Universität Augsburg
Rechenzentrum

Phishing
Wie kann ich mich schützen?

Wie erkenne ich mögliche Phishing-Mails?

Wie erkenne ich gefährliche Links in Phishing-Mails?

Informationssicherheit@uni-augsburg.de, 24. Okt. 2022

Was ist Phishing?

Angreifer versuchen über E-Mails sensible Daten, wie beispielweise Ihre Anmeldedaten zu bekommen -
oder Sie zu bestimmten Handlungen zu bewegen, wie z.B. einer Überweisung oder Bestellung.

Phishing E-Mails sehen optisch oft so aus, als ob sie von bekannten Personen, Firmen oder Banken gesendet würden.

Phishing ist Teil des sogenannten „Social Engineering“, bei dem es darum geht, Menschen geschickt zu manipulieren.

Manipulation durch Social Engineering

Mehr als 80% aller erfolgreichen Angriffe nutzen Social Engineering. Hacker versuchen beim Social Engineering durch andere Personen unberechtigten Zugriff auf Computersysteme und wichtigen Informationen zu erlangen. Menschliche Eigenschaften werden geschickt ausgenutzt, wie …

- Angst – z.B. durch die Drohung, dass Daten unwiderruflich gelöscht werden.
- Zeitdruck – z.B. soll eine angeblich wichtige Überweisung schnell durchgeführt werden, wobei das Geld beim Angreifer landet.
- Hilfsbereitschaft – z.B. eine nett gemeinte Gefälligkeit, wie eine kleine Bestellung, ein Klick auf eine scheinbare Bewertung, …
- Vertrauen zu Personen, die man kennt – z.B. geben sich Täter als Freunde oder Bekannte aus.
- Respekt gegenüber Autoritätspersonen – z.B. gegenüber dem Chef/wichtigen Personen, was dazu führen kann, dass man bei E-Mails mit seltsamen Inhalten nicht nachfragt sondern es einfach tut.

Oft auch in Kombination führt das zu einem schnellen Klick, der Informationen preisgibt, Türen zu internen Verfahren öffnet, Bestellungen, Bezahlungen oder Verschlüsselung wichtiger Daten oder Schlimmeres auslöst.

Social Engineering missbraucht gute menschliche Eigenschaften

Was können Sie tun?
Seien Sie aufmerksam und im gesunden Maß skeptisch. Im Folgenden lernen Sie, wie sie der Gefahr durch Phishing erfolgreich begegnen.

PHISHING-MAILS ERKENNEN

Phishing-Mails – werden immer besser

Bookling.com

Buchungsnummer: **1446303004**
PIN-Code: **6497**

Vielen Dank Thomas [redacted]

Die Buchung in Berlin wurde bestätigt

- Das Hotel Novut Select Hotel Berlin Mitte wurde gebucht am 2018/05/10 09:51:51
- Ihre Zahlung geht direkt an das Unternehmen. Die Immobilie Novut Select Hotel Berlin kümmert sich um alle Zahlungen, siehe unten für mehr Informationen darüber
- Mit nur ein paar Klicks können Sie Ihre Buchung ändern oder eine Frage über die Unterkunft stellen

Ändern Sie Ihre Buchungen einfach online, indem Sie ein Passwort erstellen.

Buchung ändern | Bestätigung auf Handy speichern

Novut Select Hotel Berlin

Charlotannstr. 56, Mitte, Berlin, 10117, Germany - Anfahrtsroute ansehen
Telefon: +4930221260500
E-Mail an die Unterkunft senden

Klicken Sie hier, um die Buchungsbestätigung zu drucken

Ihre Buchung	1 Nacht, 1 Zimmer
Anreise	2018/05/10 09:51:51
Abreise	2018/05/10 11:31:51

Buchung stornieren

Original oder Fälschung?

Welche Buchungsbestätigung ist die richtige?

Booking.com

Buchungsnummer: **1571703239**
PIN-Code: **1329**

Vielen Dank, Thomas!

Ihre Buchung in Budapest ist bestätigt.

- Die Unterkunft **Estilo Fashion Hotel Budapest** erwartet Sie am **28. Januar**
- Sie zahlen direkt an die Unterkunft. Die Unterkunft Estilo Fashion Hotel Budapest kümmert sich um alle Zahlungen, weiter unten finden Sie hierzu weitere Informationen
- Mit nur wenigen Klicks können Sie Änderungen an Ihrer Buchung vornehmen oder der Unterkunft eine Frage stellen

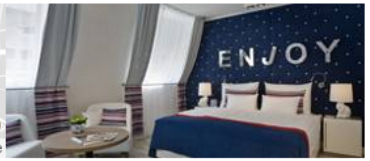
[illegible]ung ändern | Ihre Buchung in der App verwalten

Estilo Fashion Hotel Budapest .genius 10% Schnäppchen

Geschäftsreise

Váci utca 83., 05. Belváros - Lipótváros, Budapest, 1056, Ungarn -

Telefon: +3617997170
E-Mail an Unterkunft



Hier geht's zur Druckversion

Ihre Buchung	3 Nächte, 3 Zimmer
Ihre Gruppe	3 Erwachsene
Anreise	Sonntag, 28. Januar 2018 (ab 14:00)
Abreise	Mittwoch, 31. Januar 2018 (bis 12:00)

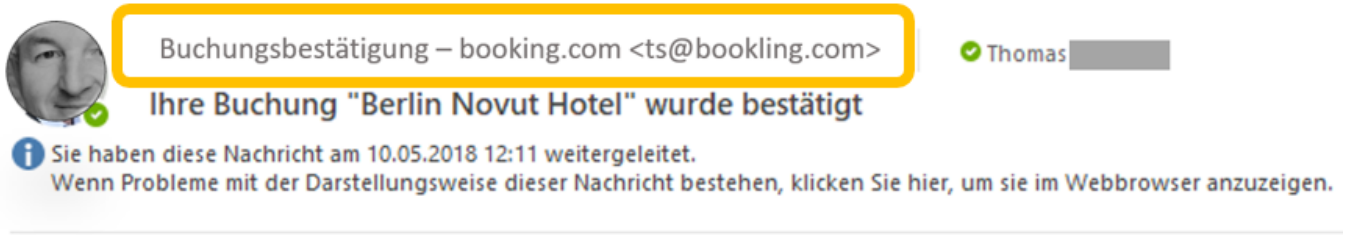
Woran haben Sie das Original erkannt? Wie erkennen Sie Phishing?

Prüfen Sie den Absender!

- Passt der Absender zum Inhalt?
- Kenne ich den Absender?

Prüfen Sie den Inhalt des Mails!

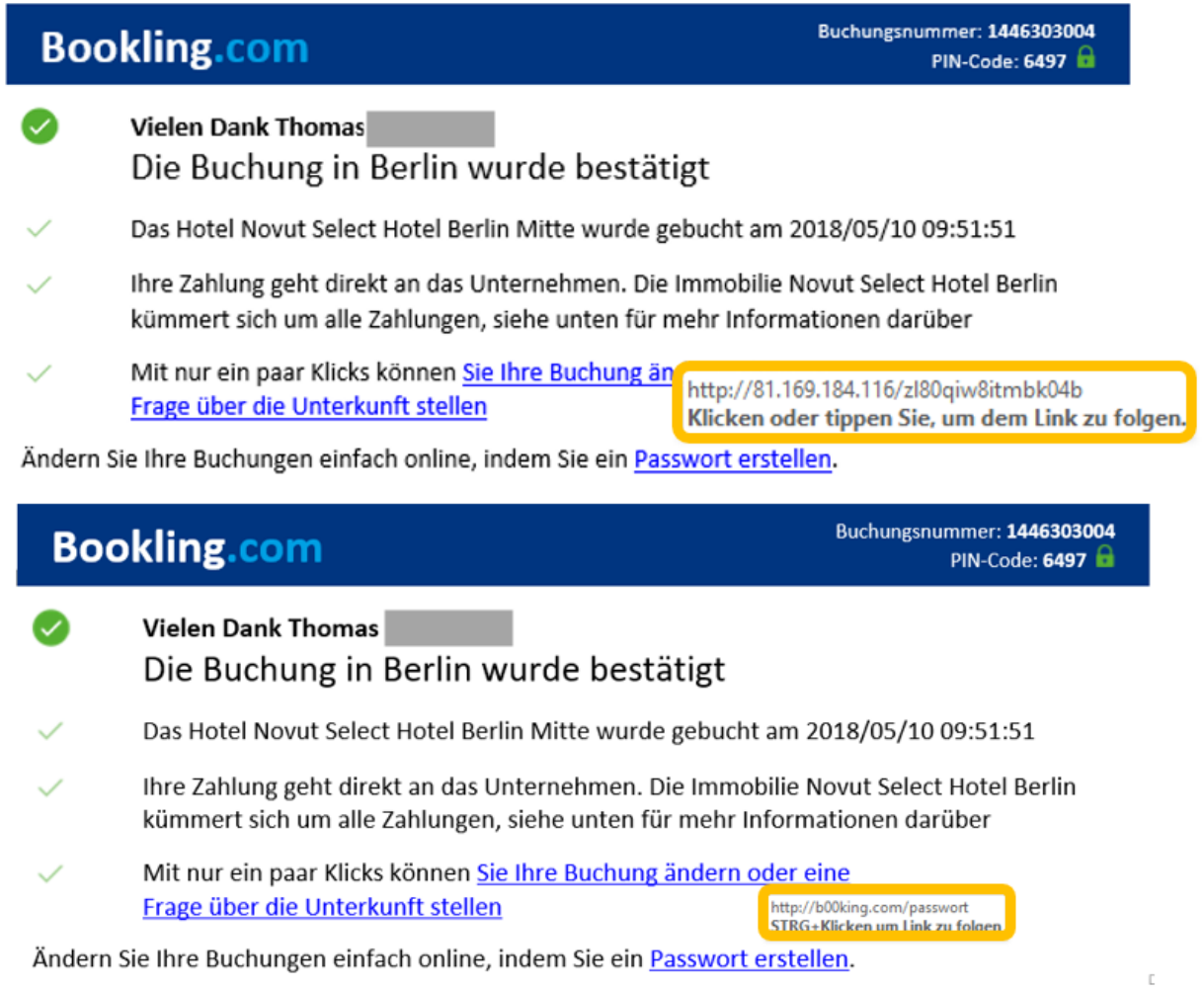
- Design
- Anrede
- Sprache (Rechtschreibfehler, Grammatik)
- Fremdsprache
- Androhung einer Strafe
- Großes Versprechen
- Zeitdruck
- Übermitteln von sensiblen Informationen



