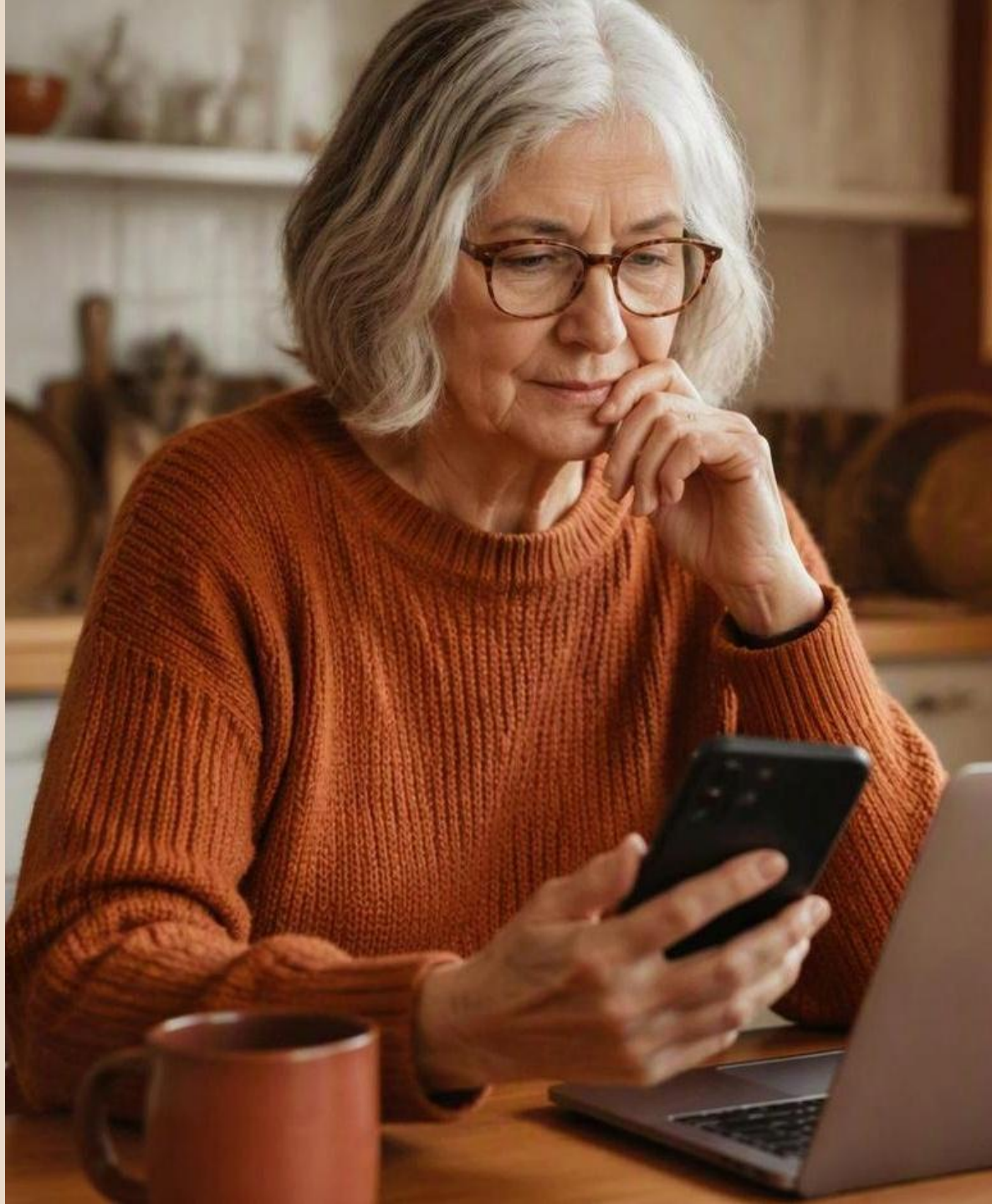
Betrug beginnt mit Zeitdruck.

Und endet oft mit einem falschen Klick.

Phishing, Smishing, Telefonbetrug & Co.
Sicher erkennen.
Ruhig prüfen. Richtig handeln.



Was meinen Sie?

Wie viele Menschen in Deutschland waren innerhalb der letzten 12 Monate Opfer von Cyberkriminalität?

Etwa jeder zehnte Mensch in Deutschland war innerhalb eines Jahres von Cyberkriminalität betroffen.

Quelle: Polizeiliche Kriminalprävention (11.05.2026)

Wie viele Euro Schaden verursachen Betrüger jedes Jahr durch Enkeltrick, Schockanrufe, Internetbetrug und ähnliche Maschen in Deutschland??

Rund 200 Milliarden Euro pro Jahr!

Quelle: Bundeslagebild Cybercrime 2025

ORIENTIERUNG

Heute geht es um drei Fragen

1 Erkennen — Welche Warnzeichen tauchen immer wieder auf?

2 Prüfen — Wie kontrollieren Sie eine Nachricht ohne Risiko?

3 Handeln — Was tun Sie vor, und nach einem falschen Klick?

Online-Betrug ist kein Randthema.

11 %

wurden innerhalb eines Jahres Opfer einer Straftat im Internet

88 %

der Betroffenen berichten von einem Schaden

33 %

der Betroffenen erlitten einen finanziellen Verlust

Betroffenheit ist häufig — Schuld liegt immer bei den Tätern.

Quelle: Cybersicherheitsmonitor 2026 von BSI und Polizeilicher Kriminalprävention

DIE STOPP-REGEL

Die 10-Sekunden-Pause ist Ihr stärkstes Werkzeug

S – Stopp Nichts anklicken.

T – Tief durchatmen Keinen Zeitdruck akzeptieren.

