

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




01. November 2017
Sicherheitsforum "Online-Banking"
Dr. Marco Ghiglieri
Benjamin Reinheimer



Vertrauen Sie dieser E-Mail?

Von Service Dienst <noreply@happyclients.com>
Betreff Bitte bestätige deine E-Mail Adresse!
An martin.mueller.77@web.de

SecurePay 

Hallo,

Von **Service Dienst <noreply@happyclients.com>**
Betreff Bitte bestätige deine E-Mail Adresse!
An martin.mueller.77@web.de

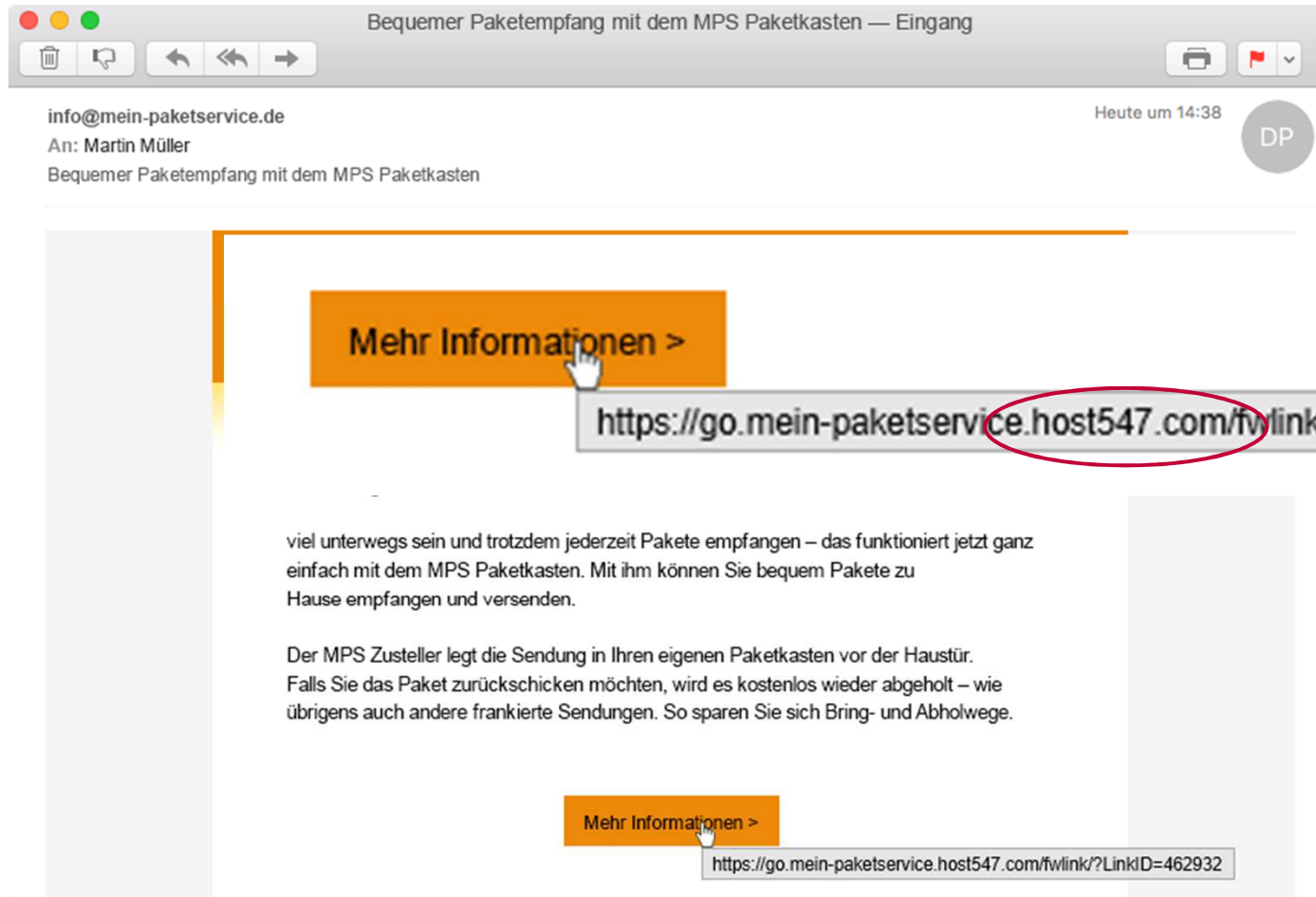
Herzliche Grüße,
du da. Als
Bitte klicke auf folgenden Link, um deine Anmeldung.

