



SECUSO
SECURITY · USABILITY · SOCIETY

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



Prof. Dr. Melanie Volkamer
Dr. Marco Ghiglieri



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?

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

Hallo,

SecurePay 

Herzlicher
du da. Als
Bitte klicke

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

E-Mail-Adresse bestätigen

Danke
Dass SecurePay24-Team



Vertrauen Sie dieser E-Mail?



Vertrauen Sie dieser E-Mail?

The screenshot shows a Gmail inbox on a desktop browser. The email subject is "Ihr Mein Paketservice - Tarifwechsel beauftragt". The sender is "Mein Paketservice Control-Center" with a URL <https://control-center.mein-paketservice.de>. The email content includes a breadcrumb trail: "Mein Vertrag > Leistungsbeschreibung > Preisliste", followed by "Service und Kontakt" and a paragraph: "In Ihrem Mein Paketservice Hilfe-Center gibt es nützliche Informationen und Tipps rund um die Produkte und Leistungen von Mein Paketservice. Schauen Sie einfach". A red arrow points from the URL in the email body to the URL in the sender information. A context menu is open over the sender information, listing "Kontakte", "Gmail", "In der Inbox gruppiert", "Reisen", and "Gespeichert". At the bottom of the context menu, there is a link: ".https://control-center.mein-paketservice.de" in neuem Tab öffnen. The browser address bar shows "inbox.google.com".

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.

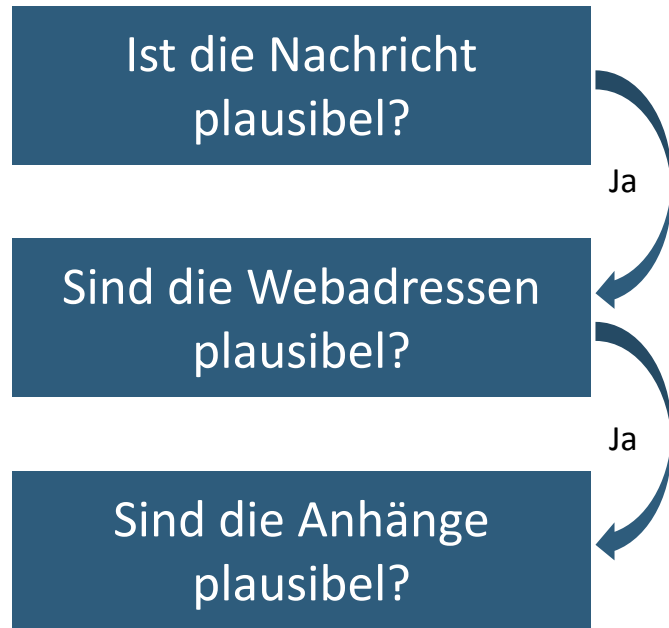
Wenn Sie innerhalb der nächsten zwei Stunden nach dem Öffnen dieser E-Mail [hier](#) klicken, erhalten Sie einen kostenlosen eReader.

Ihr shopping-total Team

Psychologische
Tricks

Wie erkennt man gefährliche Nachrichten?

Wie?