Wie erkenne ich die Phishing-Mails?

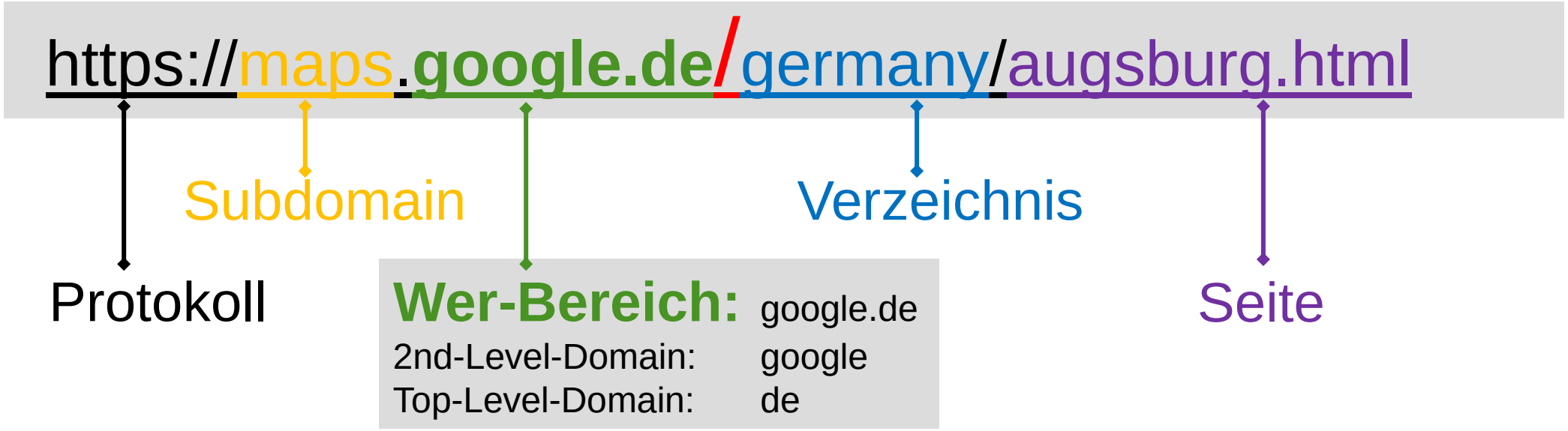
Prüfen Sie die Links, bevor Sie diese anklicken. Dies können Sie tun, indem Sie mit der Maus über auf den entsprechenden Eintrag gehen aber nicht klicken.

- Bei IP-Adressen zu Beginn der URL (wie z.B. https://81.169.184.116) sollten Sie stets kritisch sein. Im Zweifelsfall nicht klicken.
- Analysieren Sie den Wer-Bereich der Web-Adresse des Links aufmerksam. Kritisch sind
  - zusätzliche oder geänderte Buchstaben,
  - zusätzliche Bindestriche,
  - erweiterter Wer-Bereich,
  - seltsame Zeichen, z.B. in einer fremden Sprache (wie kyrillische oder griechische Buchstaben)



Prüfen Sie jede URL bevor Sie klicken

Jeder Aufruf im Browser geschieht über einen sogenannten URL. Hier ein Beispiel.



Entscheidend ist immer der **Wer-Bereich** (vor dem ersten „/“)
Dieser sollte für Sie stimmig und nicht verdächtig sein.
Im Verdachtsfall: NICHT anklicken!

Schätzen Sie selbst ein: Welche URLs sollten Verdacht erregen?

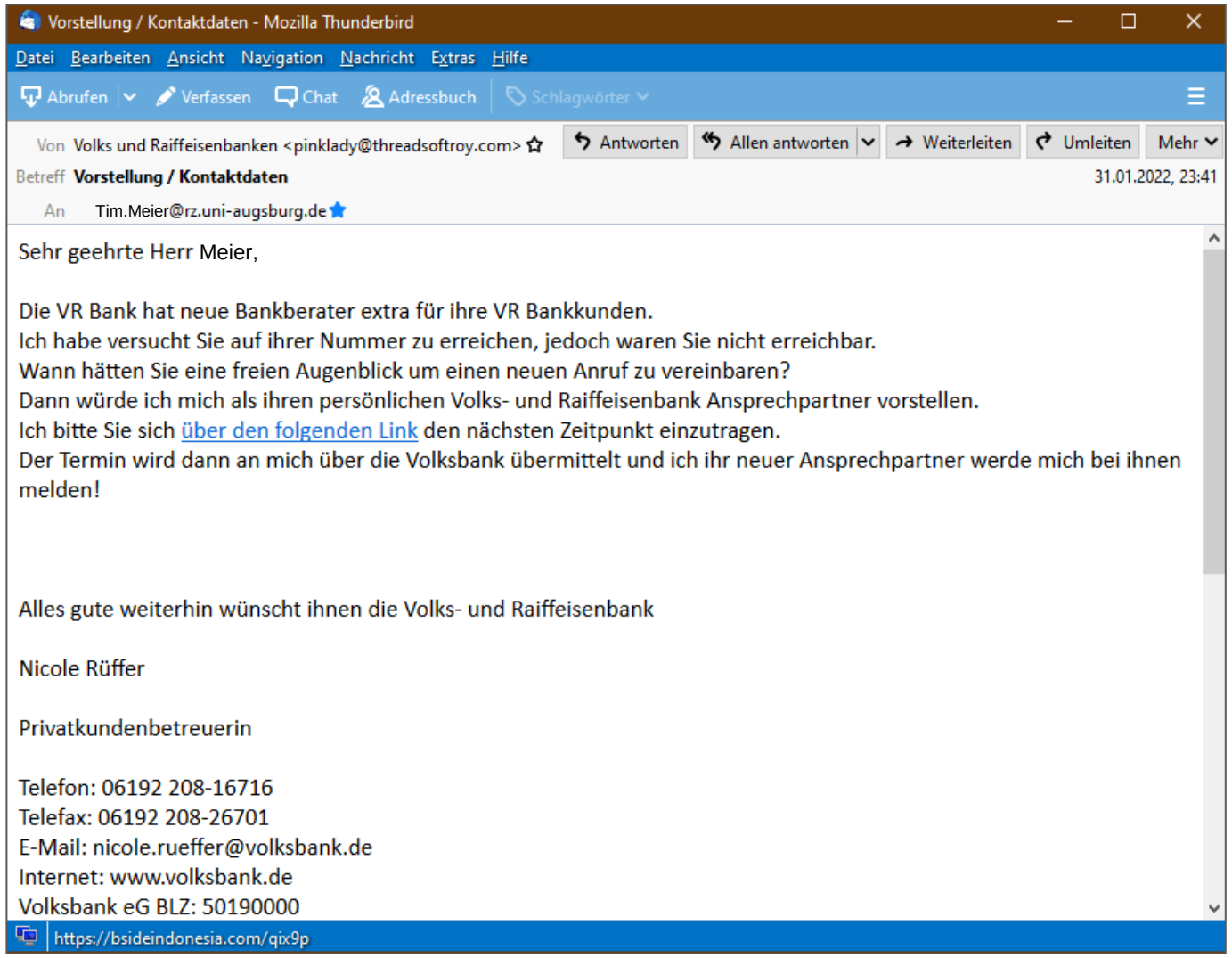
URL		Verdächtig - Warum?
https:// uni--augsburg.de		
www.uni-augsburg.de		
https://216.58.208.35		
https://wettter.de		
http://UNI-AUGSBURG.DE		
https://INSTAGRAM.COM.HACKMICH.VU		
https://stadtsparkasse.ru		
https://amazon.co.uk		
https://baHn.de		
https://booκing.com		
https://weber3.com/amazon.de		
https://uni_augsburg.de		
https://G00GLE.com		

Schätzen Sie selbst ein: Welche URLs sollten Verdacht erregen?