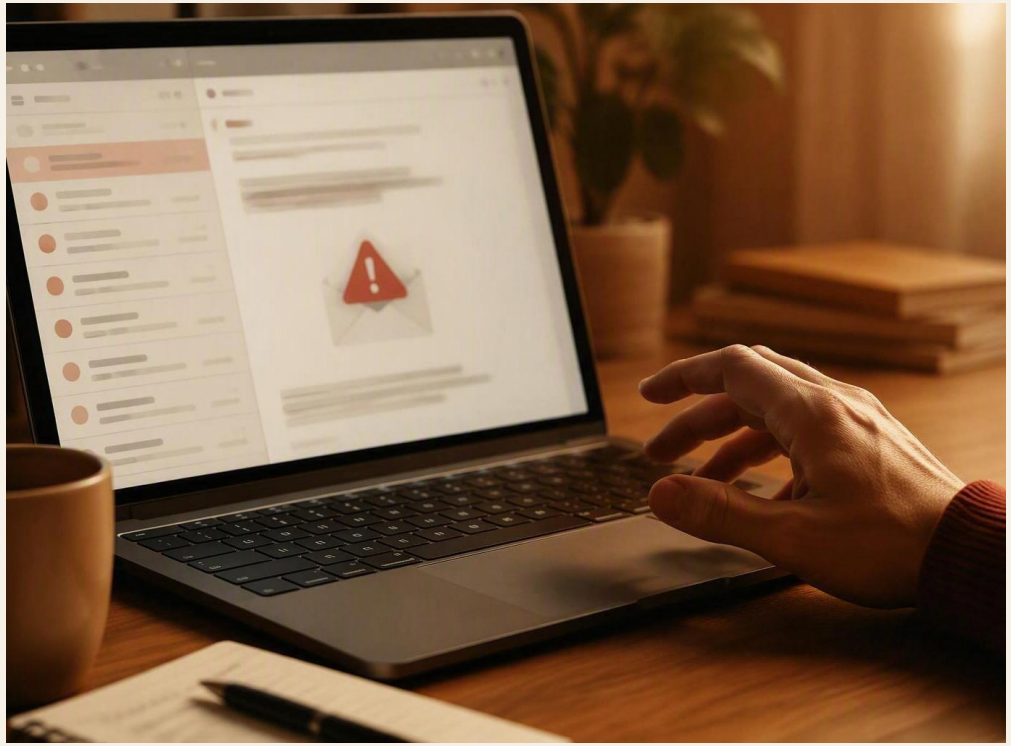
O – Original prüfen Ist die Nachricht überhaupt echt?

P – Prüfen Über einen bekannten und sicheren Kontaktweg nachfragen

P – Problem melden Wenn etwas verdächtig ist, melden.

E-MAIL

Phishing-Mails verraten sich durch Absender, Druck und Links

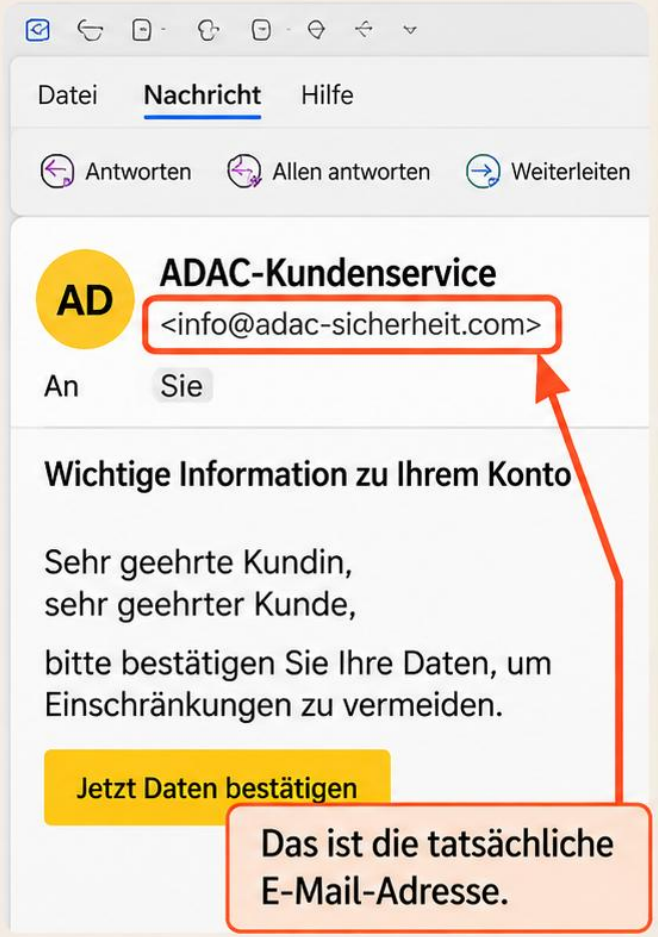


- **Absender**
  Nicht nur den angezeigten Namen, sondern die vollständige Adresse prüfen.
- **Druck**
  Frist, Sperre oder Drohung sind Gründe zum Innehalten.
- **Link**
  Nicht öffnen. Die bekannte Website selbst eintippen oder Favorit nutzen.

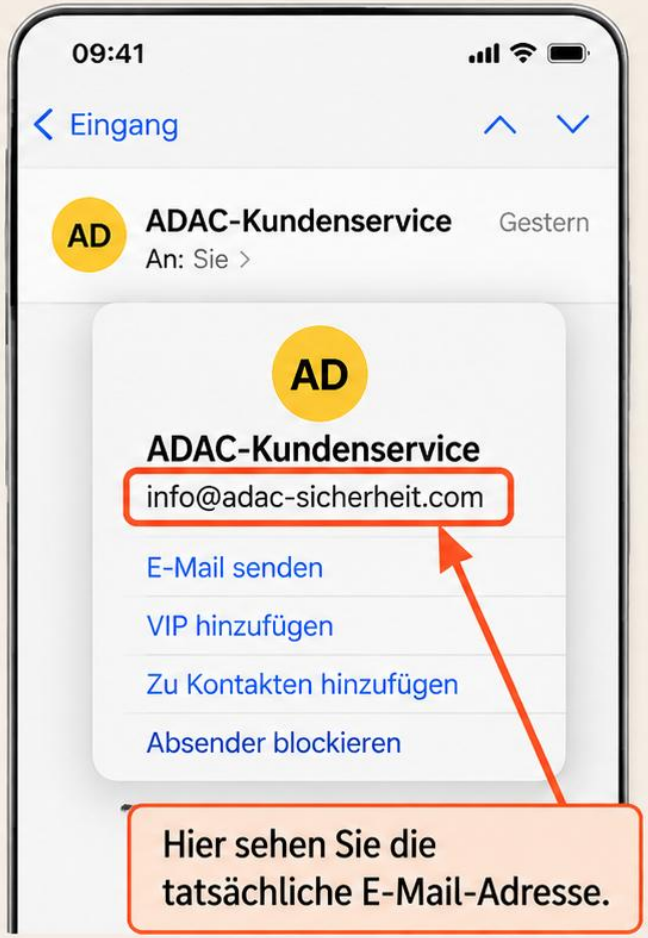
Quelle: BSI – Phishing erkennen und richtig handeln