E-Mail-Adresse bestätigen

Danke
Das SecurePay24-Team

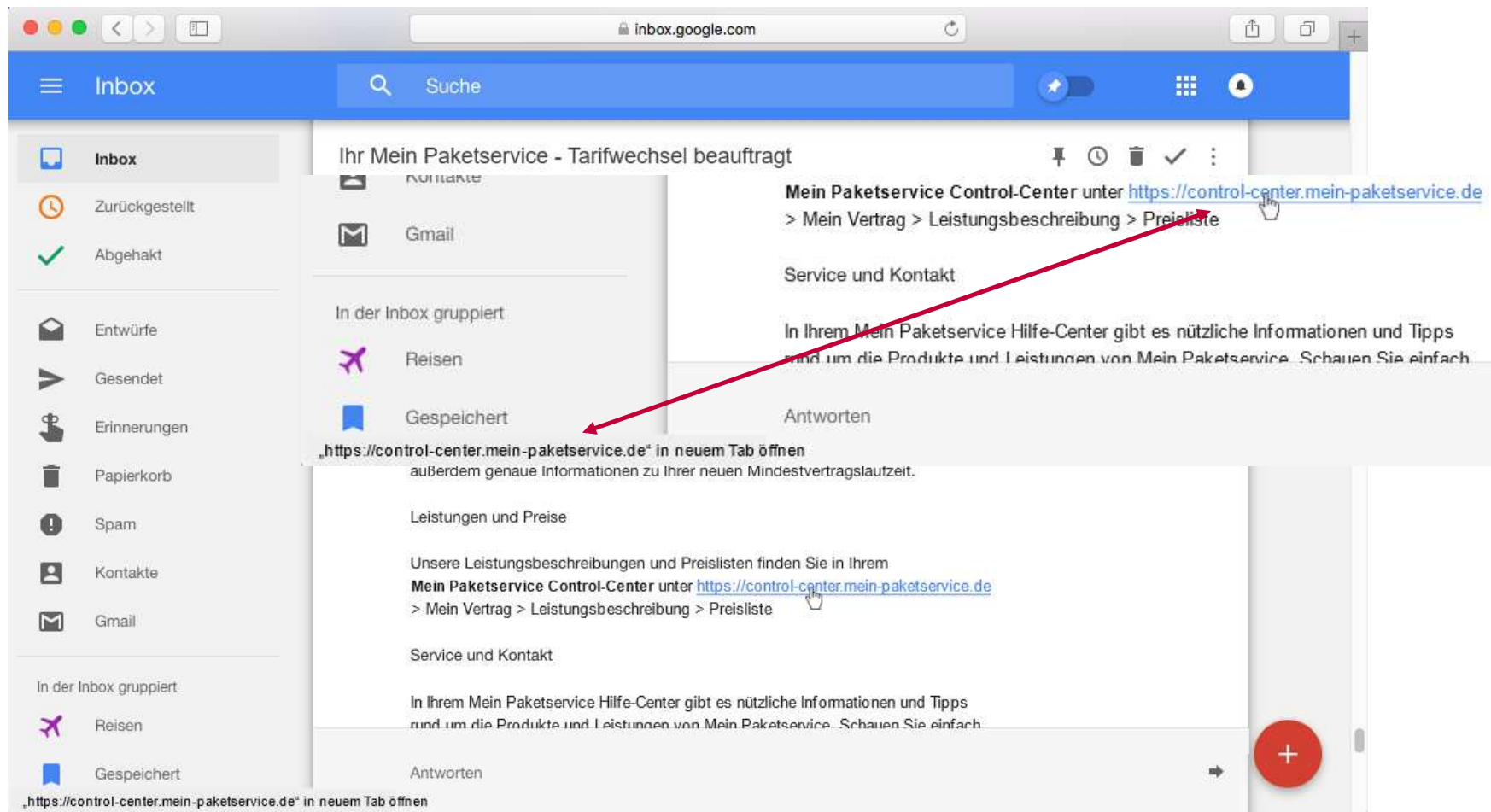


Vertrauen Sie dieser E-Mail?





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?

Von Kundenservice <1und1service@forsurija.ru> Antworten Weiterleiten

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.

Ihr Kundenservice

Relevant ist der Bereich mit dem „@“, aber auch dieser kann gefälscht sein.




Vertrauen Sie dieser E-Mail?

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

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.

Ihr Kundenservice

 https://www.1und1.de.rulowinka.ru/product/ADKGHJWEKE_ref=1321423&JASH/refilogh/d43....



Wie erkennen Sie gefährliche Nachrichten?

Ist die Nachricht plausibel?

Ja

Sind die enthaltenen Webadressen plausibel?

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?

