



# 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:



Bundesministerium  
für Wirtschaft  
und Energie



**IT-Sicherheit**  
IN DER WIRTSCHAFT

aufgrund eines Beschlusses  
des Deutschen Bundestages

[www.it-sicherheit-in-der-wirtschaft.de](http://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
  - (Unbemerkt) Download von Schadsoftware
  - Öffnen betrügerischer aber authentisch aussehender Webseite zum Einloggen→ Eigene Aktionen an Ihrem Gerät *durchführen* bis hin zur Blockierung der Nutzung durch Sie  
→ Identitätsdiebstahl, Erpressung, ...
- Aufforderung sensible Daten wie Passwörter und Bankdaten zu schicken → Ihre Daten/Aktionen im Account *einsehen*  
→ Identitätsdiebstahl, Erpressung, ...
- Aufforderung Rechnung zu begleichen durch Überweisungen oder vermeintliche Geschäftspartner anzurufen → 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

„Phishing“

# 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 Schutzmaßnahmen  
... 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



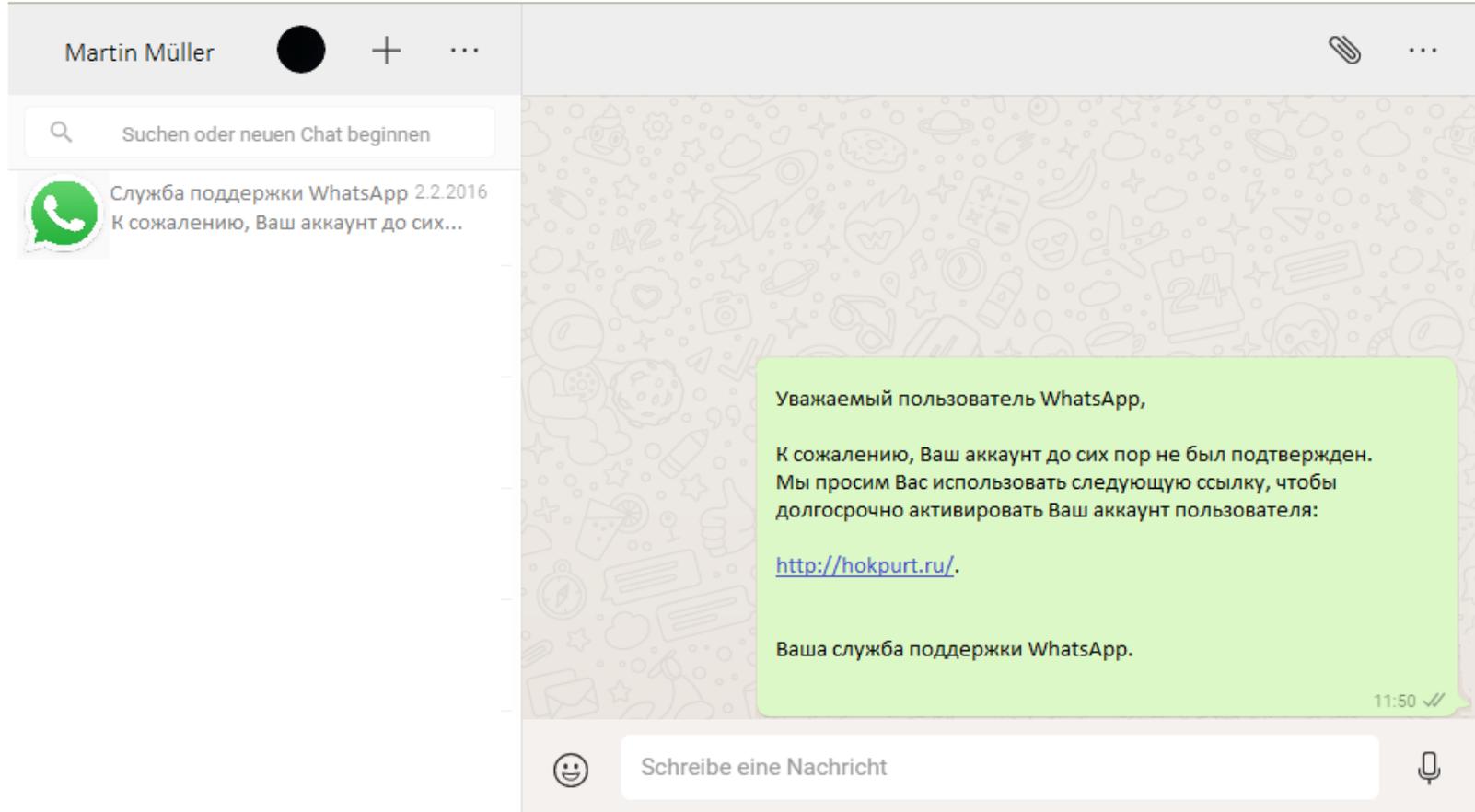
Link

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?



