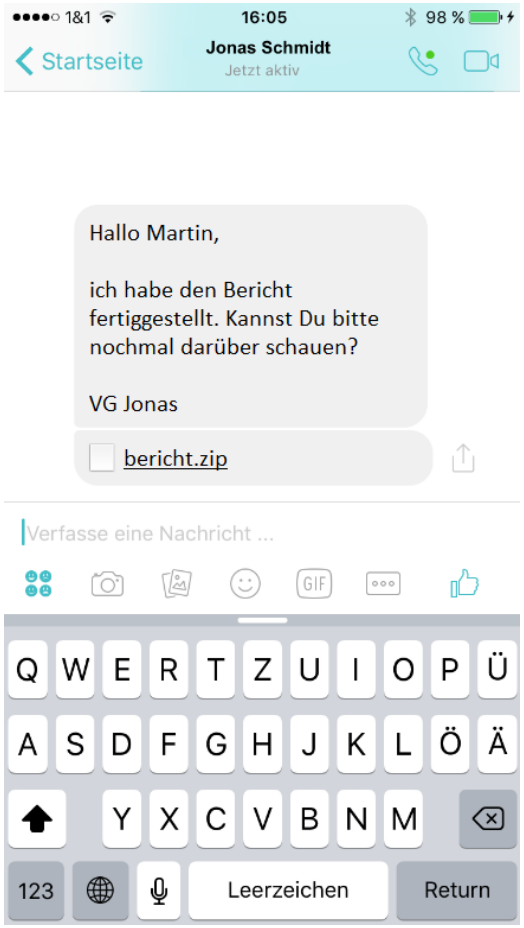
Weit verbreitete potentiell gefährliche Formate:

a) Ausführbare Dateiformate, z.B. .exe, .bat, .com, .cmd, .scr, .pif

b) Dateiformate, die sogenannte Makros auszuführen erlauben:
z.B. .doc, .docx, .ppt, .pptx, .xls, .xlsx