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

Betreff **Auftragsbestätigung** 16:28

An mich




Hallo Martin Müller,

Ihre Auftrag ist bei uns eingegangen.

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

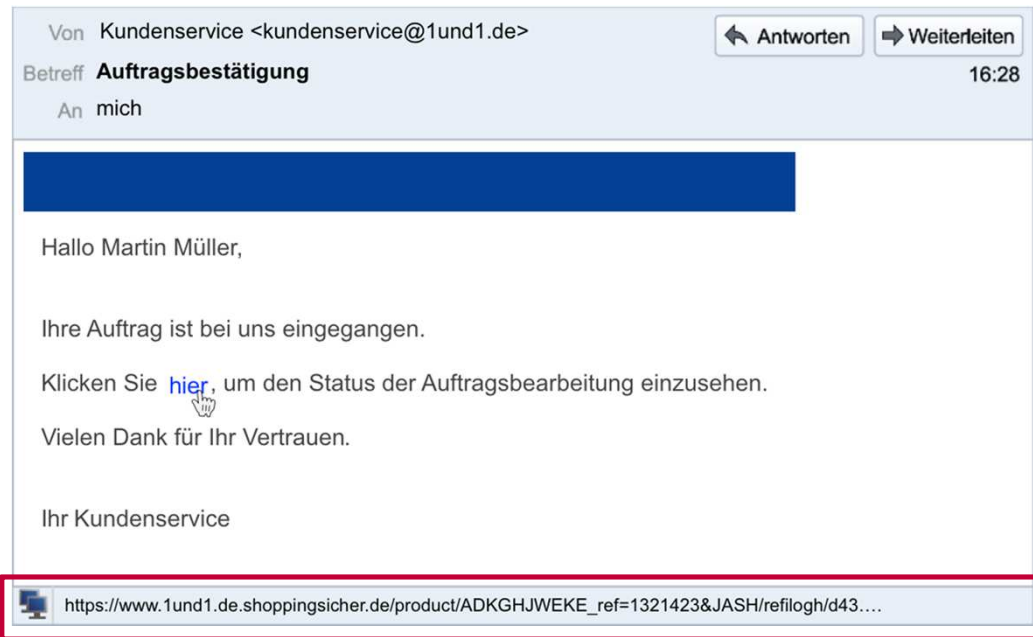
Vielen Dank für Ihr Vertrauen.

Ihr Kundenservice

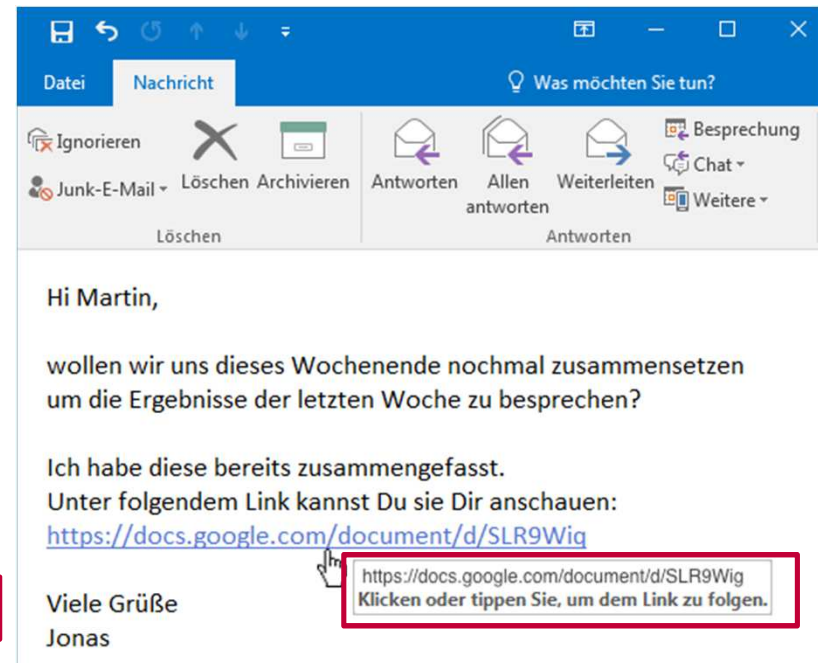




Welche Webadresse steckt hinter dem Link?



Statusleiste
(z.B. Thunderbird)



Tooltip
(z.B. Outlook)



Vorsicht Falle: Falscher Tooltip

From Jonas Schmidt <jonas.schmidt.77@web.de> ☆

Subject **Meeting Minutes** 2

To Martin Müller <martin.mueller.77@web.de> ☆

Hi Martin,

as discussed the meeting minutes of our today's appointment. I saved it in our workspace: <https://www.ourworkspace.com/doc=288291/edit>
If you have any changes, please let me know. Thank you for your contribution.