Phishing-Mails Beispiele #1

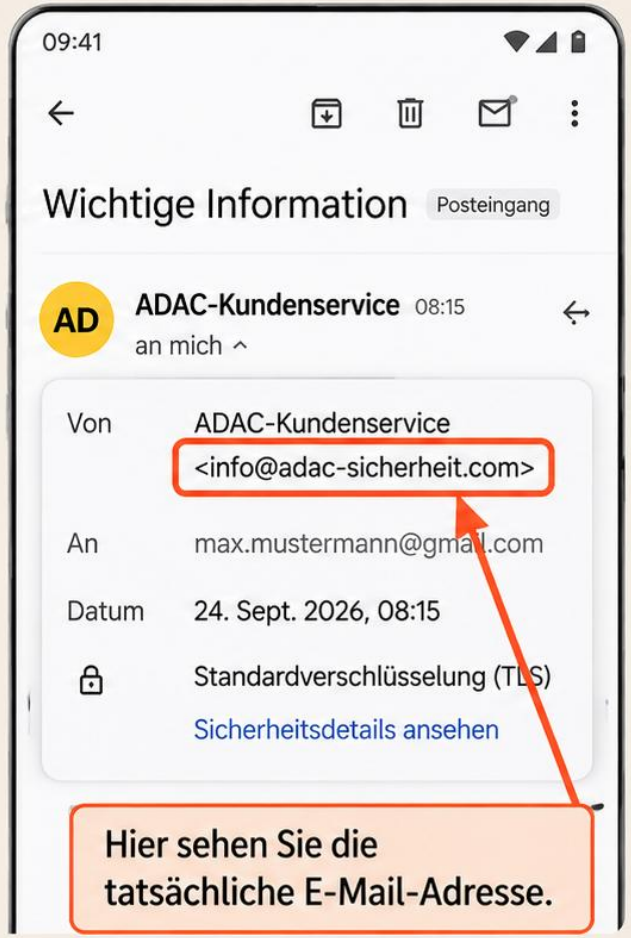
1. Am PC (z. B. Outlook)