Hallo Kolege, morgen find spontaner Betriebsausflug stat!  
Schauen Sie Plan:

16:04



plan.docx  
11 KB

16:04

---

per Skype

Nachricht hier eingeben



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

Von 1&1 Kundenservice <1und1service@forsurija.ru>  

Betreff **Auftragsbestätigung** 16:28

An mich



Hallo Martin Müller,

Ihre Auftrag ist bei uns eingegangen.

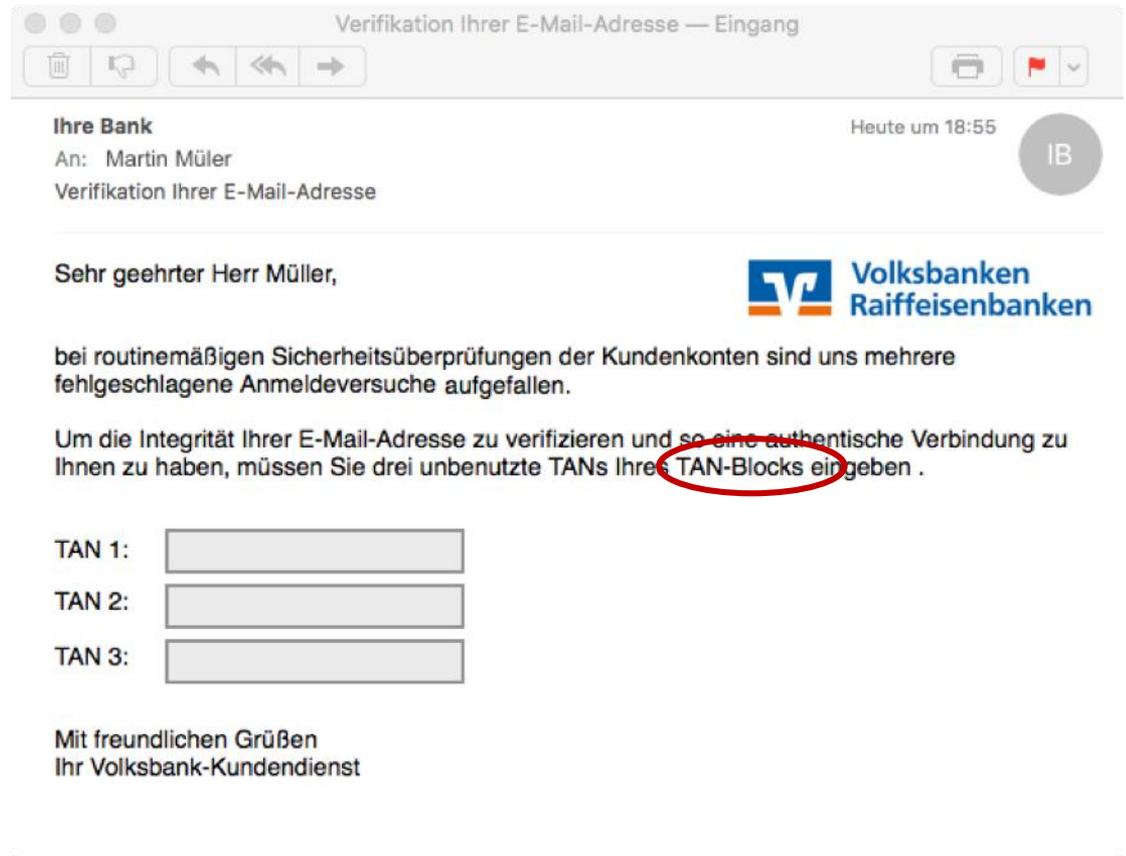
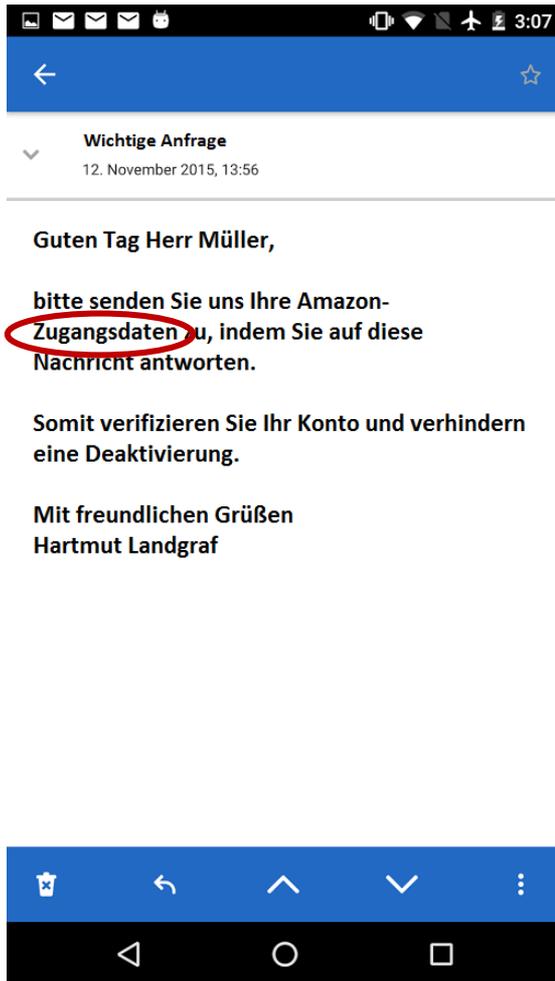
Klicken Sie [hier](#), um den Status der Auftragsbearbeitung einzusehen.