Click here

<https://www.ourworkspace.com/doc=288291/edit>

Best.

Jonas



<https://secure-documents-online.com/join>



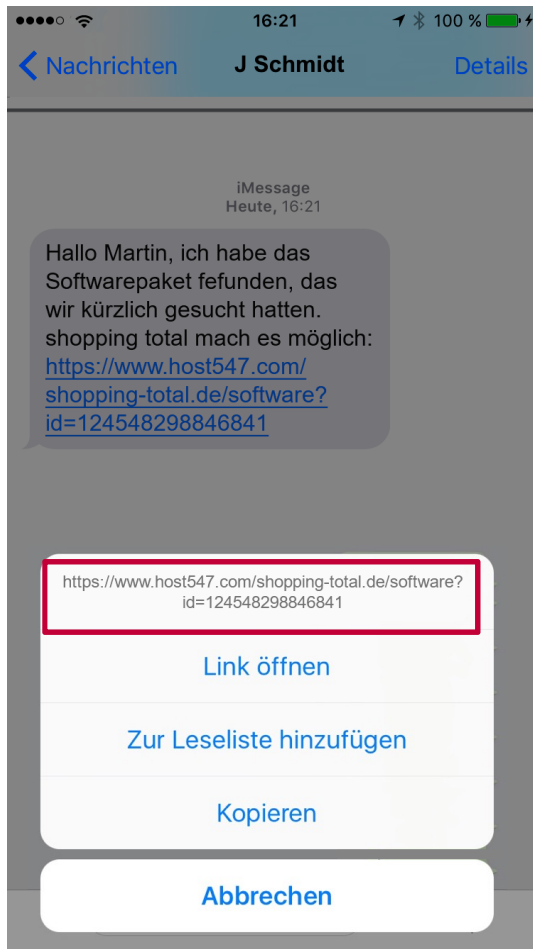


Vorsicht Falle: Webadresse bereits in Nachricht sichtbar

The screenshot shows an email client interface. The email is from Jonas Schmidt <jonas.schmidt.78@web.de> with the subject "Vorschläge für den Retreat". The email content includes a greeting "Hallo Martin," and a request for feedback on two hotel alternatives. The URLs provided are <https://hotels.ab-in-den-urlaub.de/de/EUR/hotel/id432432> and <https://hotels.ab-in-den-urlaub.de/de/EUR/hotel/id784693>. A red warning triangle icon is placed to the right of the second URL. At the bottom, the address bar shows the URL <http://www.wasere.com/> circled in red. The interface also shows standard email actions like "Antworten", "Weiterleiten", "Archivieren", "Junk", "Löschen", and "Mehr".

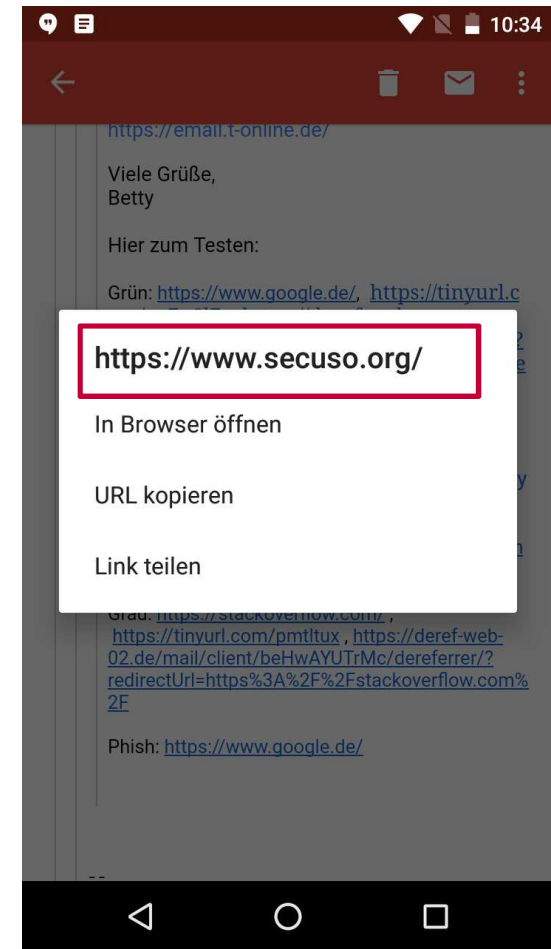


Welche Webadresse steckt hinter dem Link?



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?

<https://nophish.secuso.org/login>

Wer-Bereich

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?