2. Am Smartphone (z. B. iPhone)

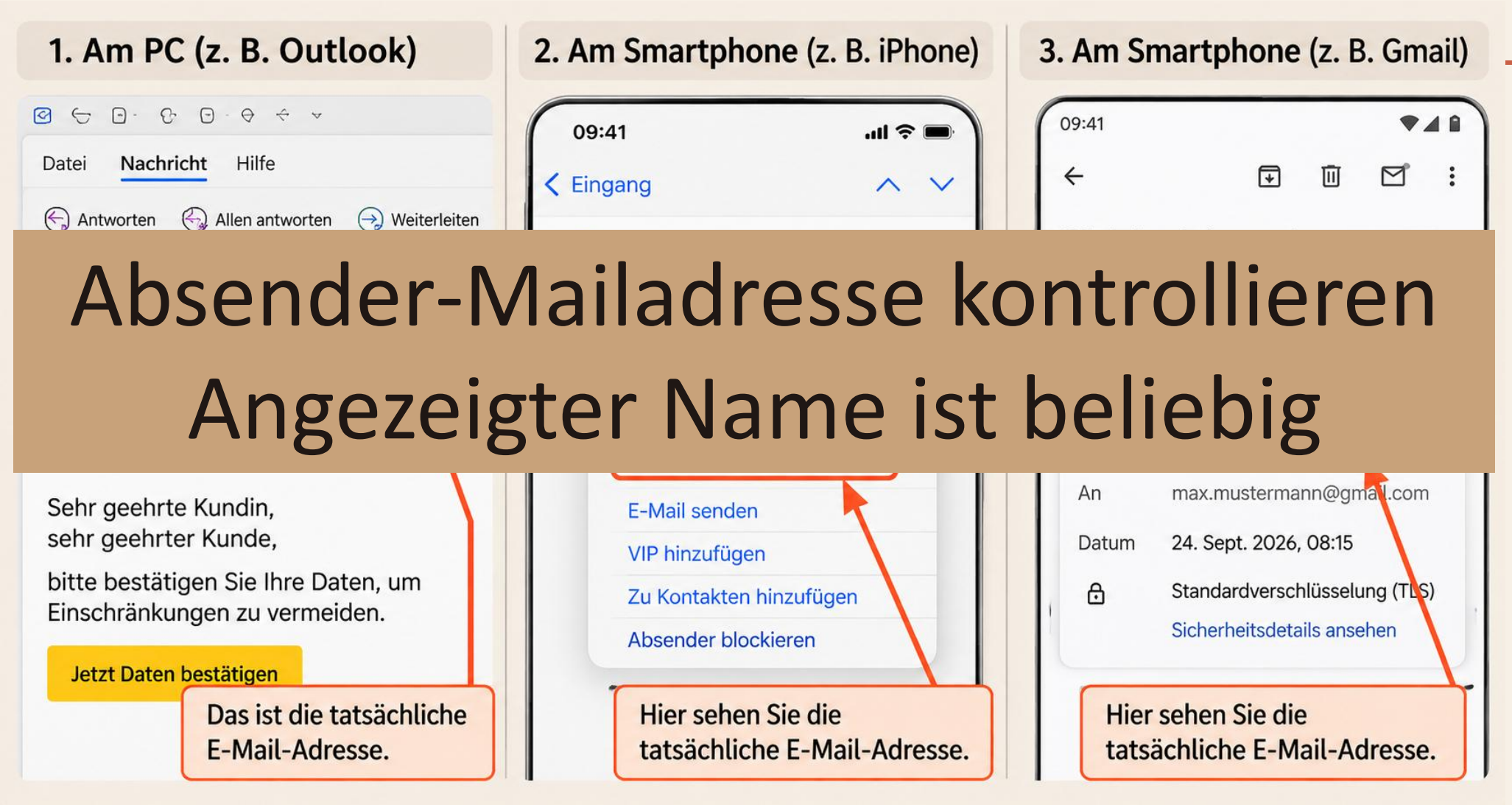


3. Am Smartphone (z. B. Gmail)



Quelle: BSI – Phishing erkennen und richtig handeln

Phishing-Mails Beispiele #1



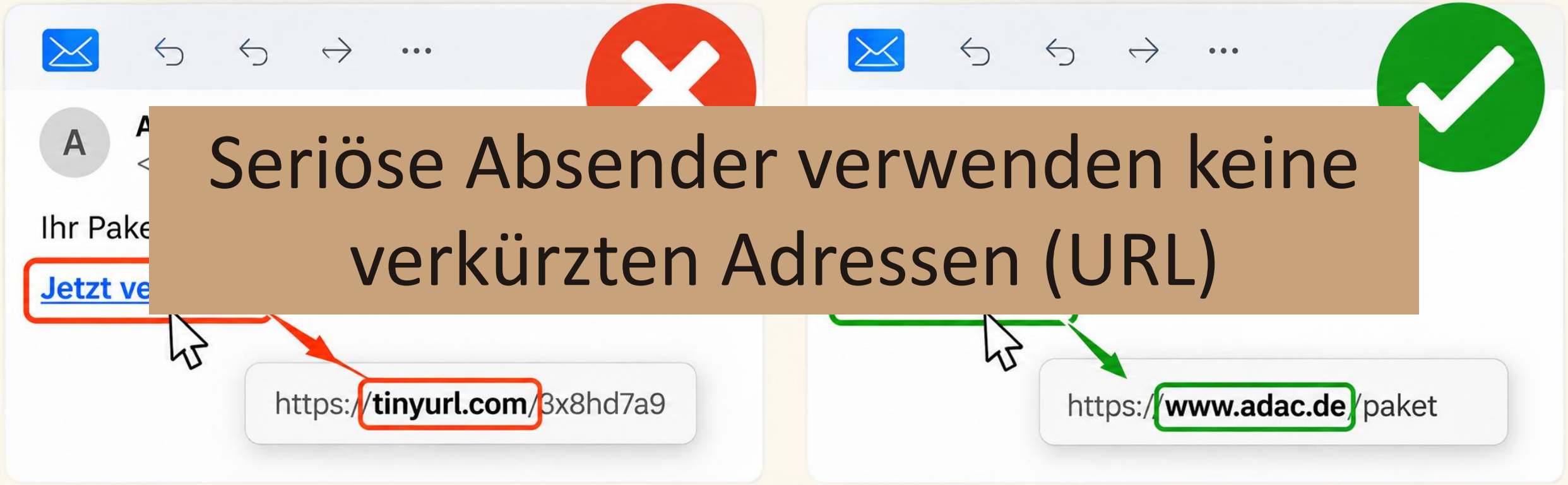
Quelle: BSI – Phishing erkennen und richtig handeln

Phishing-Mails Beispiele #2



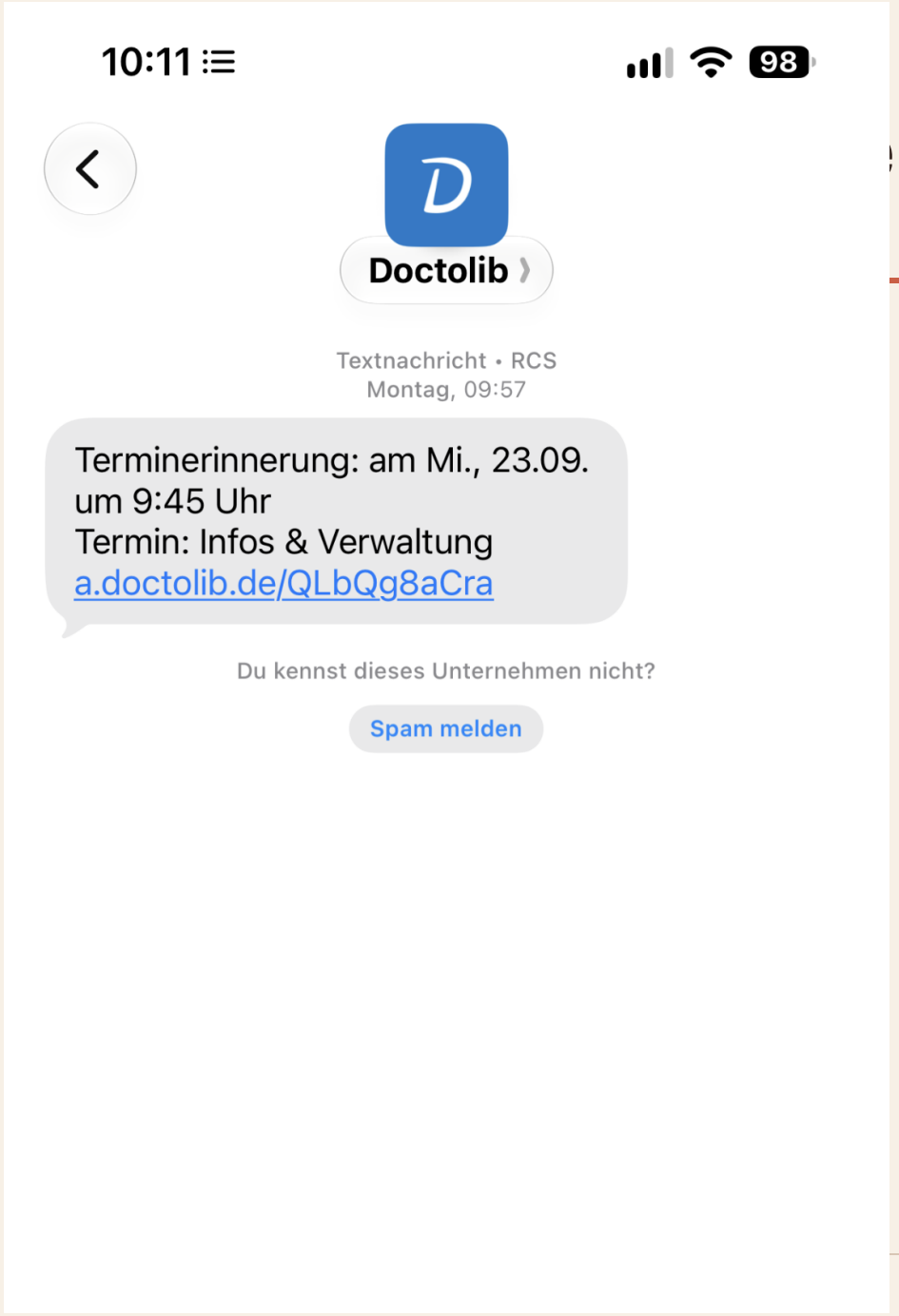


Phishing-Mails Beispiele #2



Seriöse Absender verwenden keine verkürzten Adressen (URL)

Quelle: BSI – Phishing erkennen und richtig handeln



SMS — der Druck bleibt derselbe

„Ihr Paket wartet. Zahlen Sie 1,99 €.“

Drei Prüfungen

- **Erwarte ich das?**
  Bestellung in der echten App oder auf der selbst geöffneten Website prüfen.
- **Passt die Nummer?**
  Absendernummern können gefälscht oder zufällig sein.
- **Wohin führt der Link?**
  Nicht auf den SMS-Link tippen. Die Website oder App selbst öffnen.

WhatsApp-Betrug beginnt oft mit „neuer Nummer“ *

*Quelle: Mimikama „Hallo Mama Betrug“

„Hallo Mama, mein Handy ist kaputt. Das ist meine neue Nummer …“

Was tun bei „Hallo Mama“-Betrug?