URL		Verdächtig - Warum?
https:// uni--augsburg.de	V	Doppelter Bindestrich im Wer-Bereich
www.uni-augsburg.de		Wenn das Protokoll fehlt macht das nichts
https://216.58.208.35	V	IP Adressen statt einem Wer-Bereich sollten immer ihren Verdacht erregen
https://wettter.de	V	wettter mit 3 t im Wer-Bereich
http://UNI-AUGSBURG.DE		Gross-Schreibung stört nicht
https://INSTAGRAMM.COM.HACKMICH.VU	V	Instagram ist falsch geschrieben, spätestens HACKMICH.VU sollte Sie skeptisch machen
https://stadtsparkasse.ru	V	.ru russische Stadtsparkasse?
https://amazon.co.uk		das wiederum ist eine Ausnahme von der Regel co.uk gibt es wirklich und ist durchaus plausibel. Aber wenn Sie skeptisch sind, besser nicht klicken!
https://baHn.de		Das große H sollte Sie nicht mehr stören
https://booкing.com	V	Achtung, hier hat sich ein kyrillischer Buchstabe versteckt к statt k
https://weber3.com/amazon.de	V	Wenn Sie zu weber3.com wollen ist das okay, danach amazon.de ist komisch
https://uni_augsburg.de	V	uni_ ist nicht uni-
https://G00GLE.com	V	00 wie WC – steht bestimmt nicht für GOOGLE

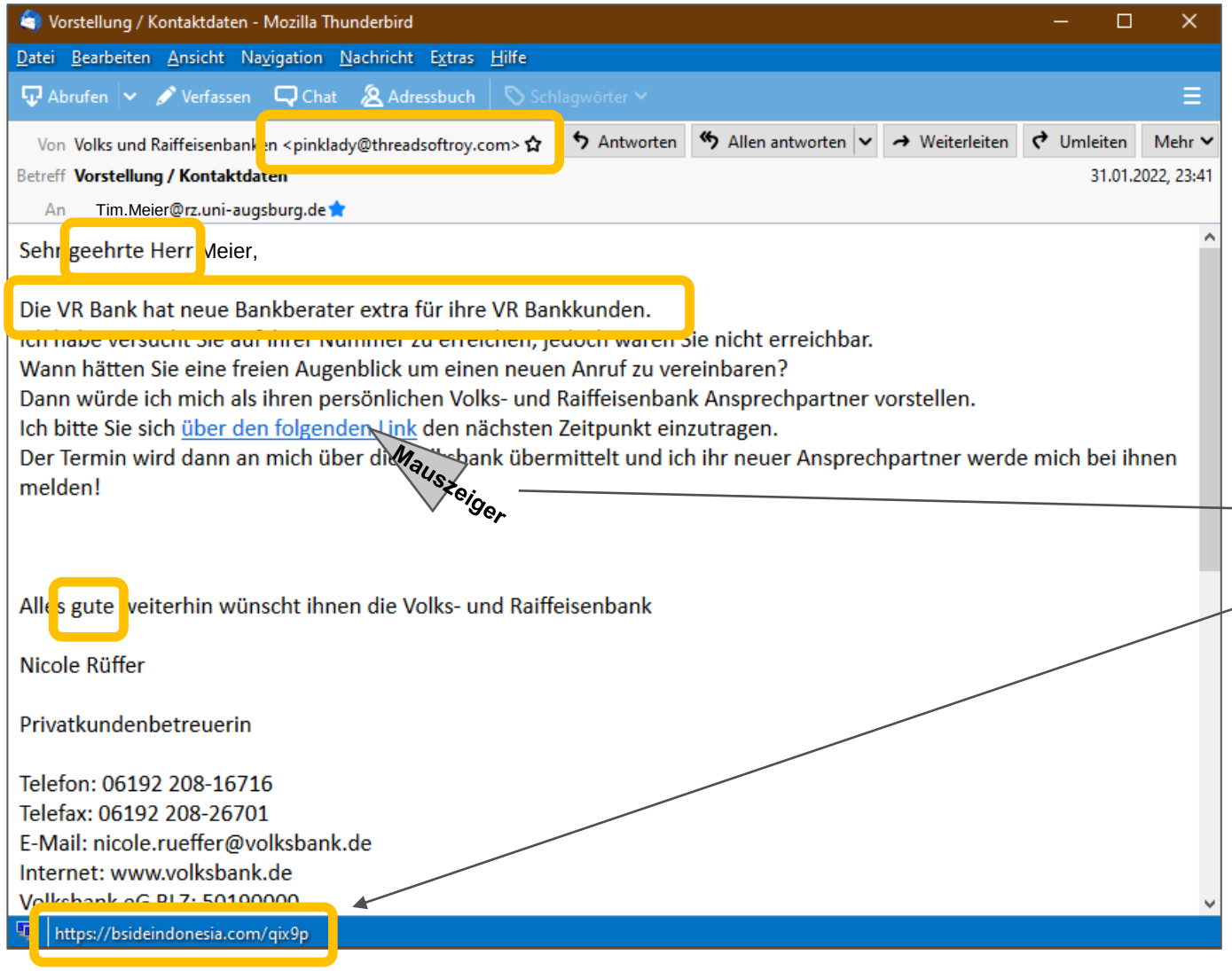
TESTEN IHR WISSEB AN AKTUELLEN PHISHINGMAILS

Was macht Sie stutzig?



1. Begutachten Sie folgende E-Mail kritisch.
2. Beurteilen Sie, ob es Phishing sein könnte.
3. Markieren Sie Stellen, die Sie skeptisch machten.

Was macht Sie stutzig?

