POLIZEI
Nordrhein-Westfalen
Düsseldorf

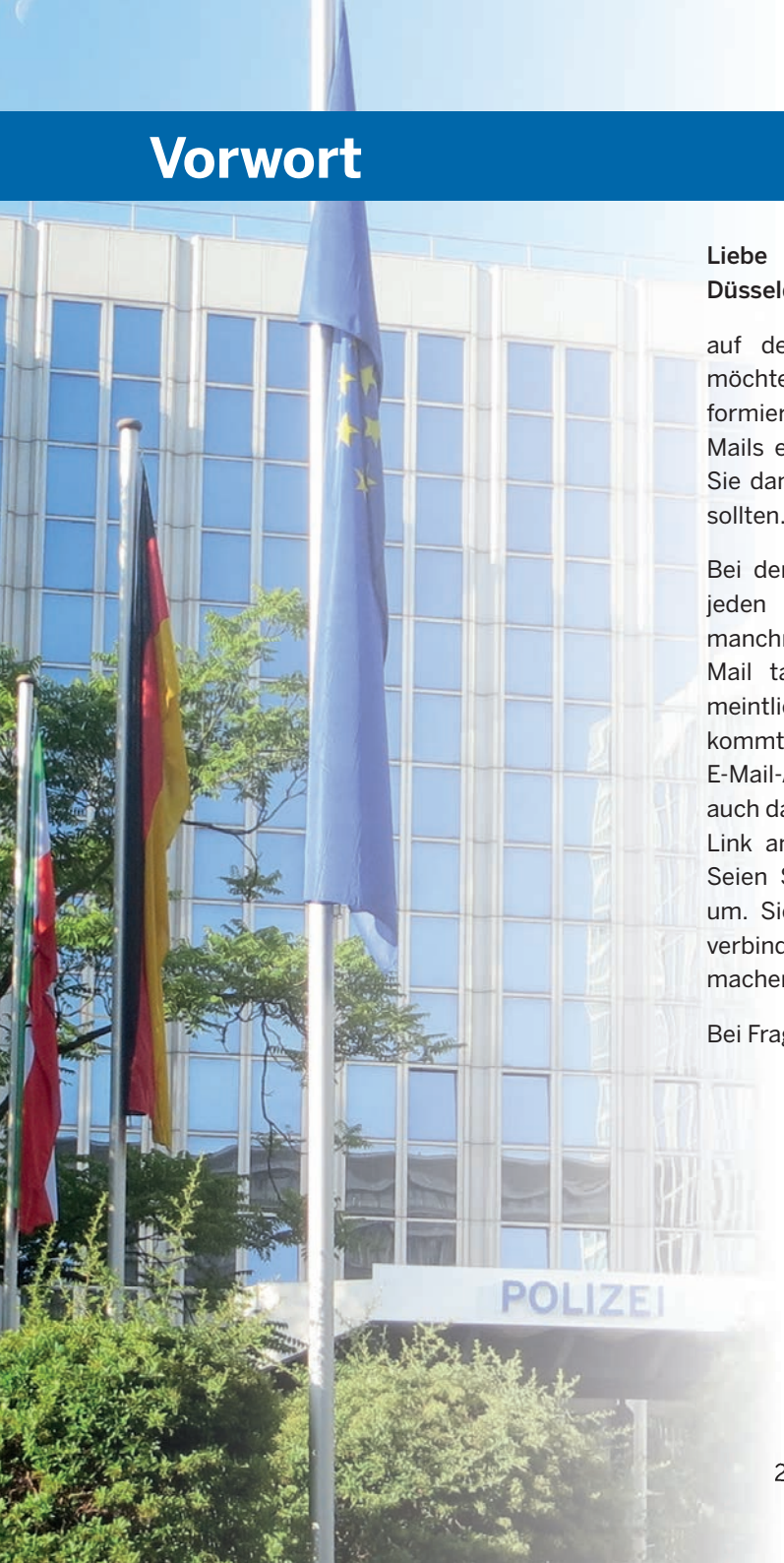
bürgerorientiert · professionell · rechtsstaatlich