1. Nicht antworten
2. Alte Nummer anrufen
3. Keine Überweisung tätigen
4. Chat sichern und melden
5. Bank sofort kontaktieren (falls Geld gesendet)

Familienregel

Ein Satz schützt alle:
„Ich rufe dich zurück.“
oder
Password vereinbaren

WhatsApp-Betrug beginnt oft mit „neuer Nummer“ *

*Quelle: Mimikama „Hallo Mama Betrug“

„Hallo Mama, mein Handy ist kaputt.
Das

Alle bekannten Messenger sind betroffen

W

1. Nicht antworten
2. Alte Nummer anrufen
3. Keine Überweisung tätigen
4. Chat sichern und melden
5. Bank sofort kontaktieren (falls Geld gesendet)

Ein Satz schützt alle:
„Ich rufe dich zurück.“
oder
Password vereinbaren

Telefonbetrug lebt davon, dass Sie im Gespräch bleiben

AUFLEGEN

- Selbst wählen
- Behauptet jemand, von Bank, Polizei oder Microsoft zu sein?
- Gespräch beenden
- Die offizielle Telefonnummer selbst heraussuchen und anrufen.

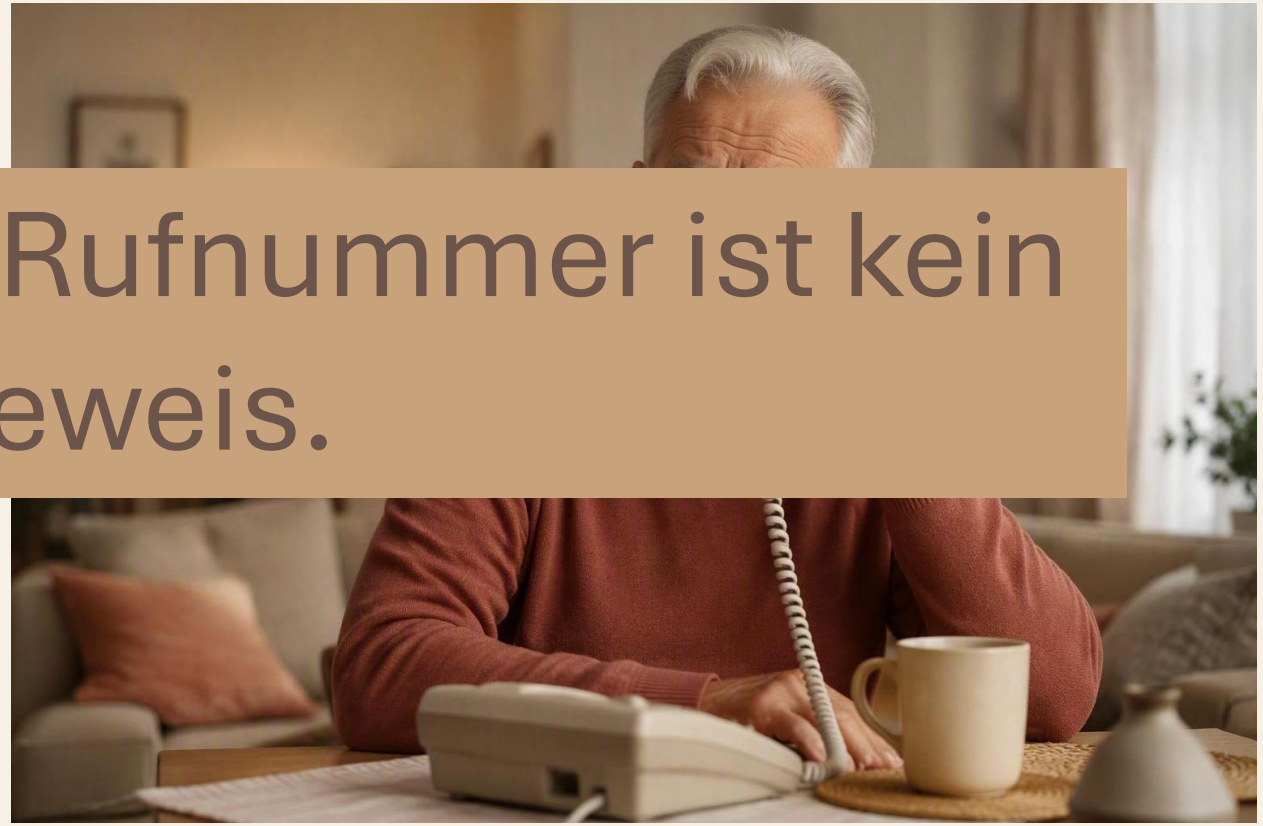


Telefonbetrug lebt davon, dass Sie im Gespräch bleiben

AUFLEGEN

- **Se**
- **Be**

  Po
- **Gespräch beenden**
- **Die offizielle Telefonnummer selbst heraussuchen und anrufen.**



Die angezeigte Rufnummer ist kein Beweis.

Telefonbetrug: Drei Sätze, die den Anruf beenden

„Ich rufe zurück.“

Über die Nummer auf der Bankkarte oder der offiziellen Website. Nie über die Nummer vom Display oder aus dem Gespräch.

„Ich nenne keine Kontostände.“

Ein unerwarteter Anrufer, der Ihren Kontostand wissen will, ist ein Warnsignal. Nennen Sie ihn nicht.

„Ich überweise nichts auf ein Sicherheitskonto.“

Banken und Behörden verlangen keine Überweisung auf ein „Sicherheitskonto“. Wer Sie dazu auffordert, versucht Sie zu betrügen.

Quelle: Polizeiliche Kriminalprävention – Falsche Polizeibeamte

TELEFON

Telefonbetrug: Drei Sätze, die den Anruf beenden

„Ich rufe zurück.“

Über d
der off
Numm
Gesprä

„Ich nenne keine Kontostände.“

n
gnal.

Eine echte Behördennummer auf dem Display und ein Gesicht im Videoanruf beweisen nichts.

Nur der Rückruf auf eigenem Weg zeigt, wer wirklich dran ist.

Banken und Behörden verlangen keine Überweisung auf ein „Sicherheitskonto“. Wer Sie dazu auffordert, versucht Sie zu betrügen.

Quelle: Polizeiliche Kriminalprävention – Falsche Polizeibeamte

KI macht Stimmen und Bilder Glaubwürdiger, nicht wahrer.

7 Warnsignale am Telefon

1. Der Anruf beginnt mit einem **Notfall**, der sofortiges Handeln verlangt.
2. Die **Person** bittet um Geld, Gutscheinkarten, Überweisungen oder Kryptowährungen.
3. Sie sollen **niemandem** von dem Anruf erzählen.
4. Rückfragen werden **ausweichend** beantwortet.
5. Die Stimme klingt **vertraut**, aber die Wortwahl passt **nicht** ganz zur Person.
6. Es wird behauptet, das Handy sei **kaputt** oder eine andere Nummer **müsse** verwendet werden.
7. Es entsteht starker **Zeitdruck**: „Bitte sofort“, „sonst ist es zu spät“, „du darfst nicht auflegen“.