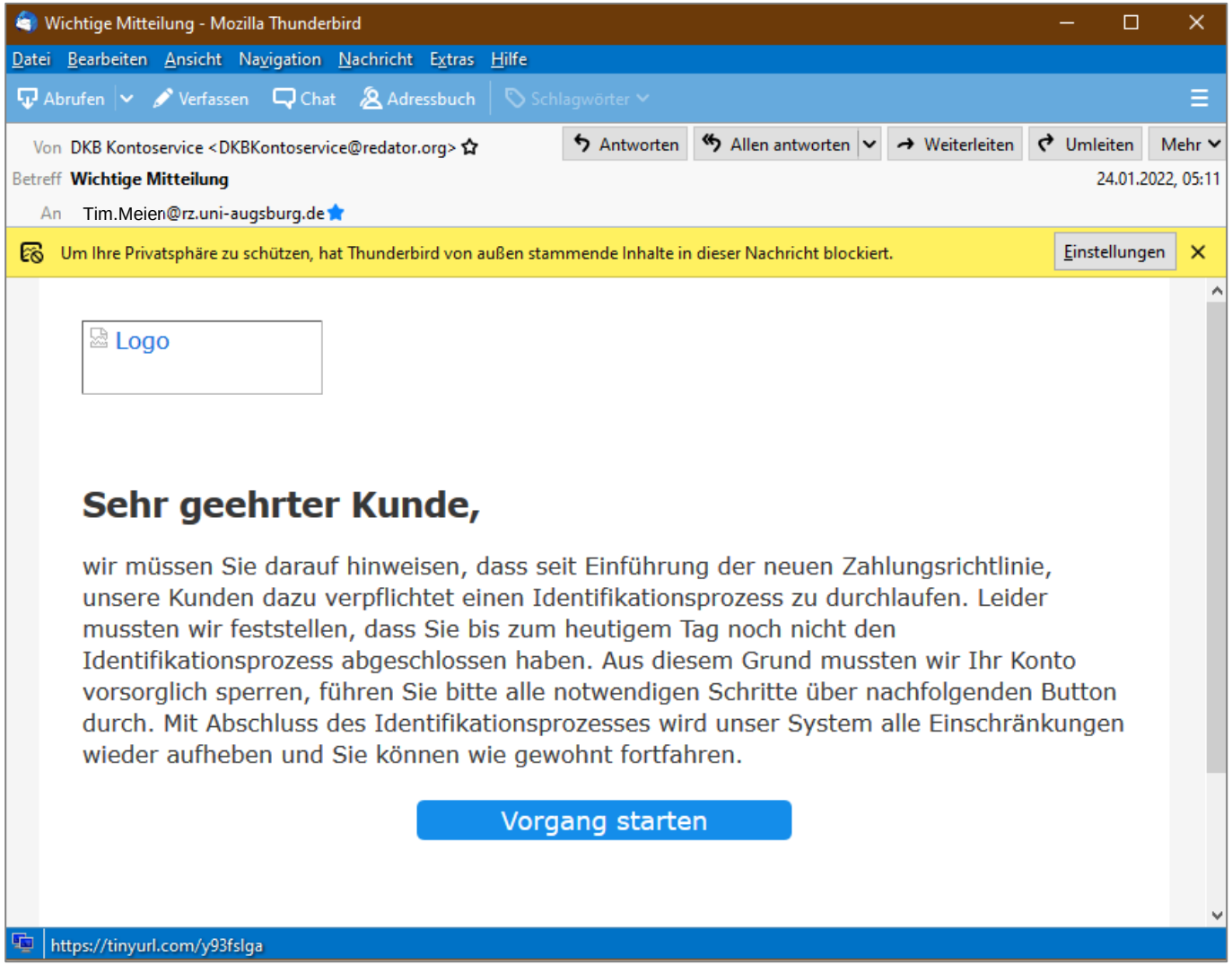


Keine Email-Adresse der Volks- und RaiBa

Rechtschreibfehler und schlechtes Deutsch

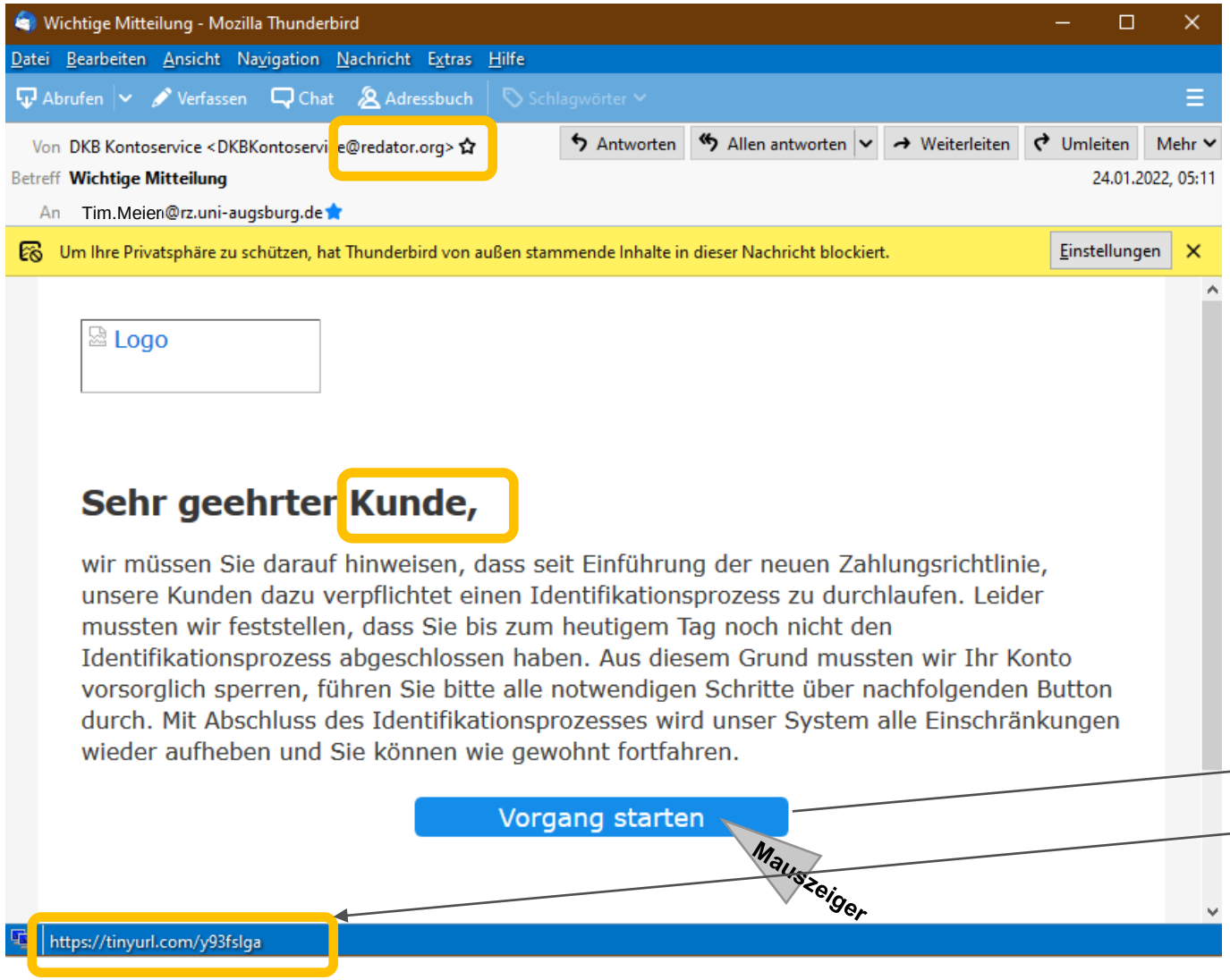
Hoover mit der Maus zeigt einen verdächtigen Link

Was macht Sie stutzig?



1. Begutachten Sie folgende E-Mail kritisch.
2. Beurteilen Sie, ob es Phishing sein könnte.
3. Markieren Sie Stellen, die Sie skeptisch machten.

Was macht Sie stutzig?