Vielen Dank für Ihr Vertrauen in 1&1.

Ihr 1&1-Kundenservice



# Werden Sie aufgefordert sensible Daten zu schicken?



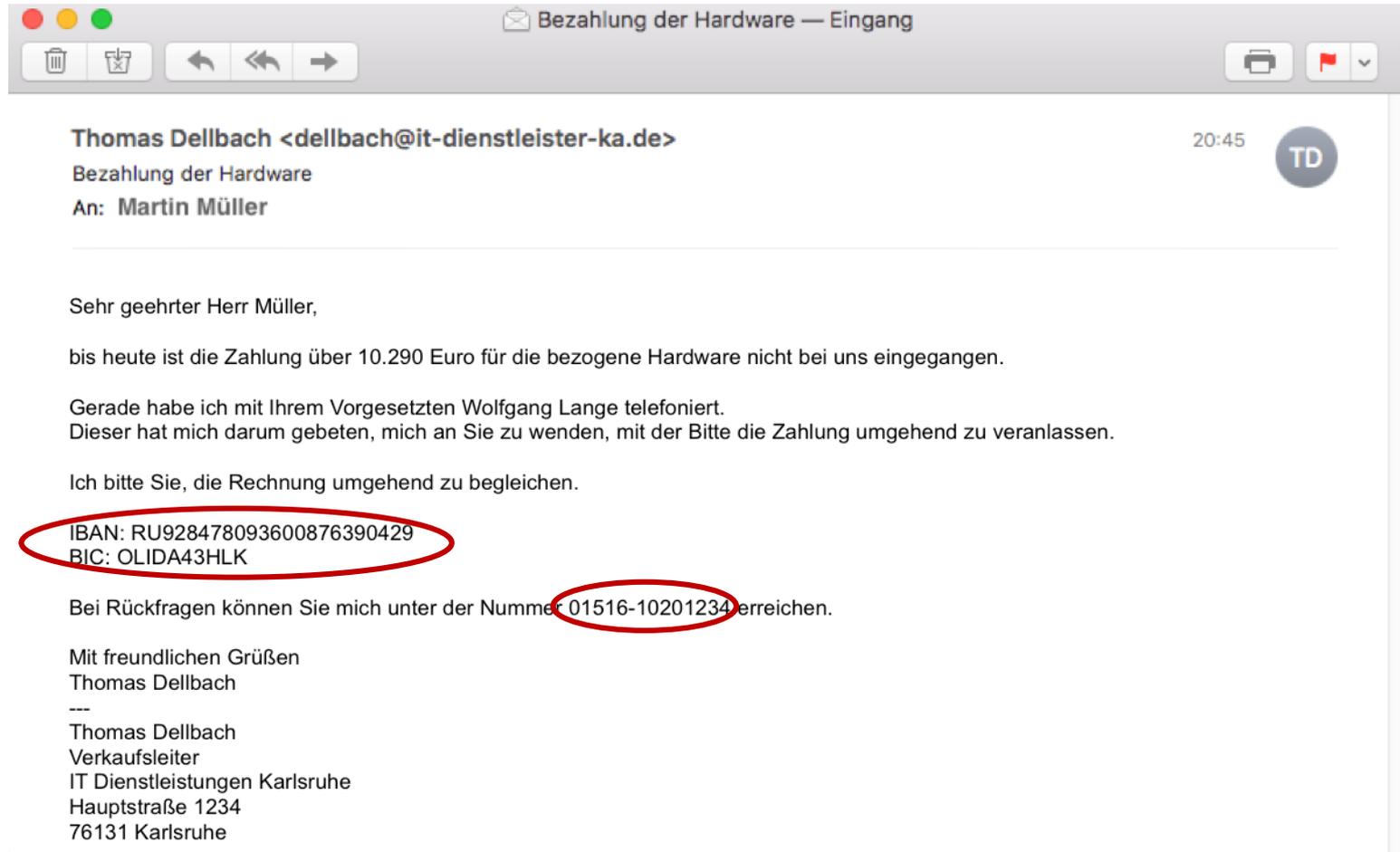
Seriöse Unternehmen werden Sie nicht zur Angabe derartiger Daten in einer Nachricht auffordern!