Quelle: Cybersicherheitsmonitor 2026, BSI/ProPK

Was tun, wenn ein verdächtiger Anruf kommt?

7 Schutzmechanismen

1. Rufen Sie die angeblich **betroffene** Person selbst über eine **bekannte** Nummer zurück.
2. Stellen Sie eine Frage, die nur die **echte** Person beantworten kann.
3. Überweisen Sie kein Geld **während** eines laufenden Telefonats.
4. Geben Sie **keine** Zugangsdaten, TANs oder Bankinformationen weiter.
5. Informieren Sie **Angehörige**, wenn Sie einen solchen Anruf erhalten haben.
6. Vereinbaren Sie ein **Familien-Codewort**. Es sollte einfach zu merken, aber schwer zu erraten sein.
7. Wichtig ist: Das Codewort wird nur für **Notfälle** verwendet und nicht nebenbei in Chats oder Postings erwähnt.

Quelle: Cybersicherheitsmonitor 2026, BSI/ProPK

WEBSEITEN

Gefälschte Webseiten kopieren das Aussehen, nicht die Adresse

meine-bank.de ≠ meine-bank.sicher-login.de

Links steht die echte Bankadresse. Rechts gehört die Seite zu sicher-login.de — vertraute Wörter davor können täuschen.

1 Adresse selbst tippen

Nicht über Nachrichten öffnen.

2 Impressum prüfen

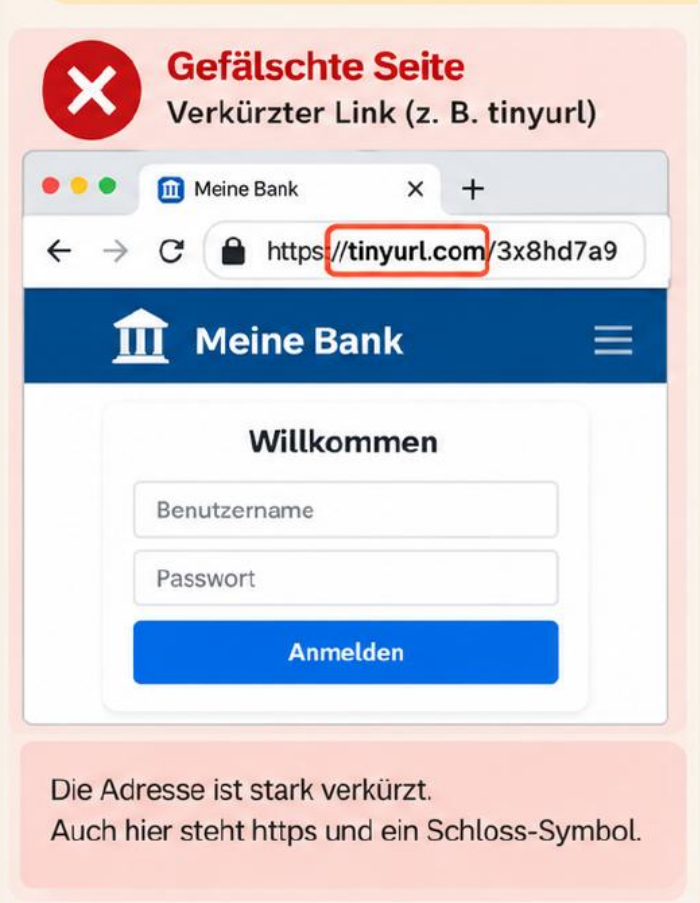
Adresse, Kontakt und Verantwortliche müssen plausibel sein.

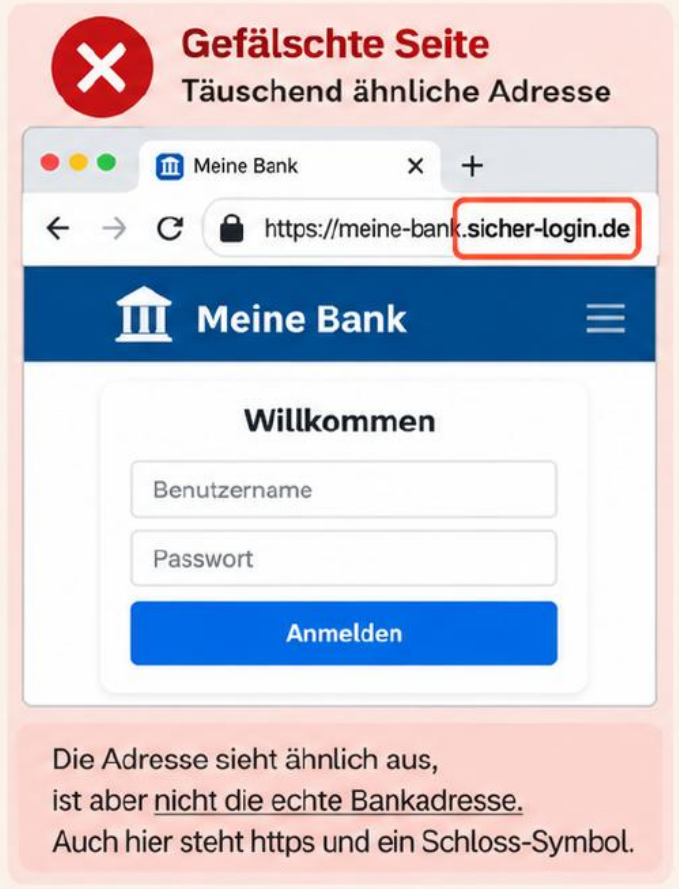
3 Bei Zweifel schließen

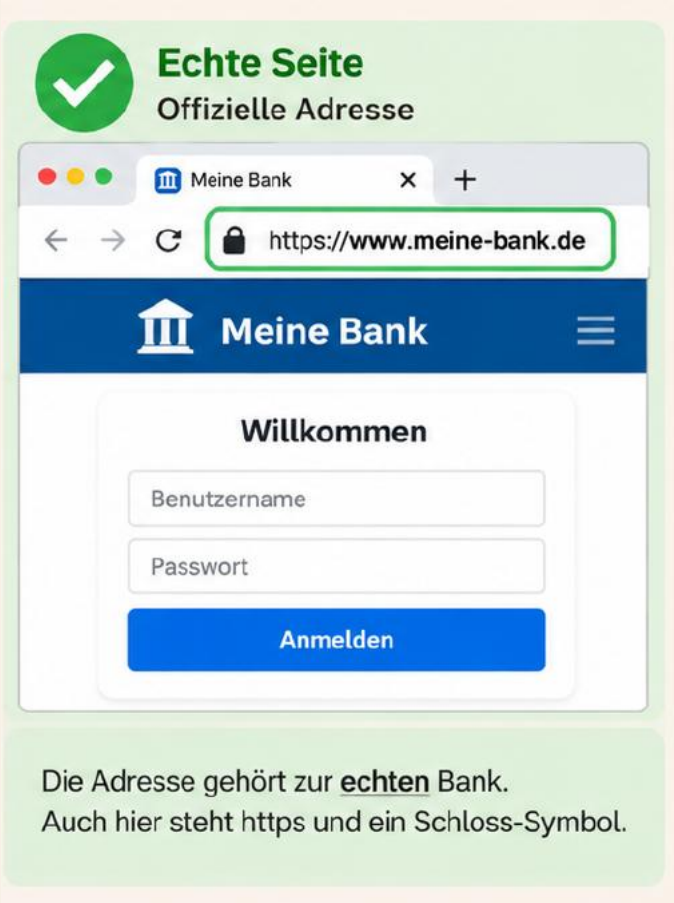
Ein echtes Anliegen bleibt auch nach erneutem Öffnen bestehen.