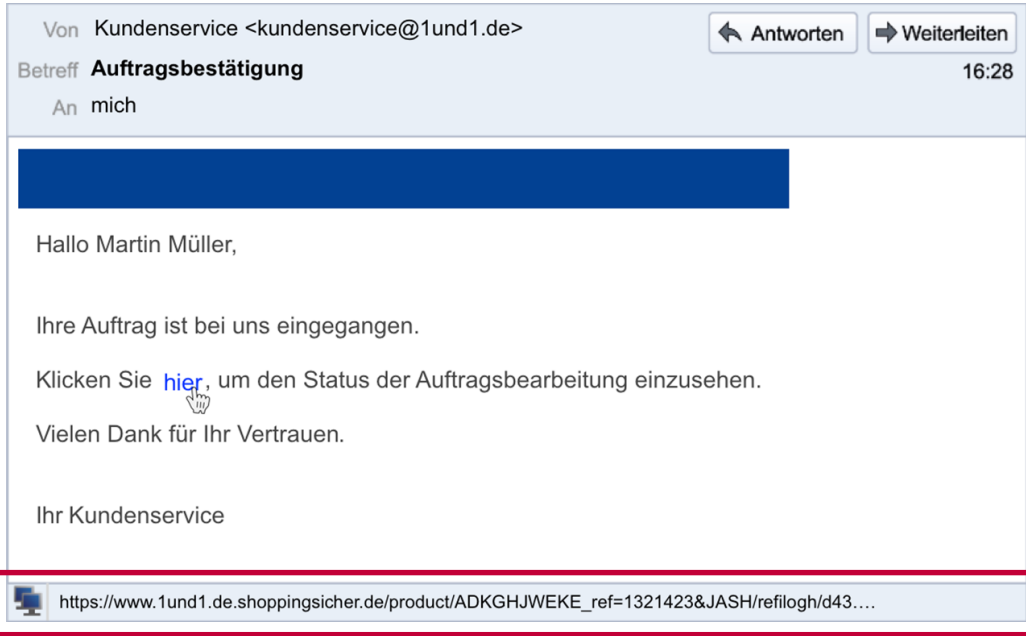


- Absender passt zum Inhalt der Nachricht?
- Richtige Webadresse identifizieren
- Identifizieren Sie den „Wer-Bereich“
- Ist „Wer-Bereich“ plausibel?
- Anhang identifizieren
- Identifizieren Sie das Dateiformat
- Erwarten Sie den Anhang vom Absender?



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

Welche Webadresse steckt hinter dem Link?



Von Kundenservice <kundenservice@1und1.de>

Betreff **Auftragsbestätigung** 16:28

An mich

Hallo Martin Müller,

Ihre Auftrag ist bei uns eingegangen.

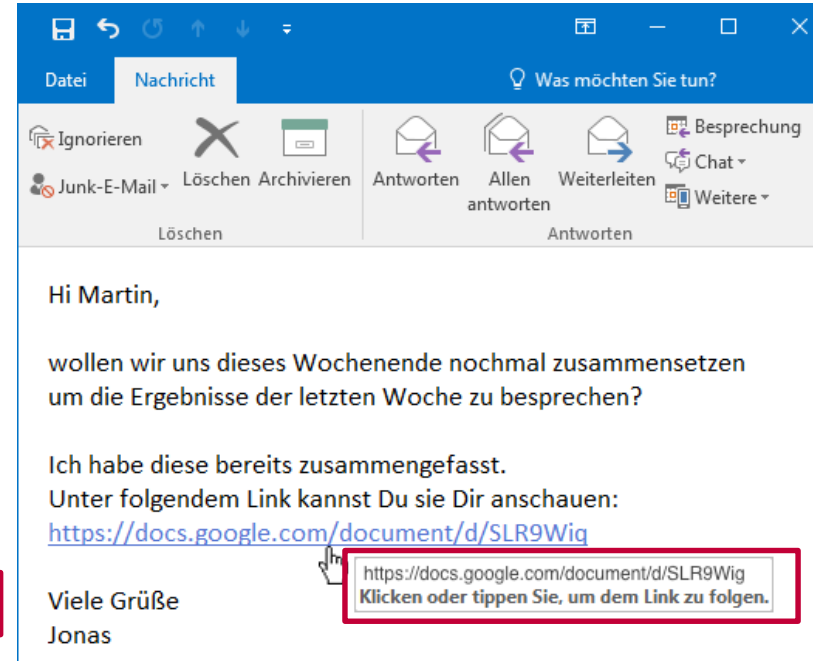
Klicken Sie [hier](#), um den Status der Auftragsbearbeitung einzusehen.

Vielen Dank für Ihr Vertrauen.

Ihr Kundenservice

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

Statusleiste
(z.B. Thunderbird)



Hi Martin,

wollen wir uns dieses Wochenende nochmal zusammensetzen um die Ergebnisse der letzten Woche zu besprechen?

Ich habe diese bereits zusammengefasst.
Unter folgendem Link kannst Du sie Dir anschauen:
<https://docs.google.com/document/d/SLR9Wig>

Viele Grüße
Jonas

<https://docs.google.com/document/d/SLR9Wig>
Klicken oder tippen Sie, um dem Link zu folgen.