# 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?





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

Von 1&1 Kundenservice <kundenservice@1und1.de>

← Antworten

→ Weiterleiten

Betreff **Auftragsbestätigung**

16:28

An mich

**1&1** Kundenservice

Hallo Martin Müller,

Ihre Auftrag ist bei uns eingegangen.

Klicken Sie [hier](#), um den Status der Auftragsbearbeitung einzusehen.

Vielen Dank für Ihr Vertrauen in 1&1.

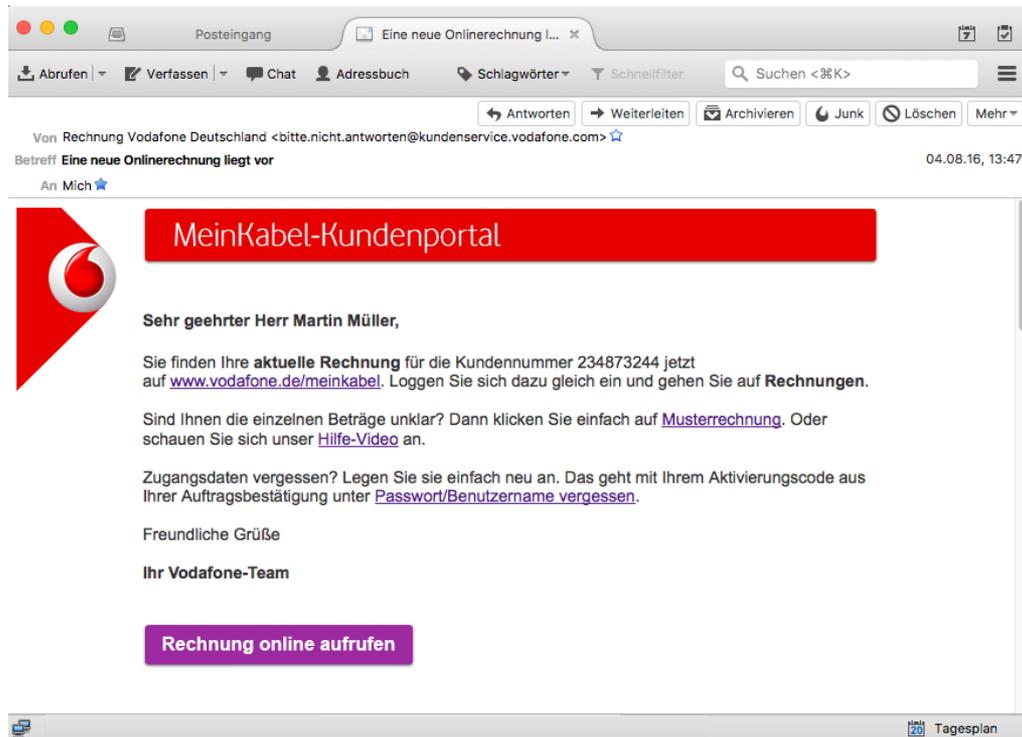
Ihr 1&1-Kundenservice



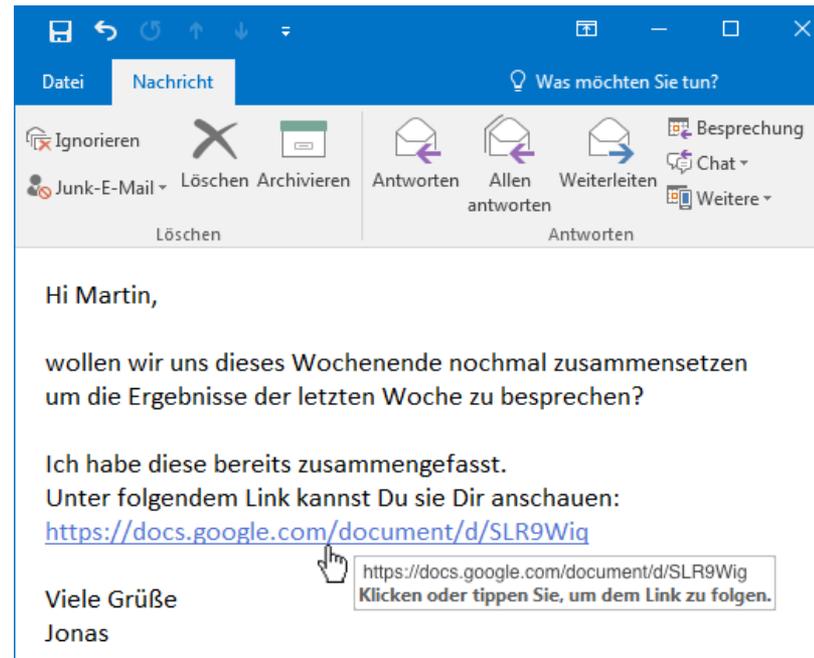
[https://www.1und1.de.shoppingsicher.de/product/ADKGHJWEKE\\_ref=1321423&JASH/refilogh/d43...](https://www.1und1.de.shoppingsicher.de/product/ADKGHJWEKE_ref=1321423&JASH/refilogh/d43...)