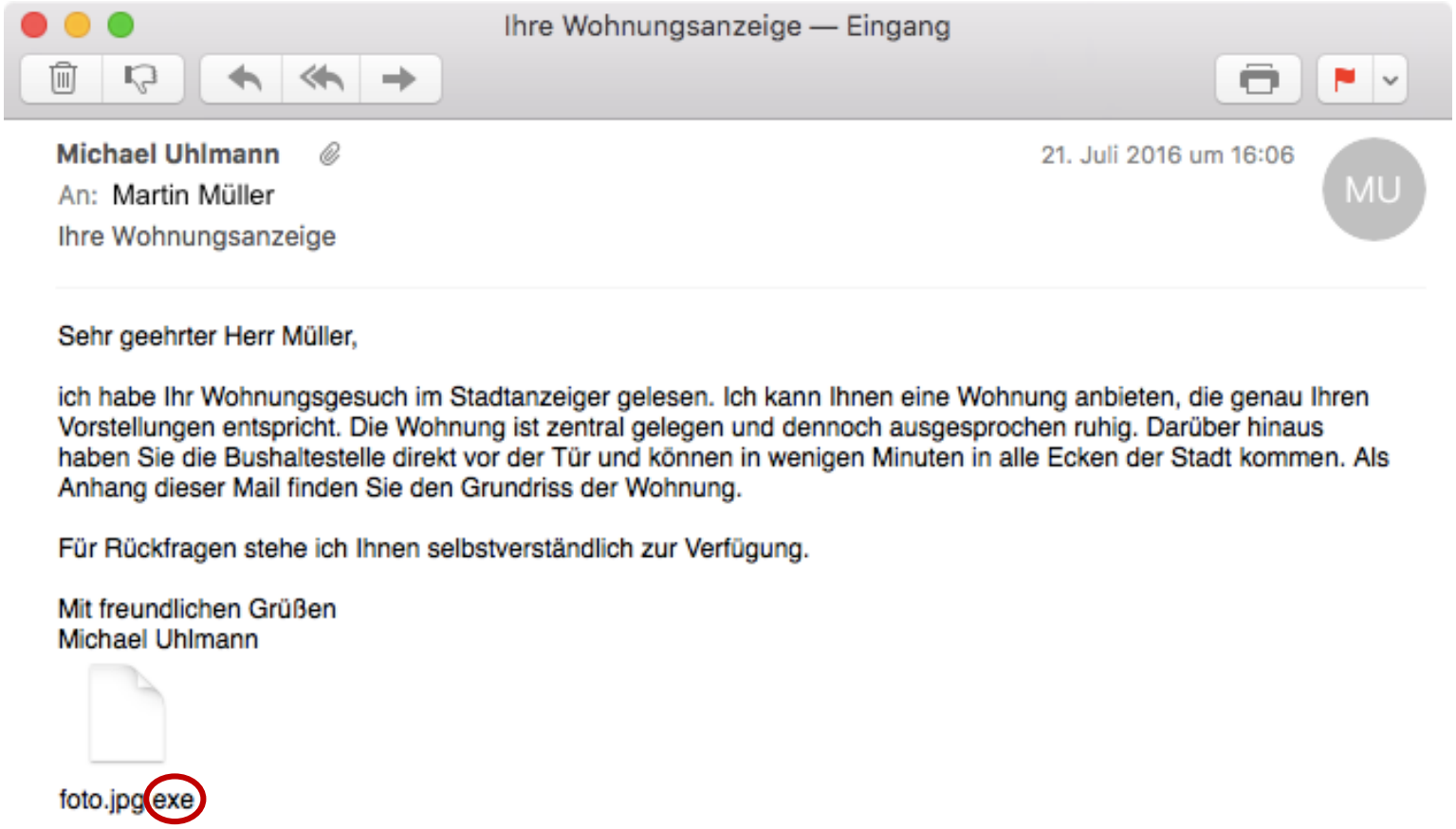
Unbekannte Formate = potentiell gefährlich