Tooltip
(z.B. Outlook)



Vorsicht Falle: Falscher Tooltip

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

Subject **Meeting Minutes**

21:55

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 ch

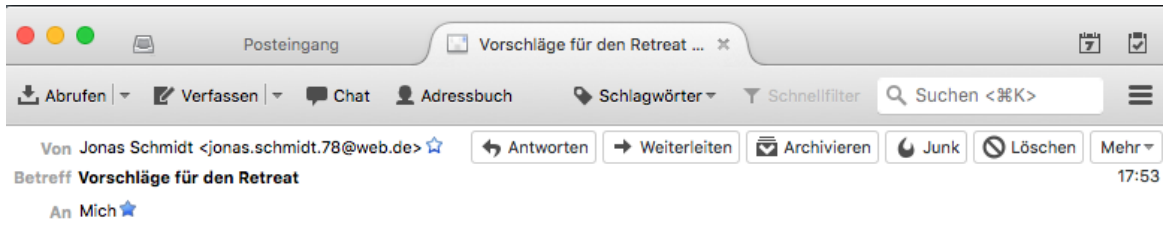
Click here
<https://www.ourworkspace.com/doc=288291/edit>

Best.
Jonas



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

Vorsicht Falle: Webadresse bereits in Nachricht



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

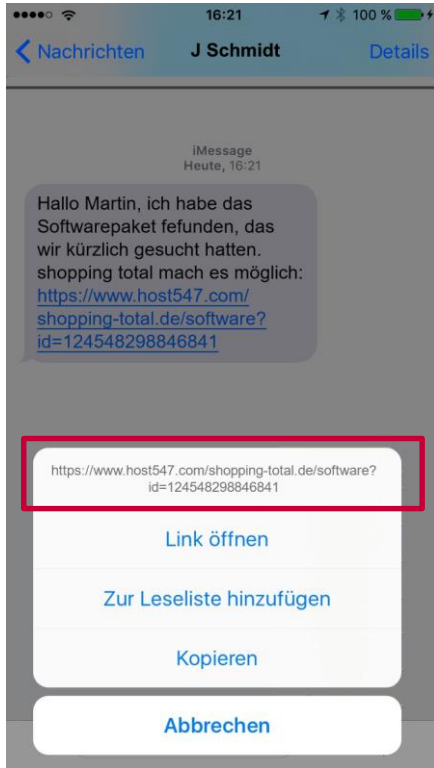


<http://www.wasere.com/>

87%

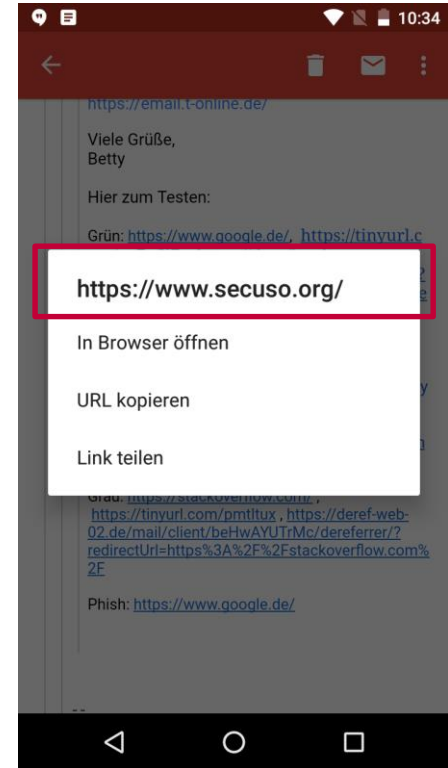
Tagesplan

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.shopping-total.de/login>

Wer-Bereich

<https://www.shopping-total.de.secure.de.host547.com>

<https://host547.com/www.shopping-total.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=1546825&JASH/filog...

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/sofortreich.de/product/ADEKMKEDLE_ref=1546825&JASH/filog...

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

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/shoppingsicher.de/product/ADEKMKEDLE_ref=1546825&JASH/filog...

Andere Beispiele:
secure, trust, usw.



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/filog...

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

- 1linkedin.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



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

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

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!

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

Psychologische Tricks:
Zeitdruck, Emotionen, etc.

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!



Materialien für Sensibilisierung, Schulungen und Werkzeuge

1. Regel: Prävention
 Nachrichten, wenn sie **schrieblich** überträgt ein **Wort**, verschwindet sie rasch, um **bei** zu löschen Sie **erst** -man zu **schaden** -Mitarbeiter
 ✓ Der Absender **shop@reze** ja **übrig** von **Schadstoffware** nicht **plausibel**.
 ✗ Der Absender **rechnung@amazon.de** mit **gefä** - Amazon **E-Mail** **plausibel**.