Von Kundenservice <kundenservice@shopping-total.de> Antworten Weiterleiten
Betreff **Auftragsbestätigung** 16:28
An mich

Mein shopping total-Kundenportal



Hallo Martin Müller,

Ihre Auftrag ist bei uns eingegangen.

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

Vielen Dank für Ihr Vertrauen.

Ihr Mein shopping total-Kundenportal



https://www.shopping-total.de/host547.com/product/ADEKMKEDLE_ref=15468



Ist der Wer-Bereich plausibel?

Von Kundenservice <kundenservice@shopping-total.de> Antworten Weiterleiten
Betreff **Auftragsbestätigung** 16:28
An mich

Mein shopping total-Kundenportal


Hallo Martin Müller,

Ihre Auftrag ist bei uns eingegangen.

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

Vielen Dank für Ihr Vertrauen.

Ihr Mein shopping total-Kundenportal



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

https://www.shopping-total.de/sofortreich.de/product/ADEKMKEDLE_ref=1546



Ist der Wer-Bereich plausibel?

Von Kundenservice <kundenservice@shopping-total.de> Antworten Weiterleiten
Betreff **Auftragsbestätigung** 16:28
An mich

Mein shopping total-Kundenportal


Hallo Martin Müller,

Ihre Auftrag ist bei uns eingegangen.

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

Vielen Dank für Ihr Vertrauen.

Ihr Mein shopping total-Kundenportal



Andere Beispiele:
secure, trust, usw.



https://www.shopping-total.de/shoppingsicher.de/product/ADEKMKEDLE_ref=15468



Ist der Wer-Bereich plausibel?

Von Kundenservice <kundenservice@shopping-total.de> Antworten Weiterleiten
Betreff **Auftragsbestätigung** 16:28
An mich

Mein shopping total-Kundenportal


Hallo Martin Müller,

Ihre Auftrag ist bei uns eingegangen.

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

Vielen Dank für Ihr Vertrauen.

Ihr Mein shopping total-Kundenportal



https://www.shopping-total.de/shoppen-im-web.de/product/ADEKMKEDLE_ref=1546825&JASH/fi



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
- eurovings.de statt eurowings.de
- sparkasse-duesselclorf.de statt sparkasse-duesseldorf.de
- Otto.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?

Ist die Nachricht plausibel?

Ja

Sind die enthaltenen Webadressen plausibel?

Ja

Sind die Anhänge plausibel?

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?

Von MPS <kundenservice@mein-paketservice.de> Antworten Weiterleiten

Betreff **Auftragsbestätigung** 16:28

An mich

 **Mein Paketservice**


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.

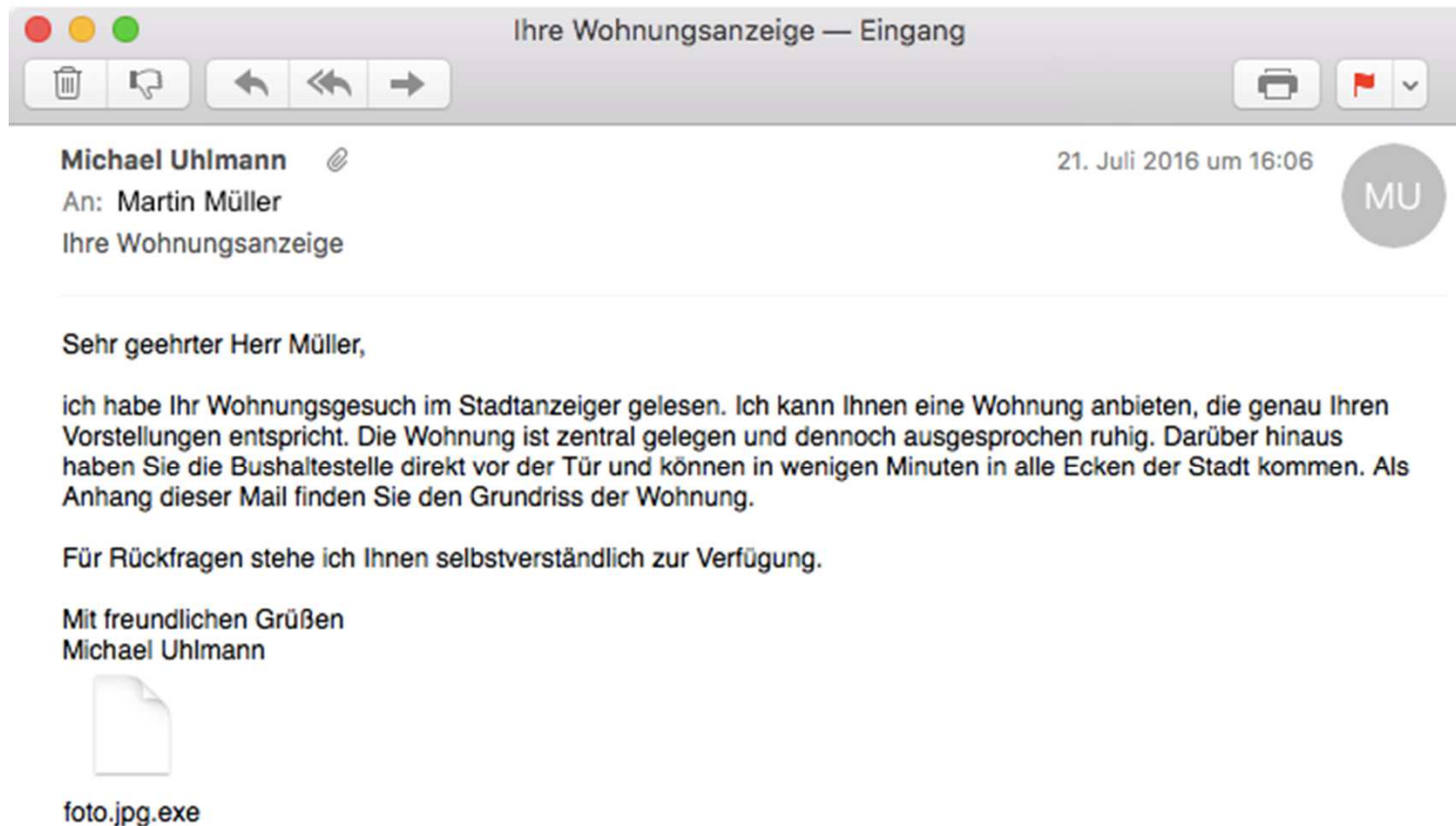
Vielen Dank für Ihr Vertrauen in Mein Paketservice.