Vorsicht Falle: gefährliche Inhalte werden „gepackt“

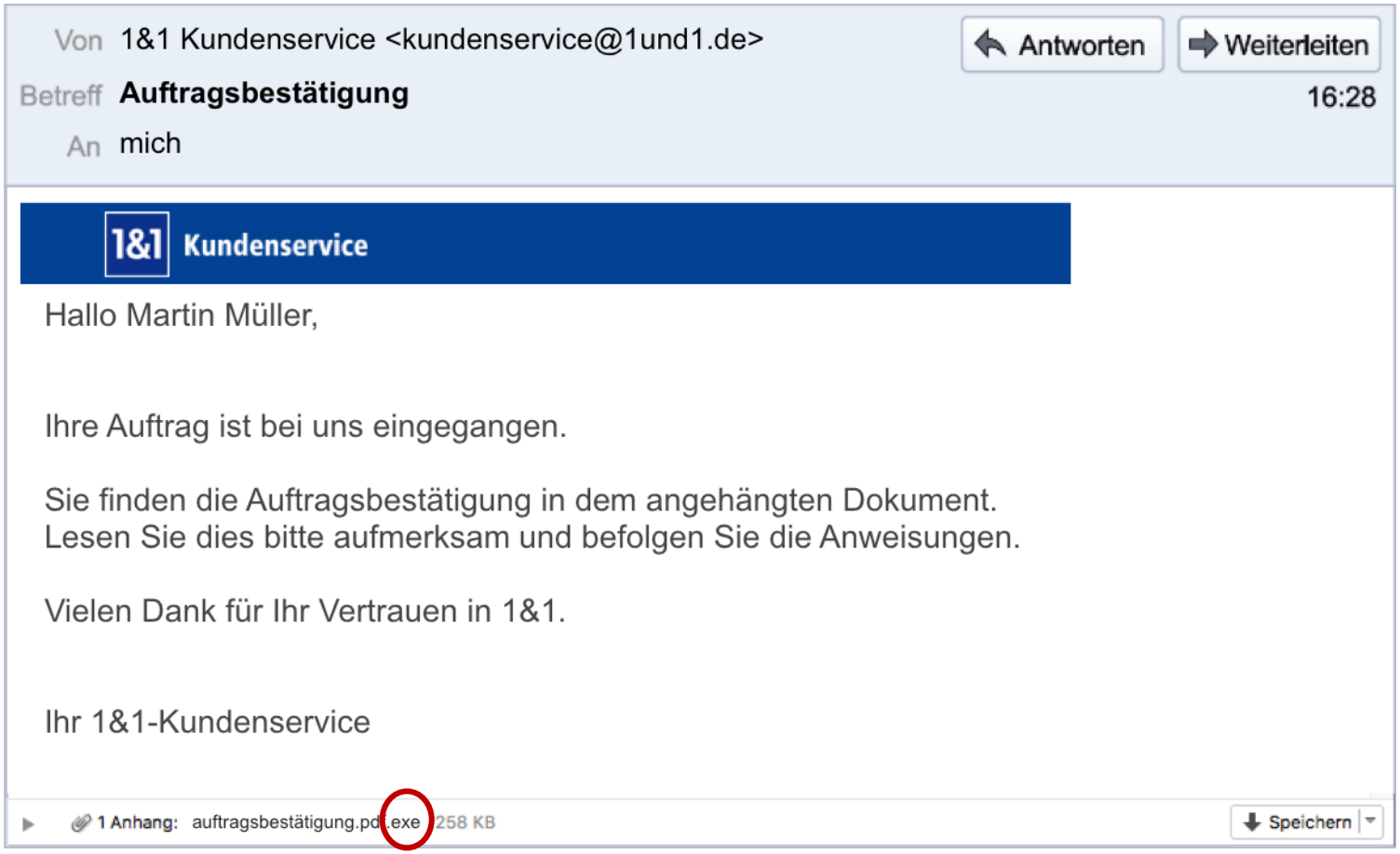


.zip und .rar wie gefährliche Formate behandeln

Vorsicht Falle: Doppel-Endung



Vorsicht Falle: 99% sieht plausibel aus



4) Dateien mit potentiell gefährlichem Inhalt löschen, wenn sie nicht genau in dieser Form erwartet werden.

- Wurde Ihnen dieser Anhang in dieser Form zuvor von dem Absender persönlich angekündigt?

- Ist die Nachricht digital signiert, so dass die Identität des Absenders als gesichert gelten kann?

Was, wenn Sie sich nicht sicher sind, ob die Nachricht so angekündigt wurde?

→ Holen Sie weitere Informationen ein

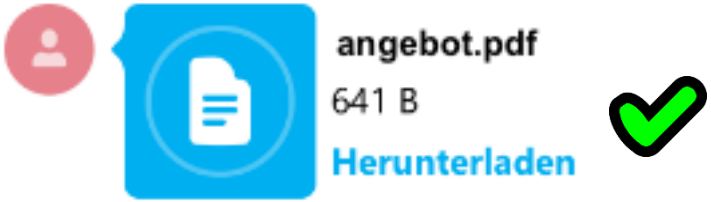
- Kontakt über bekannte Kontaktmöglichkeiten aufnehmen
- Absender bitten, Ihnen den Anhang in einem anderen Format zu schicken
- Suchen Sie nach dem Inhalt/Absender in einer Suchmaschine: Wird er bereits als betrügerisch angezeigt?

Übung: Ist der Anhang potentiell gefährlich?