Polizeipräsidium Düsseldorf · Kommissariat Kriminalprävention/Opferschutz

# Präventionshinweise für Bürgerinnen und Bürger
## Ausgabe 8

# „Fake-Mails/Phishing-Mails“

# Vorwort




**Liebe Düsseldorferinnen und Düsseldorfer,**

auf den nachfolgenden Seiten möchten wir Sie gerne darüber informieren, wie Sie betrügerische Mails erkennen können und was Sie dann auf keinen Fall machen sollten.

Bei der Flut der Mails, die man jeden Tag erhält, achtet man manchmal nicht darauf, ob eine Mail tatsächlich von dem vermeintlich bekannten Absender kommt. Immer wieder stammen Mails sogar von Bekannten, deren E-Mail-Account offenbar übernommen wurde. Achten Sie also bitte auch darauf, dass Sie sich bei Ihrem E-Mail-Provider niemals über einen Link anmelden, sondern immer die Original-Anmeldeseite aufrufen. Seien Sie bitte vorsichtig und gehen Sie sparsam mit ihren Daten um. Sie würden auch keinem Fremden auf der Straße ihre Kontoverbindung nebst Passwort für das Online-Banking geben – daher machen Sie das bitte auch nicht im Netz.

Bei Fragen stehen wir Ihnen sehr gerne zur Verfügung.

**Susanna Heusgen,**
**Leiterin der Kriminalprävention**

# Wie erkenne ich Fake-Mails/ Phishing-Mails?

Immer wieder liest man in den Nachrichten oder in den sozialen Medien von Phishing-Mails. Doch was ist das und wie erkenne ich diese? Wieso sind Sie im Umlauf und wie kann ich mich davor schützen?

Phishing-Mails sind E-Mails, die Betrüger in der Hoffnung versenden, Daten von Ihnen abgreifen zu können. Dabei kann es sich um Ihren Klarnamen handeln oder sensiblere Daten, wie Kontodaten oder Passwörter zu Postfächern oder Online-Banking-Zugängen. Sie können beispielsweise aussehen wie Mails Ihrer Hausbank oder eines bekannten Onlineshops.

**Doch wie kann ich Richtig von Falsch unterscheiden? Hier müssen wir uns ein paar Details ansehen.**

Fangen wir oben an. Schauen Sie zunächst auf den **Absender:**

DA Deutsche AG Kundenservice (accoureplyxecl@netzwelt.api.bsfonline.com.br)
05.07.23, 13:39 Uhr

**Kennen Sie die Deutsche AG?** Oder was soll das kryptische „*accoureplyxecl*“ im Absender bedeuten?

**Haben Sie Kontakte in Brasilien?** Denn ***.br*** ist die länderspezifische Top-Level-Domain Brasiliens. Haben Sie eine der Fragen mit ´**Nein**´ beantwortet, so sollten Sie an dieser Stelle weiter misstrauisch bleiben.

POLIZEI
Nordrhein-Westfalen
Düsseldorf

Gehen wir also ein paar Zeilen runter und schauen uns die **Anrede** an:

Sehr geehrter Kunde,

Wenn der Absender auf Grund eines **bestehenden Kundenkontos** Ihren **Namen** kennen müsste, so können Sie davon ausgehen, dass dieser Sie auch mit diesem anreden würde.

**Hier wird zudem ein wichtiger Punkt angesprochen:**

**Sind Sie denn überhaupt Kunde?** Haben Sie ein Bankkonto bei dieser Bank oder besitzen Sie ein Kundenkonto bei diesem Onlineshop?