Ihr Mein Paketservice

 **1 Anhang:** auftragsbestaetigung.exe 258 KB Speichern



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?

Unabhängig vom Nachrichtenformat

E-Mail

Messenger

Skype

WhatsApp

SMS

Soziale Netzwerke

Facebook

Google+

Berufliche Netzwerke

Xing

LinkedIn

Vermeintlicher Absender

Bekannte Personen

Bekannter Anbieter

Amazon, PayPal, Bank

...

Unbekannte Personen

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?

Von shopping-total.de Marketplace <marketplace@shopping-total.de> Antworten Weiterleiten

Betreff **Ein Geschenk für Sie** 16:28

An martin.mueller.77@web.de



Hallo Kunde,

als treuer Kunde möchten wir uns bei Ihnen bedanken.

Wenn Sie innerhalb der nächsten zwei Stunden nach dem Öffnen dieser E-Mail [hier](#) klicken, erhalten Sie einen kostenlosen eReader.

Ihr shopping-total Team



Psychologische
Tricks




Vertrauen Sie dieser E-Mail?

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

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.

Ihr Kundenservice



 https://www.1und1.de.shoppingsicher.de/product/ADKGHJWEKE_ref=1321423&JASH/refilogh/d43...



Vertrauen Sie dieser E-Mail?

Von explore friends <accounts@explore-friends.de>
Betreff Neues Gerät
An martin.mueller.77@web.de



explore-friends.de

Hallo Martin,

Ein neues Gerät wurde deinem explore friends-Benutzerkonto hinzugefügt:

Dienstag 25 Oktober 2016, 16:50 - UTC

explore friends für macOS

Hast du explore friends auf einem neuen Gerät installiert oder dich auf einem bestehenden Gerät erneut eingeloggt? Wenn dies nicht der Fall ist, gehe in der explore friends-App in die Einstellungen, entferne das Gerät und [setze dein Passwort zurück](#).

Das Team von explore friends

[Datenschutzrichtlinie](#) - [Missbrauch melden](#)