Sie haben eine Nachricht mit dem folgenden Anhang erhalten:

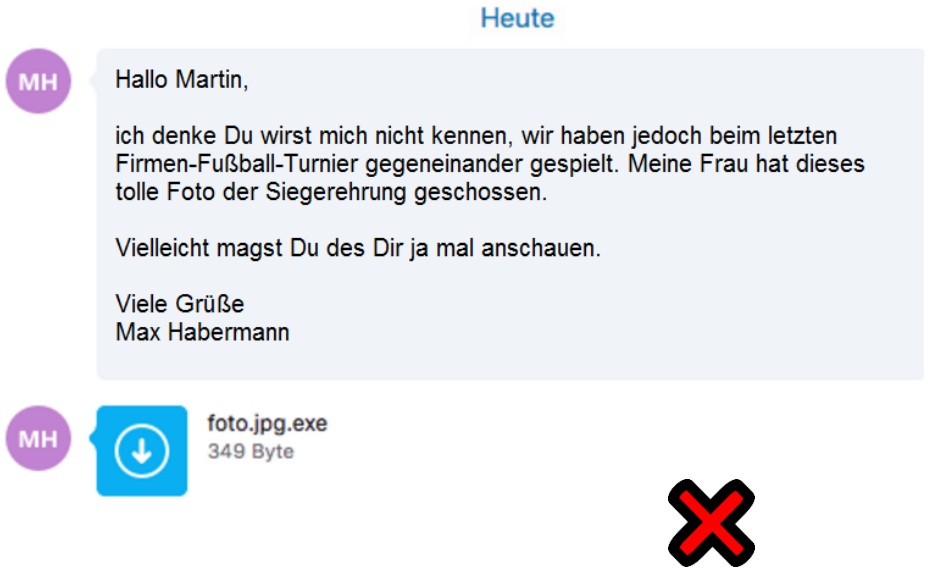
Übung: Ist der Anhang potentiell gefährlich?

Sie haben eine Nachricht mit dem folgenden Anhang erhalten:



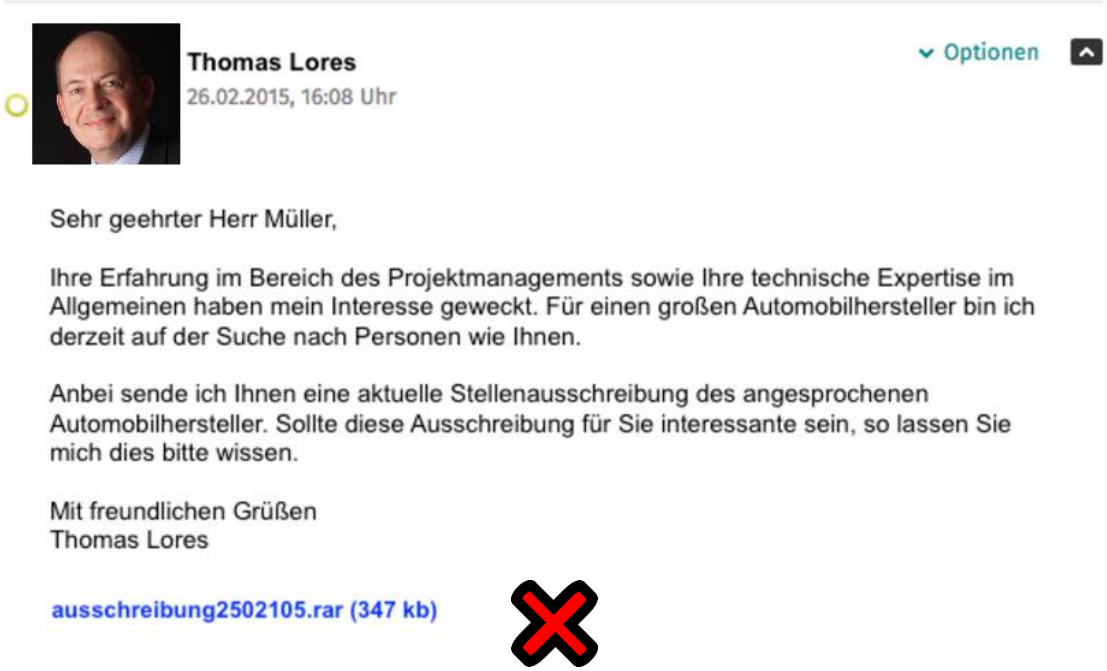
Übung: Ist der Anhang potentiell gefährlich?