Ist dies ein gefährlicher Link?

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



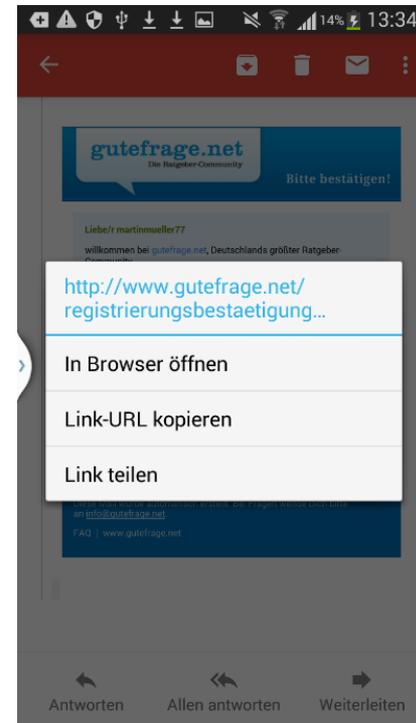
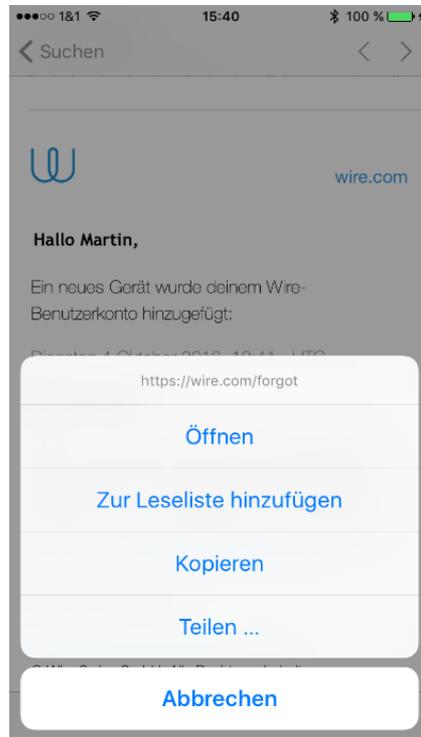
Statusleiste



Tooltip/Infocell

→ 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

Posteingang | Vorschläge für den Retreat ... x

Abrufen | Verfassen | Chat | Adressbuch | Schlagwörter | Schnellfilter | Suchen <⌘K>

Von Jonas Schmidt <jonas.schmidt.78@web.de> ☆ | Antworten | Weiterleiten | Archivieren | Junk | Löschen | Mehr ▾

Betreff **Vorschläge für den Retreat** | 17:53

An Mich ☆

Hallo Martin,

wie in der letzten Dienstbesprechung abgesprochen habe ich zwei Alternativen für unseren Retreat rausgesucht. Was hältst Du von den Angeboten?

Hier die Links zu den Hotels:

<https://hotels.ab-in-den-urlaub.de/de/EUR/hotel/id432432>

<https://hotels.ab-in-den-urlaub.de/de/EUR/hotel/id784693>

Sobald Du mir Bescheid gibst, welches Angebot ich wählen soll, kann ich das für gesamte Gruppe buchen.

Viele Grüße  
Jonas

http://www.wasere.com/ | 87% | 1 | Tagesplan



# Vorsicht Falle: Falscher Tooltip

Von Miles & More <OnlineServices@lufthansa.com>  
Betreff **Erinnerung: Bonusmeilen laufen ab**  
An martin.mueller.77@web.de

 **Lufthansa**  
Nonstop you

**Sehr geehrter Herr Müller,**

wir möchten Sie nochmals dran erinnern, dass Sie seit über 12 Monate keine Aktivität mehr auf Ihrem Nutzerkonto hatten.

Dies führt automatisch zu einer Deaktivierung Ihres Nutzerkontos inklusive dem Verfall aller bisher angesammelter Bonusmeilen.