Quelle: BSI – Sichere Webseiten und Phishing

Gefälschte Webseite können auch ein HTTPS Symbol haben







Quelle: BSI – Sichere Webseiten und Phishing

Falsche Webseiten von echten unterscheiden

Dienste im Internet zum prüfen

Verbraucherzentrale NRW e.V.	Verbraucherzentrale	Link
Virus-Total	VIRUSTOTAL	Link
GoogleSafe Browsing-Websitestatus	Google	Link

Ein Klick falsch gemacht, und was passiert dann?

1

Öffnen

Eine Seite oder Datei startet.

2

Abfragen

Passwort, Karte oder TAN verlangt.

3

Nachladen

Schadsoftware kann installiert werden.

4

Übernehmen

Konto, Gerät oder Zahlung wird missbraucht.

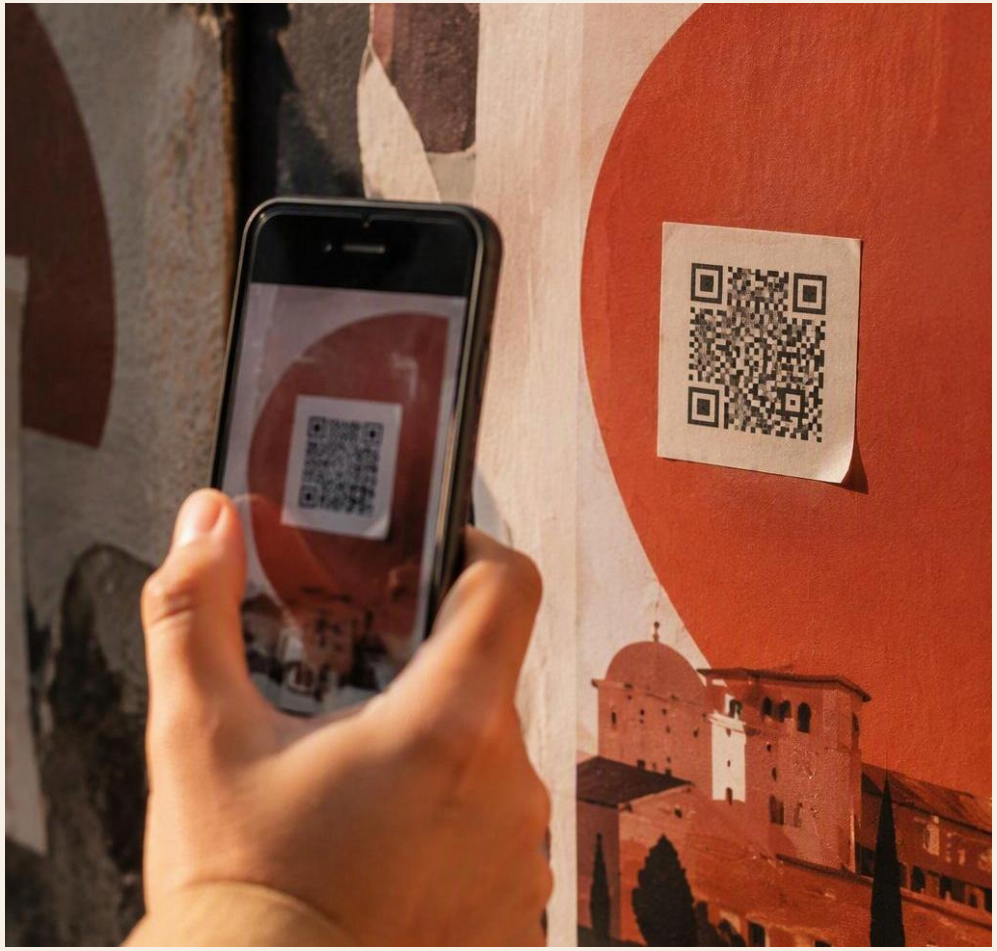
Nur geklickt? Seite schließen. Nichts eingeben. Gerät aktualisieren.
Datei geöffnet oder Daten eingegeben?

Quelle: BSI – Erste Hilfe bei Cyber-Angriffen

Was ist eigentlich Quishing?

Quishing = Phishing mit QR-Codes

- **Betrüger bringen Sie dazu, einen QR-Code zu scannen**
  Beispiele: Parkschein Automat oder Bank-überweisung
- **QR-Code führt dann zu einer gefälschten Website**
  Sieht dem erwarteten Resultat sehr ähnlich, am Smartphone kaum zu erkennen
- **Zahlung erfolgt an Unbekannt**
  Der eigentliche Service wird nicht erbracht, oftmals extra Strafen (Parkticket)