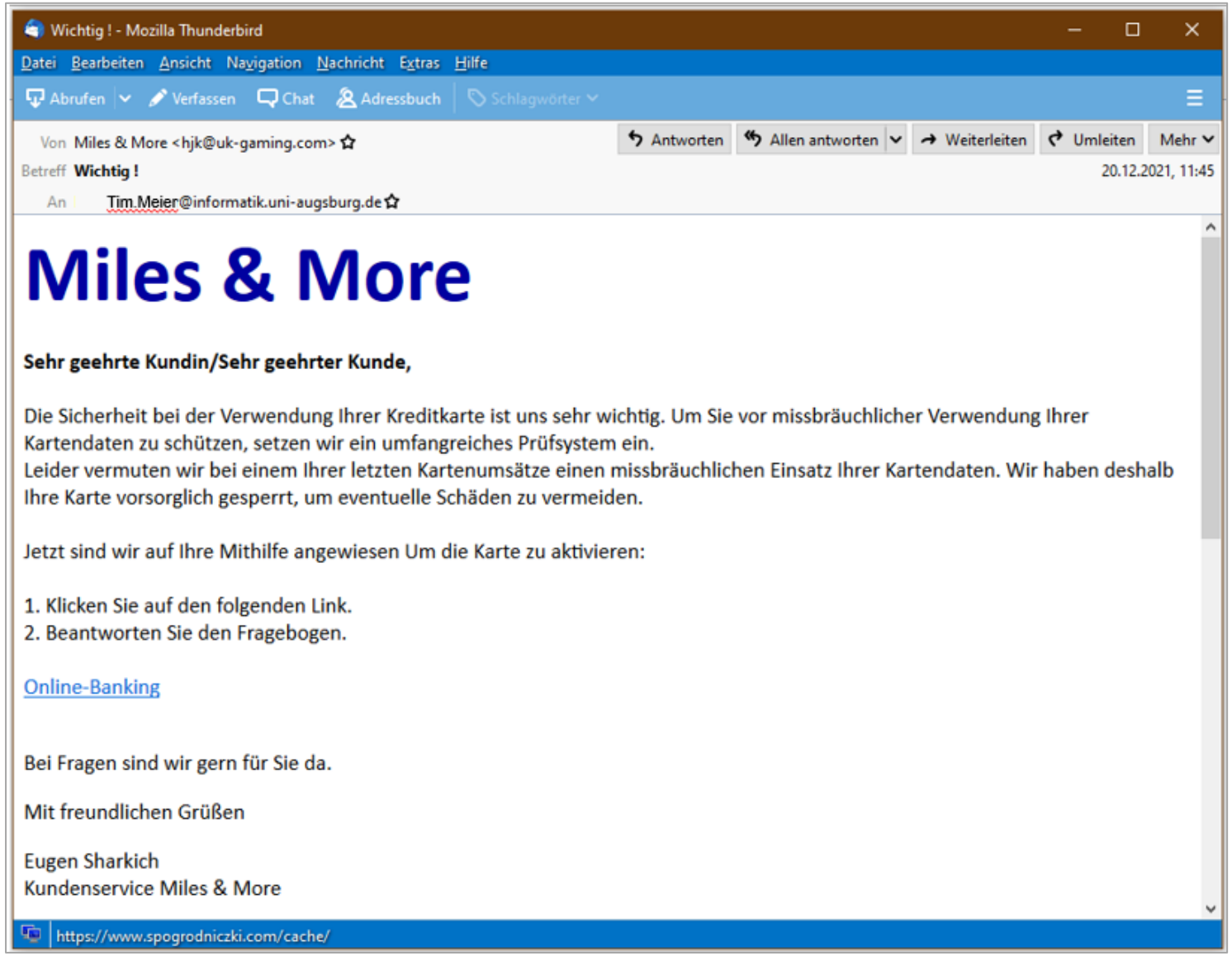


Keine Email-Adresse der DBK

Keine Name nur neutrales „Kunde“ in der Anrede

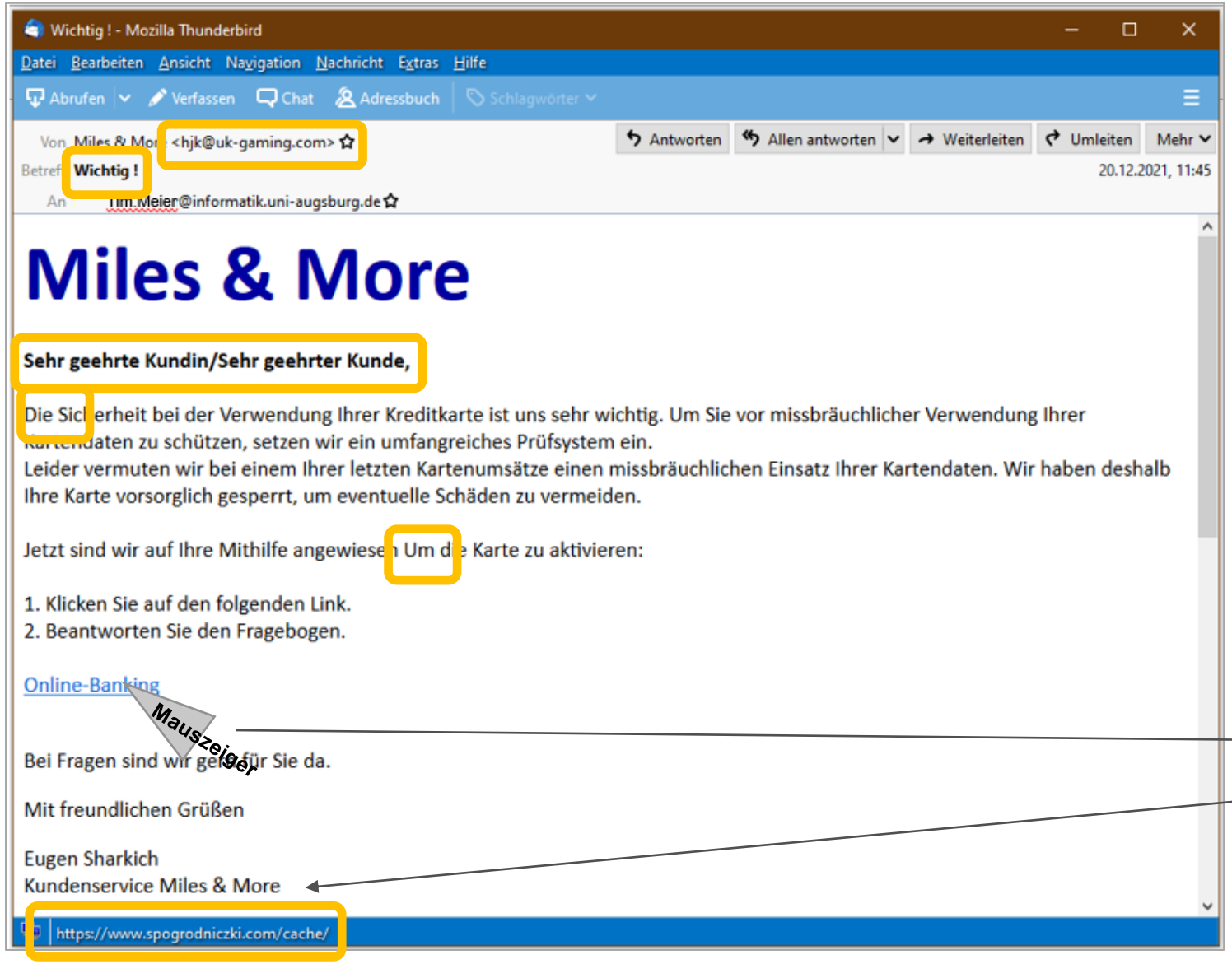
Hoover mit der Maus zeigt einen verdächtigen Link

Was macht Sie stutzig?



1. Begutachten Sie folgende E-Mail kritisch.
2. Beurteilen Sie, ob es Phishing sein könnte.
3. Markieren Sie Stellen, die Sie skeptisch machten.

Was macht Sie stutzig?



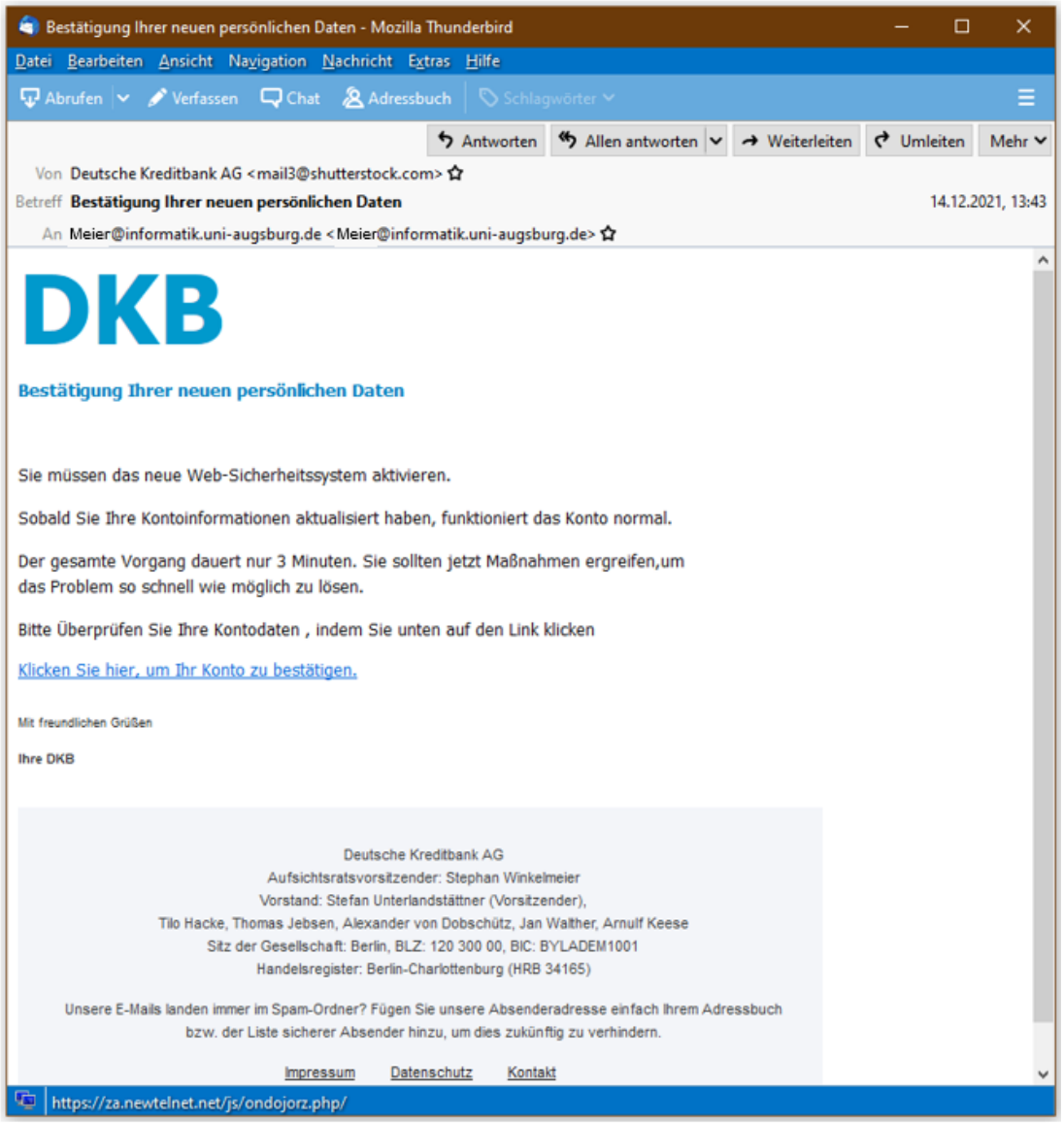
Keine Email-Adresse von Mile & More
Komischer Betreff