Falls Sie die Bonusmeilen weiterhin nutzen möchten, melden Sie sich bitte innerhalb der nächsten 24 Stunden unter dem folgenden Link bei Ihrem Konto an. Ihr Konto wird dann automatisch um 12 weitere Monate verlängert:

 <http://www.lufthansa.de/login/eh87>

Mit freundlichen Grüßen,  
Ihr Lufthansa-Kundencenter

<http://sdwasere.cc> 14 Tagesplan ^

## 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.sdwasure.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

Von 1&1 Kundenservice <kundenservice@1und1.de> Antworten Weiterleiten

Betreff **Auftragsbestätigung** 16:28

An mich

**1&1 Kundenservice**

Hallo Martin Müller,

Ihre Auftrag ist bei uns eingegangen.

Klicken Sie [hier](#), um den Status der Auftragsbearbeitung einzusehen.

Vielen Dank für Ihr Vertrauen in 1&1.

Ihr 1&1-Kundenservice

 [https://www.1und1.de/rulowinka.ru/product/ADKGHJWEKE\\_ref=1321423&JASH/refilogh/d43...](https://www.1und1.de/rulowinka.ru/product/ADKGHJWEKE_ref=1321423&JASH/refilogh/d43...)



# 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.

Von 1&1 Kundenservice <kundenservice@1und1.de> Antworten Weiterleiten  
Betreff **Auftragsbestätigung** 16:28  
An mich

**1&1 Kundenservice**

Hallo Martin Müller,

Ihre Auftrag ist bei uns eingegangen.

Klicken Sie [hier](#), um den Status der Auftragsbearbeitung einzusehen.

Vielen Dank für Ihr Vertrauen in 1&1.

Ihr 1&1-Kundenservice

 [https://www.ortreich.de/product/ADKGHJWEKE\\_ref=1321423&JASH/refilogh/d43...](https://www.ortreich.de/product/ADKGHJWEKE_ref=1321423&JASH/refilogh/d43...)

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



# Vorsicht Falle: Verwendung von vertrauensweckenden Begriffen

Von 1&1 Kundenservice <kundenservice@1und1.de> Antworten Weiterleiten  
Betreff **Auftragsbestätigung** 16:28  
An mich

**1&1 Kundenservice**

Hallo Martin Müller,

Ihre Auftrag ist bei uns eingegangen.

Klicken Sie [hier](#), um den Status der Auftragsbearbeitung einzusehen.

Vielen Dank für Ihr Vertrauen in 1&1.

Ihr 1&1-Kundenservice

 [https://www.sichertelefonieren.de/product/ADKGHJWEKE\\_ref=1321423&JASH/refilogh/d43...](https://www.sichertelefonieren.de/product/ADKGHJWEKE_ref=1321423&JASH/refilogh/d43...)

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-rmarkt.de                statt      media-markt.de
- eurovings.de                      statt      eurowings.de
- sparkasse-duesselclorf.de    statt      sparkasse-duesseldorf.de
- Otto.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
- microsfof.de                        statt      microsoft.de
- lufthanser.com                      statt      lufthansa.de
- zallando.de                         statt      zalando.de
- googel.de                            statt      google.de

Vorsicht mit Aussprache im Englischen



# Vorsicht Falle: 99,9% sieht plausibel aus

Von 1&1 Kundenservice <kundenservice@1und1.de> Antworten Weiterleiten

Betreff **Auftragsbestätigung** 16:28

An mich

**1&1 Kundenservice**

Hallo Martin Müller,

Ihre Auftrag ist bei uns eingegangen.

Klicken Sie [hier](#), um den Status der Auftragsbearbeitung einzusehen.

Vielen Dank für Ihr Vertrauen in 1&1.

Ihr 1&1-Kundenservice

 [https://www.1urd1.de/product/ADKGGHJWEKE\\_ref=1321423&JASH/refilogh/d43...](https://www.1urd1.de/product/ADKGGHJWEKE_ref=1321423&JASH/refilogh/d43...)



# 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.arbeitsagentur.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](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.stackoverflowv.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?

Von 1&1 Kundenservice <kundenservice@1und1.de> Antworten Weiterleiten

Betreff **Auftragsbestätigung** 16:28

An mich

**1&1 Kundenservice**

Hallo Martin Müller,

Ihre Auftrag ist bei uns eingegangen.

Klicken Sie [hier](#), um den Status der Auftragsbearbeitung einzusehen.

Vielen Dank für Ihr Vertrauen in 1&1.

Ihr 1&1-Kundenservice

 [https://www.1und1.de.shoppingsicher.de/product/ADKGHJWEKE\\_ref=1321423&JASH/refilogh/d43....](https://www.1und1.de.shoppingsicher.de/product/ADKGHJWEKE_ref=1321423&JASH/refilogh/d43....)