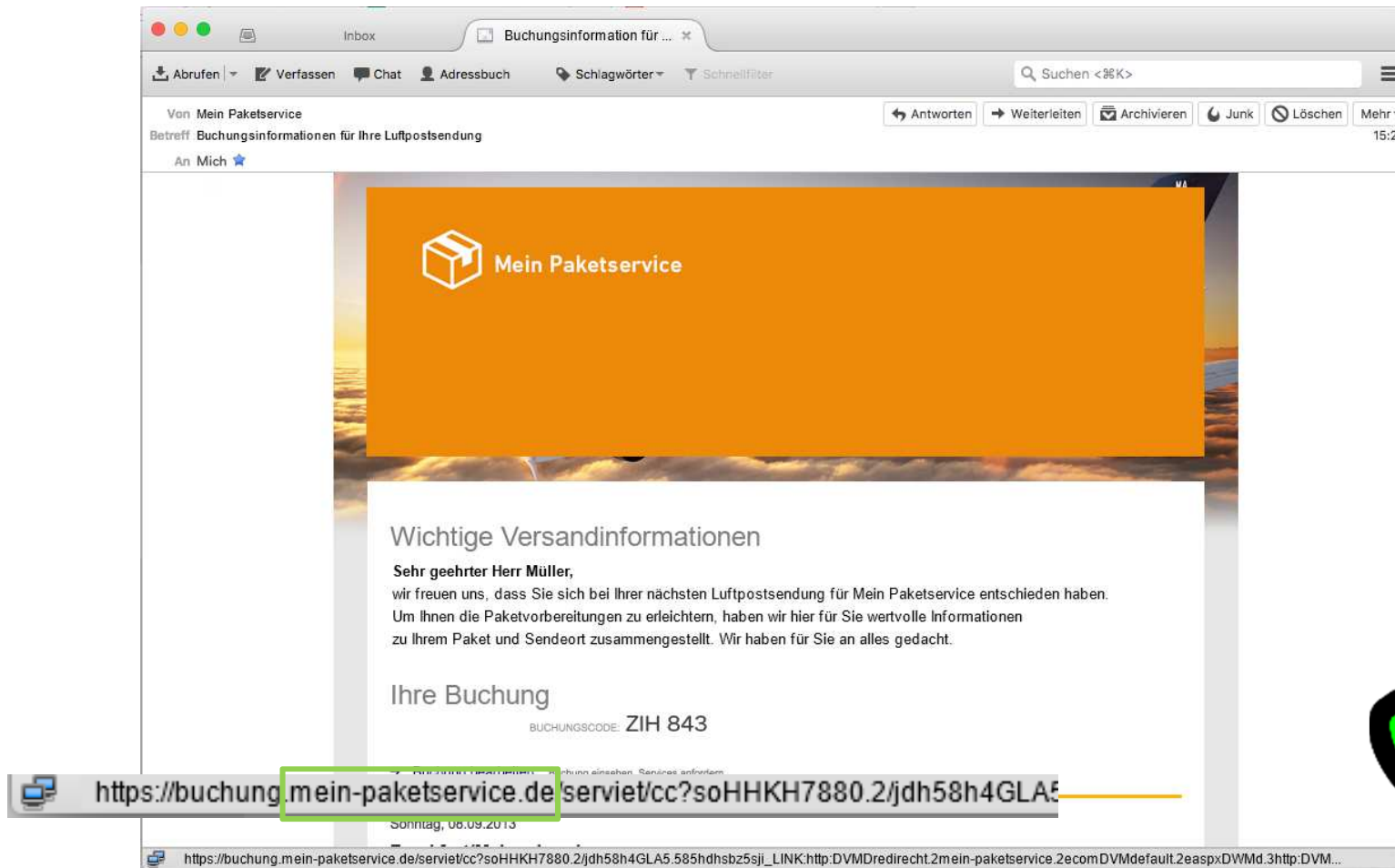
© 2017 explore friends GmbH. Alle Rechte vorbehalten.

 <https://www.explore-friends.de/host547.com/account>  14 Tagesplan





Vertrauen Sie dieser E-Mail?





Vertrauen Sie dieser E-Mail?

The screenshot shows an email interface with the following elements:

- Sender: **gewinnbestaetigung@host547.com**
- Recipient: **An: Martin Müller**
- Subject: **Ihre Newsletter Anmeldung**
- Header: **Mein Shopping-Kundenportal**
- Progress bar: **Ihre Newsletter Anmeldung** (100% complete)
- Steps: **1 Dateneingabe**, **2 E-Mail-Bestätigung**, **3 Weitere Optionen**
- Image: A woman smiling while using a tablet.
- List of benefits:
 - Aktuelle Angebote
 - Tolle Gewinnspiele
 - Wertvolle Shoppingtips
 - Exklusive Partnerinformationen
 - Ptimiert für PC und Smartphone
- Text: **Sehr geehrter Herr Müller,**
- Text: **Ein kleiner Tipp**
- URL: **<https://www.newsletter.shopping-total.de/bestaetigung/7346>** (highlighted with a red box)
- Text: **Speichern Sie die shopping-total**
- Text: **Die sichersteigenen, dass im Newsletter nicht**
- Text: **versehentlich im Spam landet.**

A large red 'X' is overlaid on the right side of the email content, indicating a security warning or lack of trust.



Vertrauen Sie dieser E-Mail?