Keine Name nur neutrale Anrede

Fehlerhafte Rechtschreibung

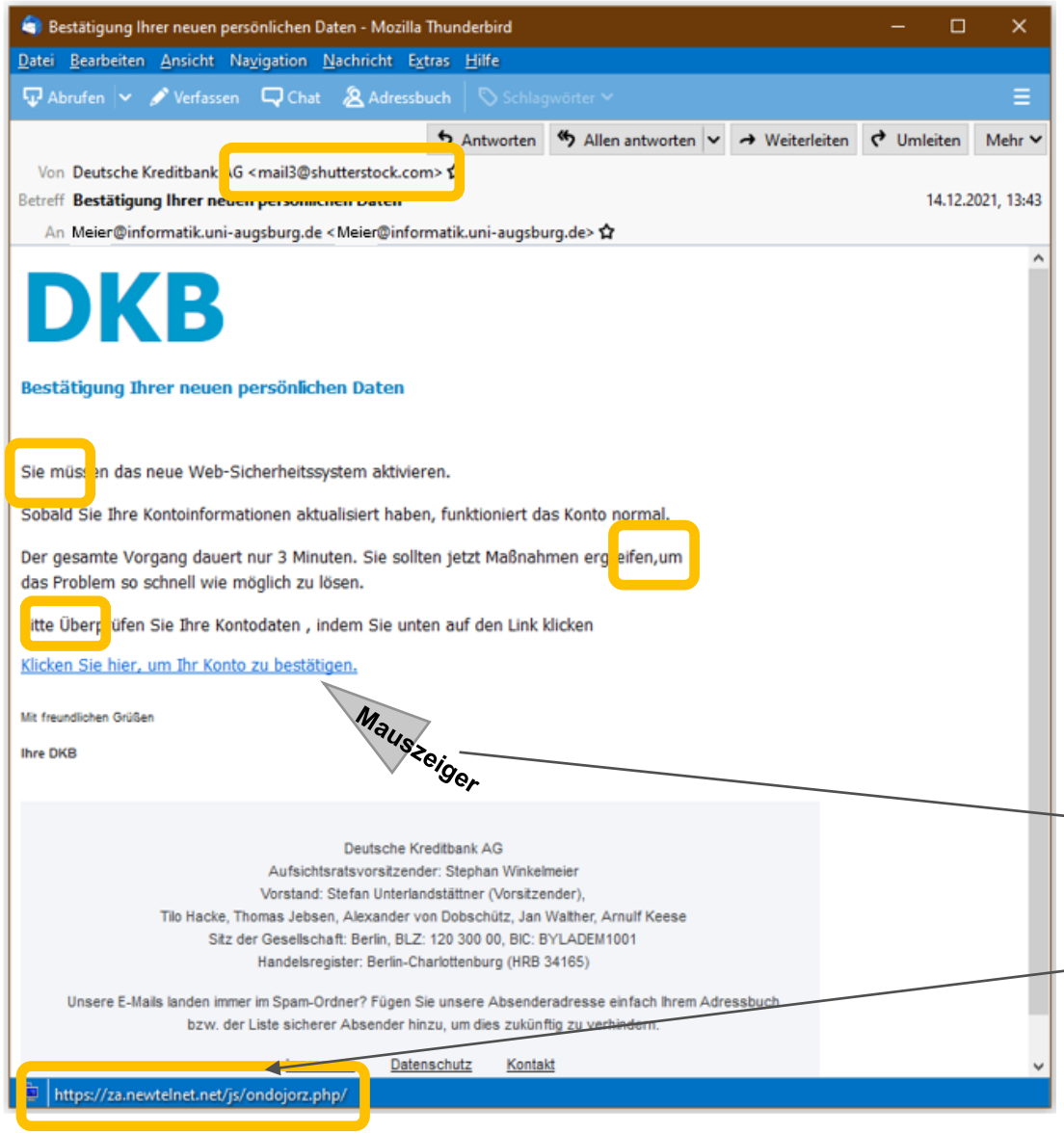
Hoover mit der Maus zeigt einen verdächtigen Link

Was macht Sie stutzig?



1. Begutachten Sie folgende E-Mail kritisch.
2. Beurteilen Sie, ob es Phishing sein könnte.
3. Markieren Sie Stellen, die Sie skeptisch machten.

Was macht Sie stutzig?