Sie haben die folgende Nachricht erhalten:



Übung: Ist der Anhang potentiell gefährlich?

Sie haben die folgende Nachricht erhalten:



Übung: Ist der Anhang potentiell gefährlich?

Sie haben die folgende Nachricht erhalten:

Weiterführende Informationen

https://www.secuso.org/schulung → Modul 4

- Automatisches Öffnen von Dateianhängen unterbinden
- Doppelendungen durch Verschlüsselungssoftware
- Weitere Links zu Übersicht über Dateiformate
- …

Viel Erfolg beim Erkennen betrügerischer Nachrichten!

Modul 1: Einführung in das Thema Nachrichten mit gefährlichem Inhalt

Modul 2: Erkennung von unplausiblen Nachrichten mit gefährlichem Inhalt

Modul 3: Erkennung von plausiblen Nachrichten mit gefährlichen Links

Modul 4: Erkennung von plausiblen Nachrichten mit gefährlichen Anhängen

Abschließende Informationen

- Ausführliche Schulungsunterlagen, Motivationsposter und Quizze: https://www.secuso.informatik.tu-darmstadt.de/de/secuso/forschung/ergebnisse/erkennung-betruegerischer-nachrichten/
- Spiele-Apps zur Erkennung betrügerischer Links: https://www.secuso.informatik.tu-darmstadt.de/de/secuso/forschung/ergebnisse/nophish/
- Video auf Youtube: https://youtu.be/4xIU1lPJs_4
- Tools zur Unterstützung der Erkennung betrügerischer Nachrichten:
  - TORPEDO: https://www.secuso.informatik.tu-darmstadt.de/de/secuso/forschung/ergebnisse/torpedo/
  - PassSec+: https://www.secuso.informatik.tu-darmstadt.de/de/secuso/forschung/ergebnisse/passsec/

Kurzlinks (Tiny-URLs)

- Kurzlinks (Tiny-URLs) erleichtern das Merken und Eintippen von Webadressen...
- ... aber sie verschleiern das Ziel des Links. Hinter dem Kurzlink

http://tinyurl.com/hdb8j3c

steht eigentlich die Webseite

https://www.secuso.informatik.tu-darmstadt.de/en/secuso-home/

- Dienste zu Rate ziehen, die echte Webadressen hinter Kurzlinks ermitteln, z.B.:

http://unshorten.me/

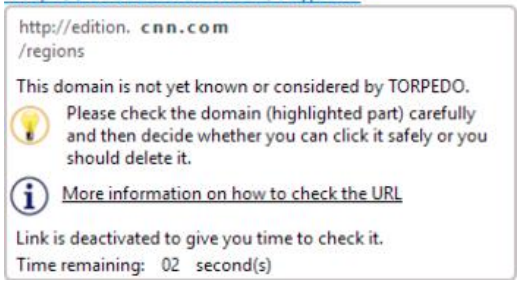
TORPEDO

TORPEDO
TOoltip-poweRed Phishing Email DetectiOn

- Thunderbird Add-On
- Hebt den Wer-Bereich von Links in E-Mails hervor
- Hinweise über die Vertrauenswürdigkeit des Wer-Bereichs auf Grundlage von
  - Expertenmeinungen
  - Nutzerhistorie

https://de.wikipedia.org/wiki/Technische_Universit%C3%A4t_Darmstadt

http://edition.cnn.com/regions



https://www.washingtonpost.com/sports/

- Freiverfügbar unter:

  https://www.secuso.org/torpedo