The screenshot shows an email interface with the following content:

martin.mueller.1977 aktivieren — Eingang

explore friends <no-reply@explore-friends.de> Heute um 12:34

An: Martin Müller

Sie haben ein Android-Gerät mit explore friends verbunden.



Hallo,

Sie haben ein Android-Gerät mit explore friends verknüpft. Super!

Sie können dieses und jedes andere verbundene Gerät auf Ihrer [Kontoseite](#) überprüfen.

<https://www.explore-friends.de//0Gn8kh89gTFZAK78knHbHKH>

Frohes Explorieren!
Das explore friends Team

P.S. Wenn Sie diese Änderung nicht vorgenommen haben, [benachrichtigen Sie uns bitte](#).

© 2017 explore friends

<https://www.explore-friends.de//0Gn8kh89gTFZAK78knHbHKH>

A large green checkmark with a black outline is positioned to the right of the email content, pointing towards the URL.



Vertrauen Sie dieser Nachricht?



Wenn Nachricht für Sie plausibel, dann



Wenn Nachricht für Sie NICHT plausibel, dann





Materialien für Sensibilisierung, Schulungen und Werkzeuge

Allgemeines über Phishing
Der Begriff Phishing steht für den Versuch, mit Hilfe von gefälschten Nachrichten (z. B. E-Mails, sozialen Netzwerken oder Skype, aber auch QR-Codes) Schadsoftware o. B. Virenladungen oder an Daten von Internetnutzern zu gelangen. Bei diesen Daten kann es sich z. B. um Passwörter, Konten- und Kreditkartennummern oder Transaktionsnummern (TANs) handeln. Internetbetrüger erheben diese Daten, um sich finanziell zu bereichern oder auch um Identitätsfälschung zu betreiben.

Hinweis
Die Inhalte des Flyers adressieren die derzeit am weitesten verbreiteten Phishing-Typen. Der Fokus liegt dabei auf der Erkennung von Phishing-URLs.

Mehr Infos und die NoPhish App:
<https://www.secuso.org/nophish>

Kontakt
SECUSO (Security, Usability & Society)
Technische Universität Darmstadt
Fachbereich Informatik
Prof. Dr. Melanie Volkamer
Gebäude 5414
Hornwegstraße 30
64279 Darmstadt
<https://www.facebook.com/secuso>
<https://twitter.com/secuso>

NoPhish
Die Anti-Phishing-Schulung

SECUSO
KMUWARE
IT-Sicherheit

Ist diese Nachricht betrügerisch?

shopping-total.de
Zustellung Ihrer Bestellung
Hallo Max Müller,
Ihre Bestellung konnte nicht zugestellt werden.
Klicken Sie hier, um gemeinsam mit uns eine Lösung zu finden.
Vielen Dank für Ihren Besuch bei shopping-total.de

Ja Nein

SECUSO

Einführung 1
Einführung und Erklärung

Navigation icons at the bottom.

ONLINE-BETRUG

Gefahren erkennen & abwehren

- 1) Identifizieren Sie die tatsächliche Wer-Bereich. Achten Sie nur auf den Wer-Bereich, erklärt, wie man sich schützen kann.
- 2) Geben Sie bei IP-Adressen keine Daten
✗ <https://95.130.22.98/google.de/sec>
- 3) Lassen Sie sich nicht von Webadressen verleiten, die den Namen der Institution außerhalb des Wer-Bereichs enthalten.
✗ <https://www.amazon.de/shoppen-im-web>
✗ <http://shoppen-im-web.de/https://www.immobilienscout24.de>
- 4) Prüfen Sie den Wer-Bereich in Bezug auf die URL.
✗ <https://www.mediarnark.de/>
- 5) Prüfen Sie den Wer-Bereich genau hinsichtlich der aussehenden Zeichen und Zahlen.
- 6) Prüfen Sie, ob der Wer-Bereich nur ein Zeichen enthält.
✗ <https://de-de.facebook-secured.com>

www.secuso.org/login

Wer-Bereich

SECUSO

Übersicht

Einführung	Level 1	Level 2
Level 3	Level 4	Level 5
Level 6	Level 7	Level 8



Wenn Sie mehr Wissen möchten

Links:

Web Training

<https://nophish-web.secuso.org>

Android App

Erhältlich im Google Play Store

Add-On für Thunderbird, das 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



TECHNISCHE
UNIVERSITÄT
DARMSTADT



CYSEC

Dr. Marco Ghiglieri

Wissenschaftlicher Mitarbeiter
marco.ghiglieri@secuso.org

Benjamin Reinheimer

Wissenschaftlicher Mitarbeiter
benjamin.reinheimer@secuso.org