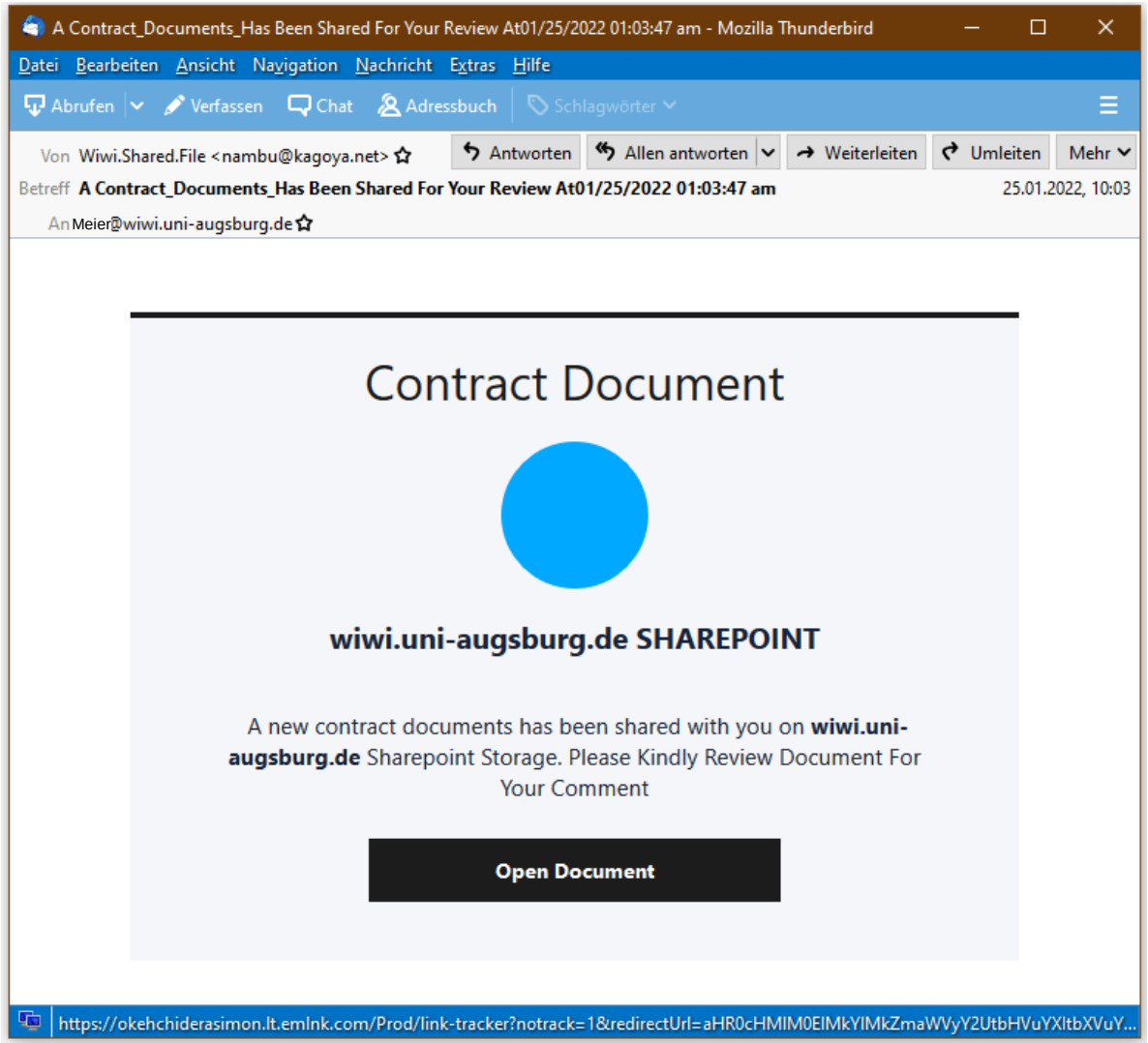
Keine Email-Adresse von DKB

Keine persönliche Anrede

Fehlerhafte Rechtschreibung

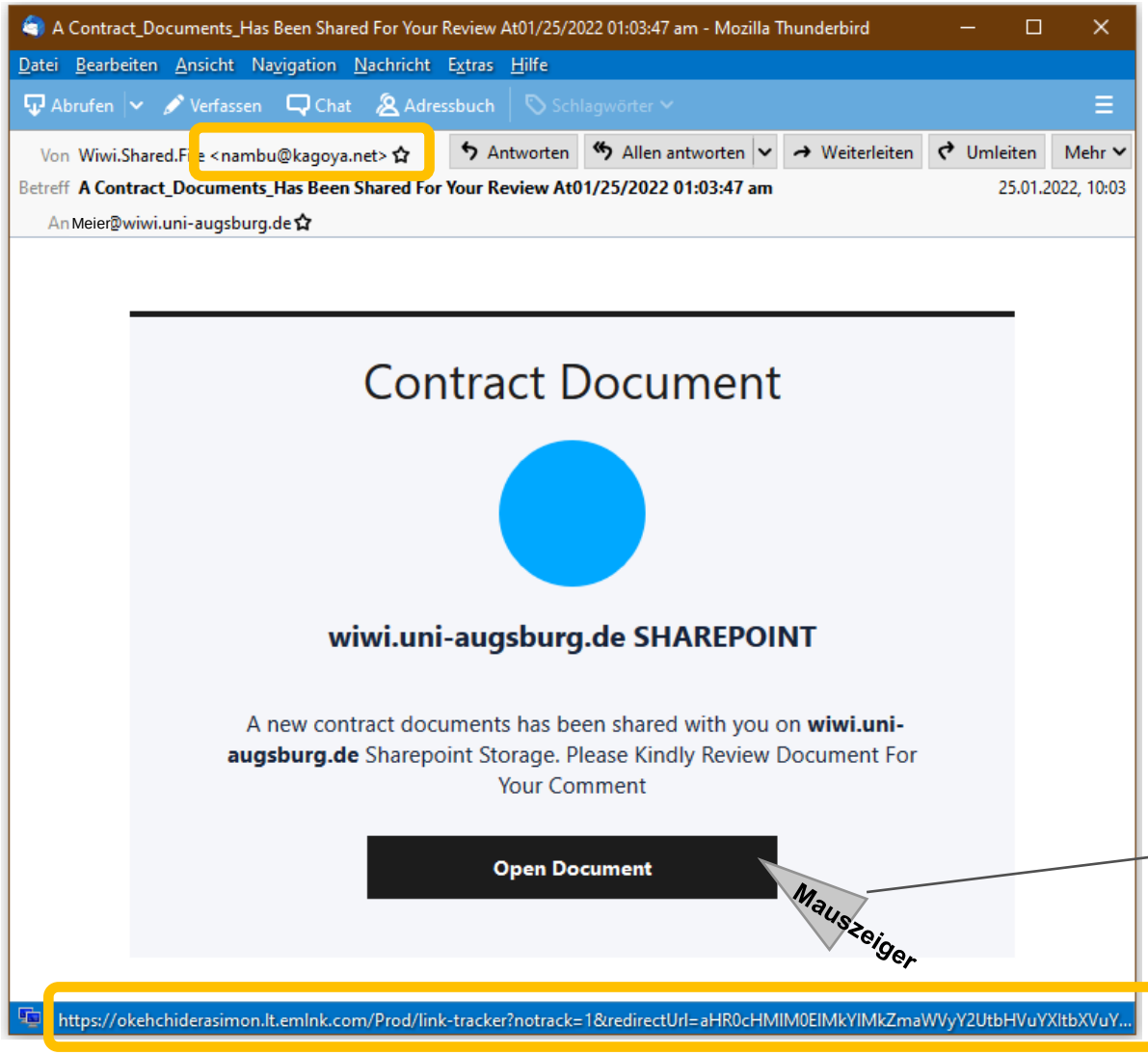
Hoover mit der Maus zeigt einen verdächtigen Link

Was macht Sie stutzig?



1. Begutachten Sie folgende E-Mail kritisch.
2. Beurteilen Sie, ob es Phishing sein könnte.
3. Markieren Sie Stellen, die Sie skeptisch machten.

Was macht Sie stutzig?

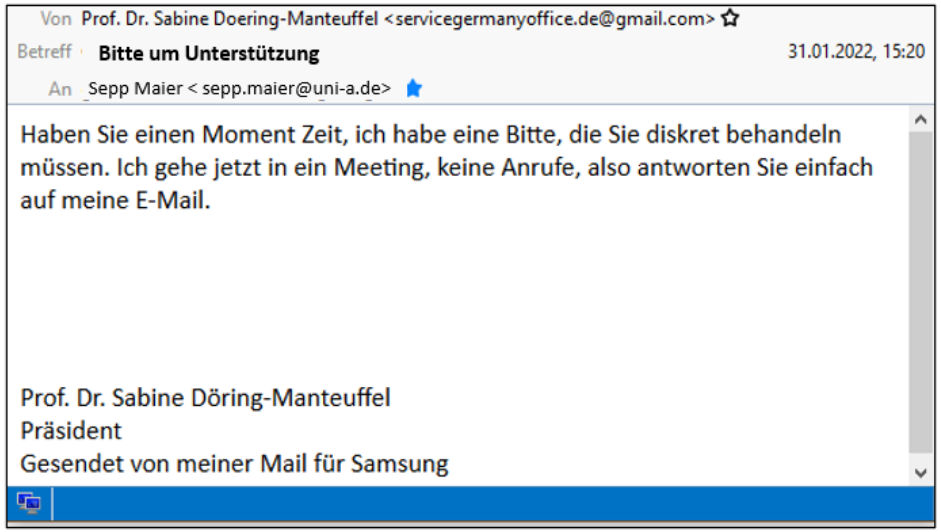


Keine Email-Adresse der Uni Augsburg

Hoover mit der Maus zeigt einen verdächtigen Link

CEO Fraud am Beispiel der Präsidentin – Was fällt Ihnen auf

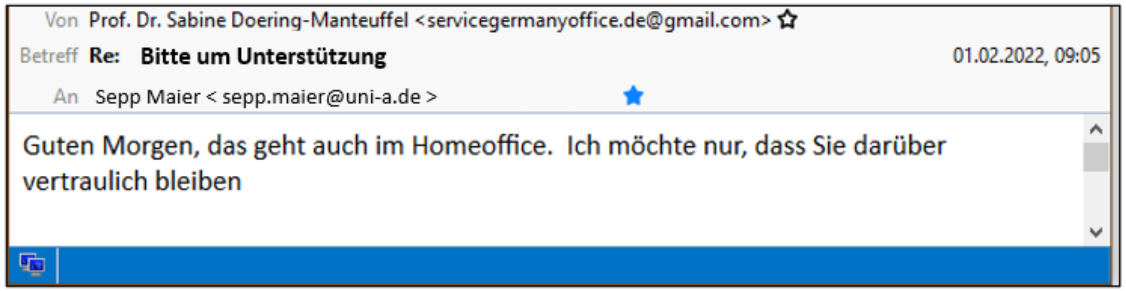
1. Kontaktaufnahme


Von Prof. Dr. Sabine Doering-Manteuffel <servicegermanyoffice.de@gmail.com>
Betreff **Bitte um Unterstützung** 31.01.2022, 15:20
An Sepp Maier < sepp.maier@uni-a.de>

Haben Sie einen Moment Zeit, ich habe eine Bitte, die Sie diskret behandeln müssen. Ich gehe jetzt in ein Meeting, keine Anrufe, also antworten Sie einfach auf meine E-Mail.