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

Von 1&1 Kundenservice <kundenservice@1und1.de> Antworten Weiterleiten

Betreff **Auftragsbestätigung** 16:28

An mich

**1&1 Kundenservice**

Hallo Martin Müller,

Ihre Auftrag ist bei uns eingegangen.

Sie finden die Auftragsbestätigung in dem angehängten Dokument.  
Lesen Sie dies bitte aufmerksam und befolgen Sie die Anweisungen.

Vielen Dank für Ihr Vertrauen in 1&1.

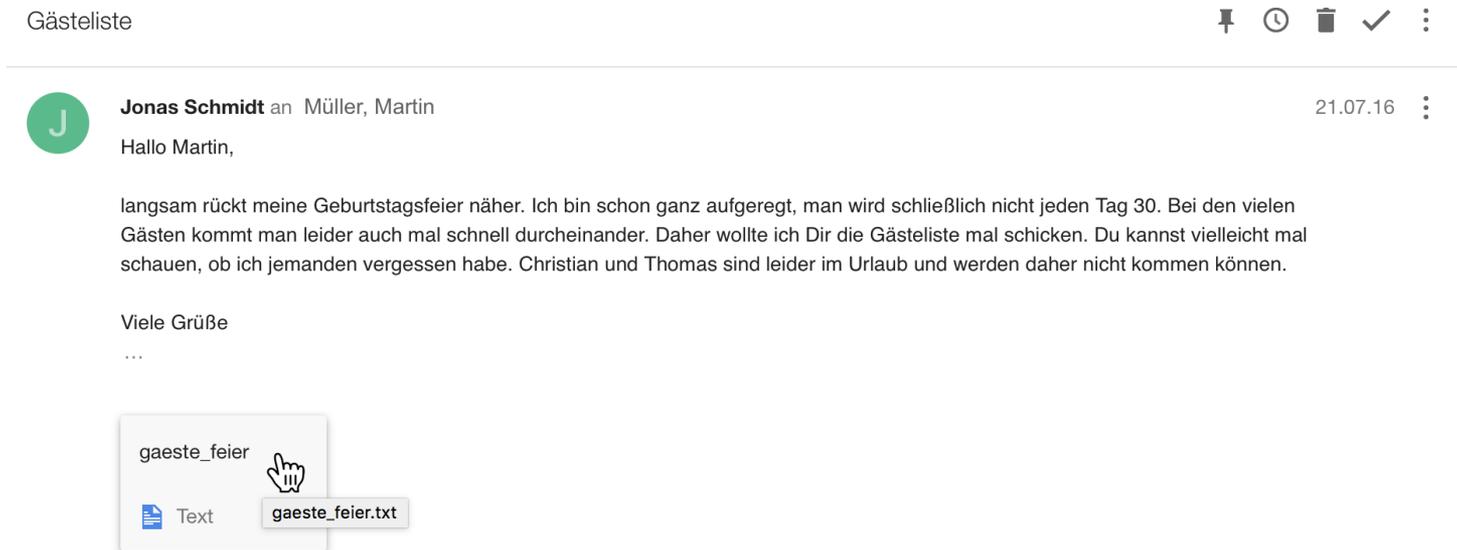
Ihr 1&1-Kundenservice

1 Anhang: auftragsbestätigung.pdf.exe 258 KB Speichern

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.

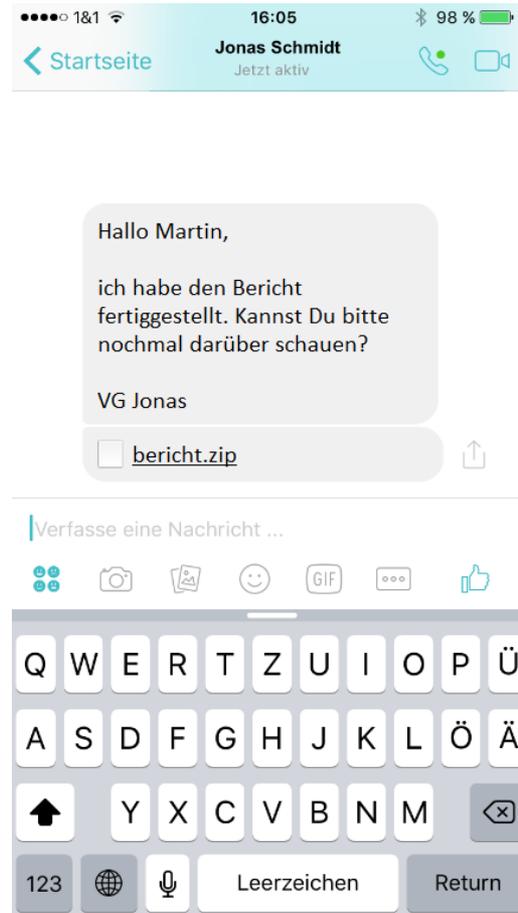
Weit verbreitete potentiell gefährliche Formate:

- 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

Ihre Wohnungsanzeige — Eingang

Michael Uhlmann  21. Juli 2016 um 16:06 

An: Martin Müller  
Ihre Wohnungsanzeige

---

Sehr geehrter Herr Müller,

ich habe Ihr Wohnungsgesuch im Stadtanzeiger gelesen. Ich kann Ihnen eine Wohnung anbieten, die genau Ihren Vorstellungen entspricht. Die Wohnung ist zentral gelegen und dennoch ausgesprochen ruhig. Darüber hinaus haben Sie die Bushaltestelle direkt vor der Tür und können in wenigen Minuten in alle Ecken der Stadt kommen. Als Anhang dieser Mail finden Sie den Grundriss der Wohnung.

Für Rückfragen stehe ich Ihnen selbstverständlich zur Verfügung.

Mit freundlichen Grüßen  
Michael Uhlmann

  
foto.jpg.exe



# Vorsicht Falle: 99% sieht plausibel aus

Von 1&1 Kundenservice <kundenservice@1und1.de> Antworten Weiterleiten

Betreff **Auftragsbestätigung** 16:28

An mich

**1&1 Kundenservice**

Hallo Martin Müller,

Ihre Auftrag ist bei uns eingegangen.

Sie finden die Auftragsbestätigung in dem angehängten Dokument.  
Lesen Sie dies bitte aufmerksam und befolgen Sie die Anweisungen.

Vielen Dank für Ihr Vertrauen in 1&1.

Ihr 1&1-Kundenservice

▶ 1 Anhang: auftragsbestätigung.pdf.exe 258 KB Speichern

## 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:

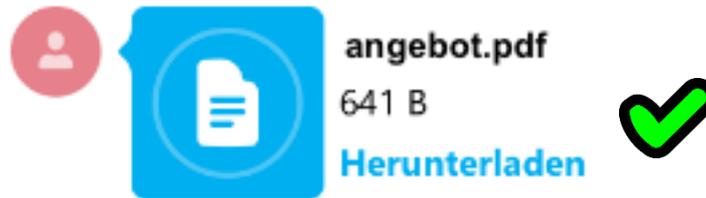


foto.jpg.exe



# 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:

Heute

MH

Hallo Martin,

ich denke Du wirst mich nicht kennen, wir haben jedoch beim letzten Firmen-Fußball-Turnier gegeneinander gespielt. Meine Frau hat dieses tolle Foto der Siegerehrung geschossen.

Vielleicht magst Du des Dir ja mal anschauen.

Viele Grüße  
Max Habermann

MH



foto.jpg.exe  
349 Byte





# Übung: Ist der Anhang potentiell gefährlich?

Sie haben die folgende Nachricht erhalten:



**Thomas Lores**

26.02.2015, 16:08 Uhr

Options

Sehr geehrter Herr Müller,

Ihre Erfahrung im Bereich des Projektmanagements sowie Ihre technische Expertise im Allgemeinen haben mein Interesse geweckt. Für einen großen Automobilhersteller bin ich derzeit auf der Suche nach Personen wie Ihnen.

Anbei sende ich Ihnen eine aktuelle Stellenausschreibung des angesprochenen Automobilherstellers. Sollte diese Ausschreibung für Sie interessant sein, so lassen Sie mich dies bitte wissen.

Mit freundlichen Grüßen  
Thomas Lores

[ausschreibung2502105.rar \(347 kb\)](#)





# 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/4xIU1IPJs\\_4](https://youtu.be/4xIU1IPJs_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/passec/>



# 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/>



- 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](https://de.wikipedia.org/wiki/Technische_Universit%C3%A4t_Darmstadt)

The URL behind this link is not the actual URL. You will be redirected to the following URL:

[https://de.wikipedia.org/wiki/Technische\\_Universit%C3%A4t\\_Darmstadt](https://de.wikipedia.org/wiki/Technische_Universit%C3%A4t_Darmstadt)

The developers considered the domain (highlighted part) of this URL as low-risk.

 [More information on this redirection case and how to check the URL](#)

<http://edition.cnn.com/regions>

http://edition. **cnn.com**  
/regions

This domain is not yet known or considered by TORPEDO.

 Please check the domain (highlighted part) carefully and then decide whether you can click it safely or you should delete it.

 [More information on how to check the URL](#)

Link is deactivated to give you time to check it.

Time remaining: 02 second(s)

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

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

You considered the domain (highlighted part) of this URL as low-risk.

 [More information on risk consideration](#)

- Freiverfügbar unter:

<https://www.secuso.org/torpedo>