Im weiteren Verlauf der Mail werden Sie dazu aufgefordert, auf einen Link zu klicken und Ihre **Zugangsdaten** zu verifizieren. **Mit dieser Eingabe öffnen Sie den Betrügern Tür und Tor.**

Wenn Sie heute nicht handeln, können Sie die Transaktion nicht mehr stornieren.

Hier sollen Sie in **Angst und Schrecken** versetzt werden, das heißt schnell handeln, ohne gar nicht richtig darüber nachzudenken, ob das jetzt wirklich Not tut. Immer wenn Sie einen solchen Satz sehen, bleiben Sie skeptisch.

**Haben Sie eine Transaktion veranlasst?**
**Haben Sie etwas gekauft, was eine Transaktion rechtfertigt?**

# Fake-Mails/Phishing-Mails

Wir warten auf Ihre Antwort-E-Mail, um Ihnen mitzuteilen, wie Sie weiter vorgehen sollen...
* Bitte senden Sie Ihre Antwort an die unten angegebene E-Mail-Adresse der Abteilung:
* diepolizei128@gmail.com

Sollen Sie jedoch eine **Antwort-Mail** verfassen (hier an einem anderen Beispiel einer Betrugsmail, welche angeblich von der Bundespolizei verfasst wurde), damit näherer Kontakt und Vertrauen zu den Betrügern aufgebaut werden kann, **so überprüfen Sie die E-Mail-Adresse!**

***Die Polizei hat sicherlich keine „@gmail.com"-Adresse, das können wir Ihnen versprechen.***

Mr [redacted]
Polizeidirektor
---
- [redacted] POLIZEIINSPEKTION
[redacted] BRIGADE FÜR DEN
JUGENDSCHUTZ

**Kommt Ihnen dieser Abschluss einer Mail auch komisch vor?** Uns auch! Da es sich angeblich um eine Person innerhalb einer deutschen Polizeibehörde handelt, wieso wird hier die englische Form („Mr.") gewählt? In dem Schwarzen Feld wird ein Name stehen, welcher unter Umständen sogar im polizeilichen Kontext verortet werden kann. Dies soll im ersten Moment Vertrauen schaffen und Sie veranlassen, den möglichen Anschuldigungen gegen Sie Glauben zu schenken.

**Zudem sei so viel verraten, dass es bei der Polizei keine „Brigade" für den Jugendschutz gibt.**

**POLIZEI**
**Nordrhein-Westfalen**
**Düsseldorf**

Doch was nun? Sind bereits Daten in die Hände der Betrüger gelangt?

Um auf Nummer sicher zu gehen, sollten Sie in jedem Fall das Passwort Ihres E-Mail-Postfachs ändern!
Beachten Sie dabei die Richtlinien für ein sicheres Passwort, beispielsweise des LKA NRW **(https://www.mach-dein-passwort-stark.de/).**

Wenn Sie sich noch nicht ganz sicher sind, ob es sich bei der versendeten E-Mail um eine Phishing-Mail handelt, informieren Sie sich über das Unternehmen mit Hilfe einer Suchmaschine und rufen Sie den Absender an.

**Antworten Sie niemals auf eine Mail oder klicken auf einen Link aus einer unsicheren Quelle.**

**Überweisen Sie in keinem Fall Geld aus einem unsicheren Gefühl heraus.** Versichern Sie sich lieber zweimal, ob die Überweisung wirklich von Nöten ist.

Gerne können Sie bei Unsicherheit oder Fragen die Präventionsstelle der Polizei zum Thema Cybercrime kontaktieren und sich beraten lassen:

**https://duesseldorf.polizei.nrw/artikel/cybercrime-2**

**Frau Liersch: 0211-870 68 65**

**KKKP-O.Duesseldorf@polizei.nrw.de**

## Impressum

**Herausgeber**
Polizeipräsidium Düsseldorf
Kommissariat Kriminalprävention/Opferschutz



Luegallee 65
40545 Düsseldorf
Tel.: 0211 - 870 5249
E-Mail: KKKP-O.Duesseldorf@polizei.nrw.de