2. Regel: Wenn Absender und Inhalt einer Nachricht **er** - erkennen und die **Nachricht** **ein** **Link** enthält, **prüfen** Sie, **es** **sich** **von** **einer** **gut** **ge** - **gemein** **gef** - **ährliche** **Nachricht** **behandeln**, **und** **die** **Nachricht** **zu** **ger** - **nicht** **vor** **dem** **technischen** **Absender** **kommen**. **Dass** **müssen** **Sie** **zunächst** **heraus** **finden**, **welche** **Webadresse** **tatsächlich** **hinter** **dem** **Link** **steckt**, **bevor** **Sie** **darauf** **klicken**.

Die **Information**, **welche** **Webadresse** **tatsächlich** **hinter** **einem** **Link** **steckt**, **ist** **je** **nach** **Gerät**, **Software** **und** **Dienst** (z. B. **Amazon**, **Dropbox**, **Slack**, **WhatsApp**, **Facebook**, **Google**, **King**, **LinkedIn**) **unterschiedlichen** **Stellen** **zu** **finden**. **Sie** **sollten** **sich** **also** **vor** **der** **Historie** **einer** **Seite**, **einer** **Software** **oder** **eines** **Dienstes** **damm** **vertrauen** **machen**, **wo** **die** **tatsächliche** **Webadresse** **eines** **Links** **zu** **finden** **ist**. **Ein** **Link** **kann** **meist** **den** **er** - **kennt** **werden**, **dass** **der** **Text** **das** **hinterlegt** **und** **unterschiedlich** **ist**.

Bei **PCs** **und** **Ma** - **weis** **Sie** **mit** **Klick** - **en**, **Das** **4** **Fenster**, **das** **wird** **er** - **öffnet** **werden**.

Online-Betrug
 Wie Sie gefährliche Nachrichten im Internet erkennen können

ONLINE-BETRUG
 Gefahren erkennen & abwehren

- Modul 1: Einführung in das Thema „Phishing und andere gefährliche Nachrichten“**
- Modul 2: Erkennung von gefährlichen Nachrichten, die unplausibel sind**
- Modul 3: Erkennung von Nachrichten mit gefährlichen Links**
- Modul 4: Erkennung von Nachrichten mit gefährlichen Inhalten**

Die einzelnen Module können durch **Phishing-Schulung** erklärt, wie man sich **SECUSO** **Wer-Bereich**

- 1) Identifizieren Sie die **tatsächliche Webadresse**. Achten Sie nur auf den **Wer-Bereich**.
 ✗ <https://95.130.22.98/google.de/secure>
- 2) Geben Sie bei **IP-Adressen** keine Daten ein.
 ✗ <https://www.amazon.de/shoppen-im-web>
- 3) Lassen Sie sich nicht von Webadressen der Name der Institution außerhalb der Webadresse verleiten.
 ✗ <http://shopen-im-web.de/https://www.immobilienscout24.de>
- 4) Prüfen Sie den **Wer-Bereich** in Bezug auf **aussehende Zeichen und Zahlen**.
 ✗ <https://www.mediamarkt.de/>
- 5) Prüfen Sie, ob der **Wer-Bereich** nur ein **aussehendes Zeichen** ist. Bei Unsicherheit befragen Sie den **Wer-Bereich**.
 ✗ <https://de-de.facebook-secured.com>

Ist diese Nachricht betrügerisch?

shopping-total.de
 Mein Konto | shopping-total.de

Hallo Herr Müller!

Ihre Bestellung könnte 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

Einführung 1
 Einführung und Erklärung

Einführung 1

Übersicht

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



Video

Link zum Video

<https://secuso.org/video>

Weitere Materialien und Tools

- Ausführliche Schulungsunterlagen, Motivationsposter und Quizze: <https://secuso.org/schulung>
- Spiele-Apps zur Erkennung betrügerischer Links: <https://secuso.org/nophish>
- Tools zur Unterstützung der Erkennung betrügerischer Nachrichten:
 - TORPEDO: <https://secuso.org/torpedo>
 - PassSec+: <https://www.secuso.org/passec>



PassSec⁺

TORPEDO



Ihre Ansprechpartner



Technische Universität
Darmstadt
SECUSO



Prof. Dr. Melanie Volkamer

Leiterin SECUSO

melanie.volkamer@secuso.org

Dr. Marco Ghiglieri

Wissenschaftlicher Mitarbeiter

marco.ghiglieri@secuso.org