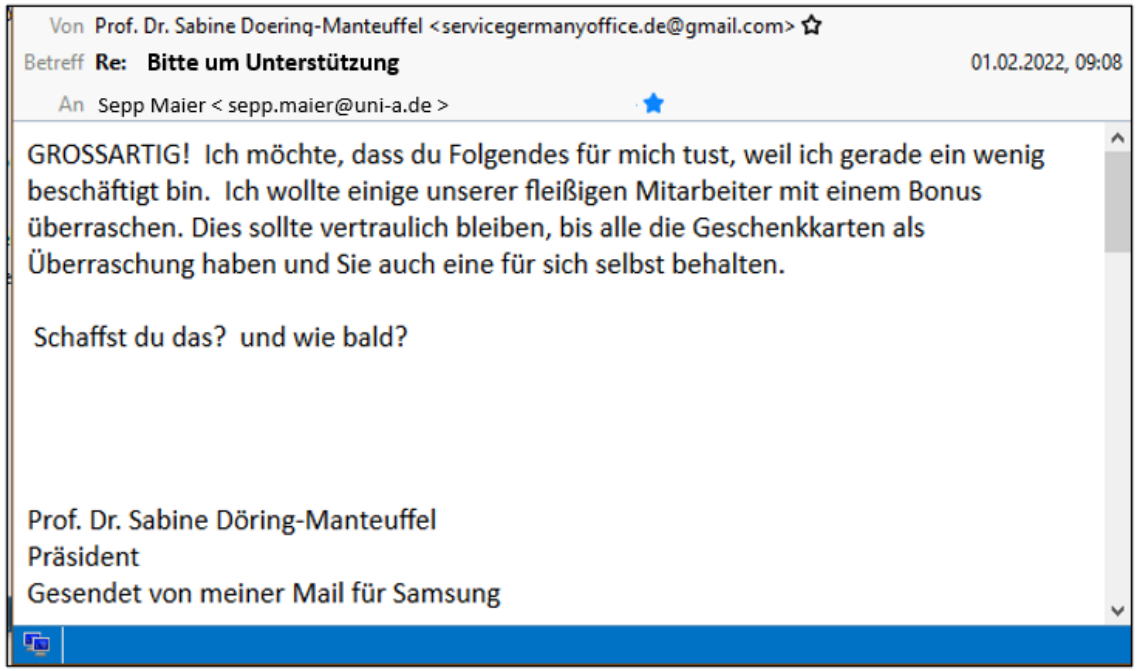
Prof. Dr. Sabine Döring-Manteuffel
Präsident
Gesendet von meiner Mail für Samsung

2. Spezifische Mail je nach der Antwort, bzw. Erinnerung, wenn keine Antwort kam


Von Prof. Dr. Sabine Doering-Manteuffel <servicegermanyoffice.de@gmail.com>
Betreff **Re: Bitte um Unterstützung** 01.02.2022, 09:05
An Sepp Maier < sepp.maier@uni-a.de >

Guten Morgen, das geht auch im Homeoffice. Ich möchte nur, dass Sie darüber vertraulich bleiben

3. Weiterführender Dialog


Von Prof. Dr. Sabine Doering-Manteuffel <servicegermanyoffice.de@gmail.com>
Betreff **Re: Bitte um Unterstützung** 01.02.2022, 09:08
An Sepp Maier < sepp.maier@uni-a.de >

GROSSARTIG! Ich möchte, dass du Folgendes für mich tust, weil ich gerade ein wenig beschäftigt bin. Ich wollte einige unserer fleißigen Mitarbeiter mit einem Bonus überraschen. Dies sollte vertraulich bleiben, bis alle die Geschenkkarten als Überraschung haben und Sie auch eine für sich selbst behalten.

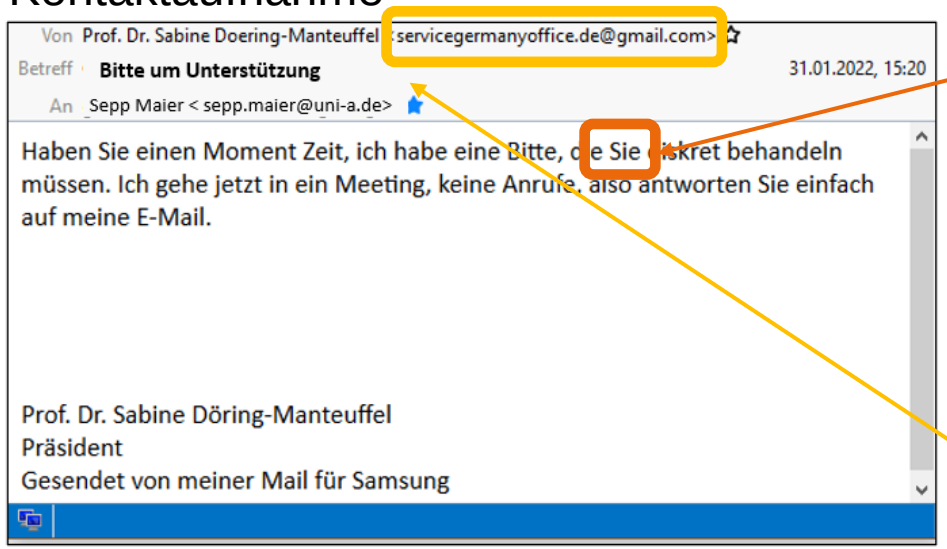
Schaffst du das? und wie bald?

Prof. Dr. Sabine Döring-Manteuffel
Präsident
Gesendet von meiner Mail für Samsung

4. Hier kommt dann die Aufforderung zur Bestellung eines Gutscheins bei Amazon oder dergleichen

CEO Fraud am Beispiel der Präsidentin

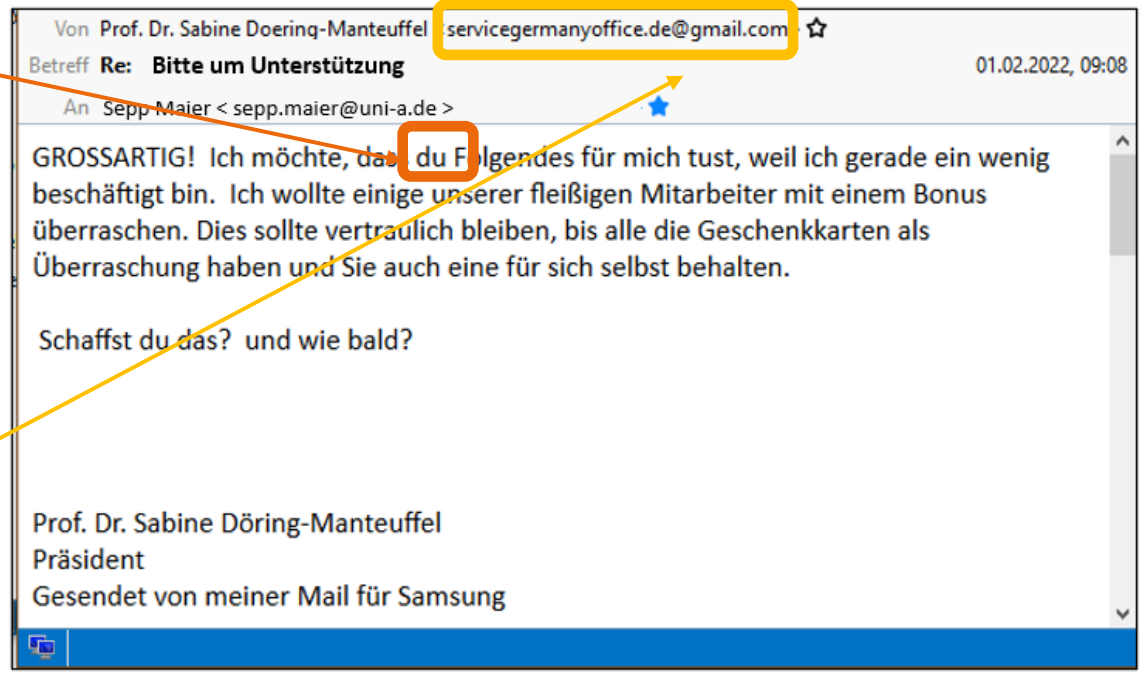
1. Kontaktaufnahme



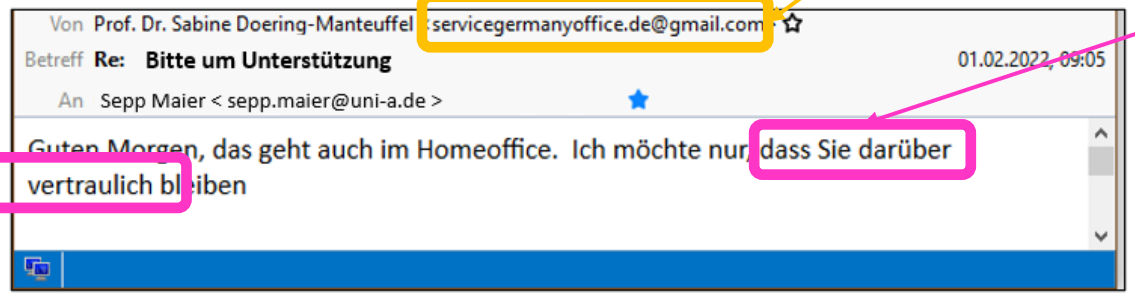
Sie → du

Adresse

3. Weiterführender Dialog



2. Spezifische Mail je nach der Antwort, bzw. Erinnerung, wenn keine Antwort kam



Schlechtes Deutsch

4. Hier kommt dann die Aufforderung zur Bestellung eines Gutscheins bei Amazon oder dergleichen