Quelle: BSI – QR-Code-Phishing / Quishing

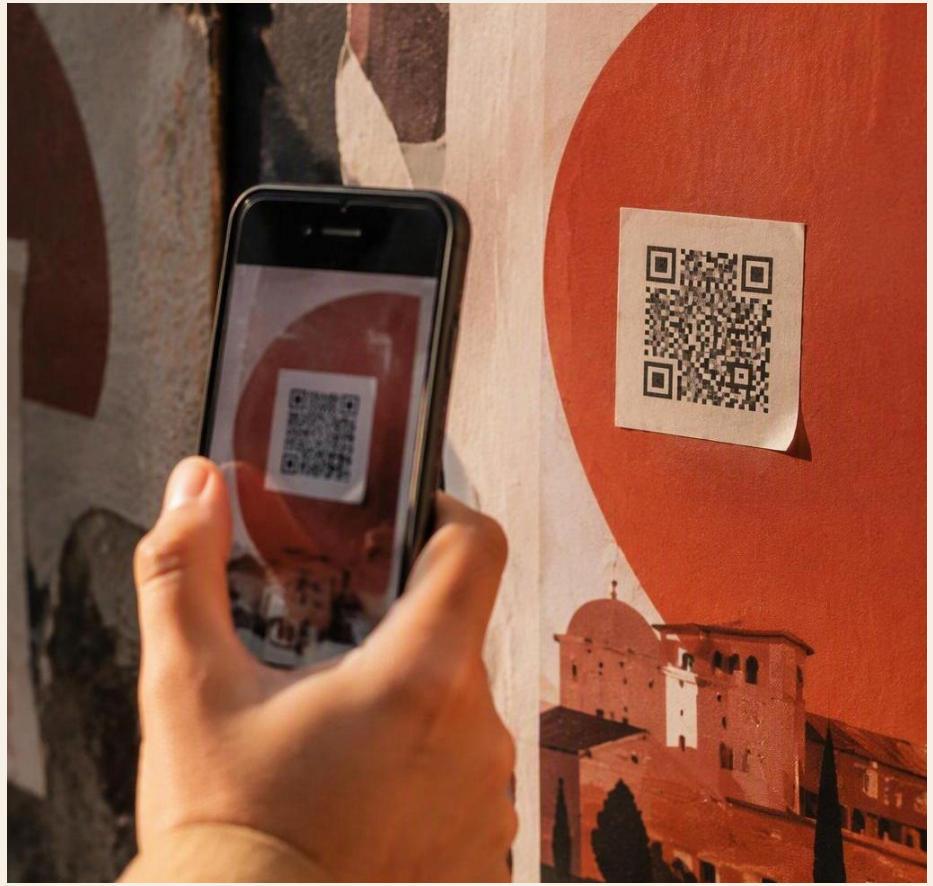
Quishing versteckt den Link hinter einem QR-Code

Vor dem Scannen

- **Aufkleber prüfen**
  Ist ein QR-Code über einen anderen geklebt?

- **Vorschau lesen**
  Zeigt die Kamera eine fremde oder verkürzte Adresse?

- **Zahlung anders öffnen**
  Parken, Bank oder Paketdienst über bekannte App starten.



Quelle: BSI – QR-Code-Phishing / Quishing

Falsche Rechnungen nutzen Gewohnheit und schlechtes Gewissen

ZAHLUNGSERINNERUNG

Rechnungsnummer • Betrag • neue IBAN • kurze Frist

„Bitte heute noch überweisen.“

Prüfen Sie drei Dinge

1 Habe ich bestellt?

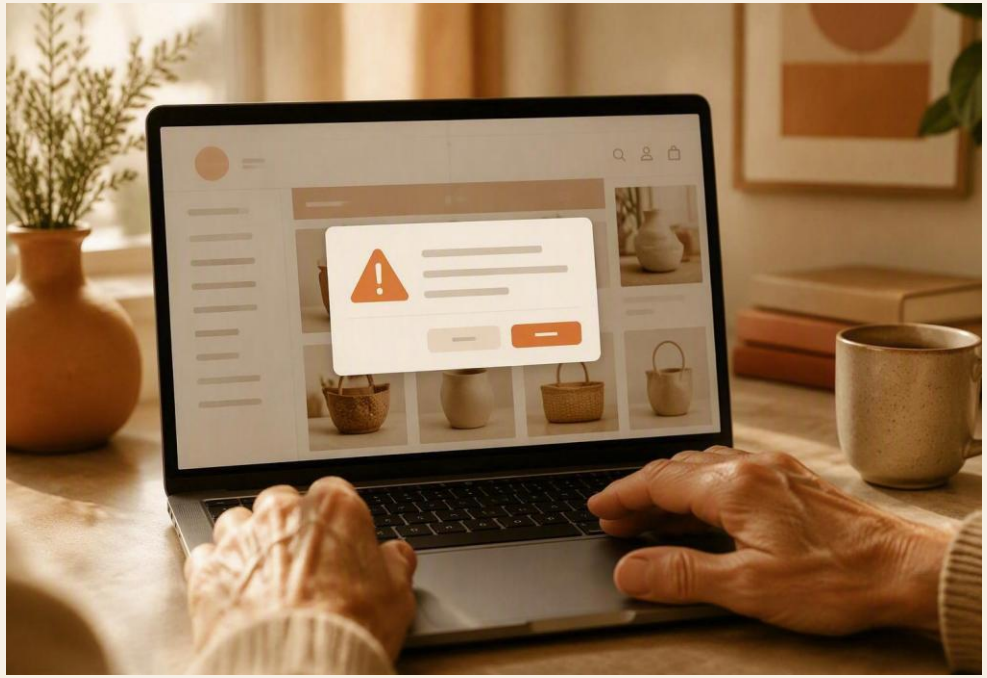
2 Passt die IBAN zu früher?

3 Bestätigt der bekannte Kontakt die Änderung?

Neue Bankverbindung = immer Rückfrage über bekannte Kontaktdaten.

Quelle: Verbraucherzentrale – Gefälschte Rechnungen

Fake-Shops sind oft perfekt gestaltet, der Zahlungsweg verrät sie



Vor dem Kauf

- **Preis**
  Extrem günstig + knapp verfügbar = Achtung!!!
- **Zahlung**
  Nur Zahlung per Vorkasse möglich und keine sicheren Zahlungsarten wie PayPal oder Kauf auf Rechnung
- **Impressum**
  Adresse, Telefon und Handelsregister plausibel prüfen.

Tipp: Fakeshop-Finder der Verbraucherzentrale nutzen.

Quelle: Verbraucherzentrale – Fakeshop-Finder

Banking-Betrug: Erst stoppen, dann prüfen

Typische Maschen

01 **„Ihre Bank“ ruft an**

Angeblicher Betrug, dringende Sicherheitsprüfung oder gesperrtes Konto.

02 **SMS oder E-Mail**

„Konto gesperrt“, „Zahlung bestätigen“ oder „Sicherheitsproblem“.

03 **Push-Freigabe auf dem Handy**

Die Freigabe soll angeblich einen Vorgang stoppen, tatsächlich wird eine Zahlung bestätigt.

Die wichtigste Regel

PIN, TAN und Freigaben niemals auf Aufforderung weitergeben oder bestätigen.

Bei Unsicherheit:

Vorgang abbrechen und die Bank selbst über die bekannte Telefonnummer anrufen.

MERKSATZ

Die Bank darf warten. Betrüger machen Druck.

Quelle: BaFin und BSI – Sicheres Online-Banking

Der Briefkasten ist inzwischen digital.

- E-Mail
- SMS
- Messenger
- Bank-App
- Kundenportal
- QR-Code

Behörden, Banken und Versicherungen nutzen bei wichtigen Vorgängen häufig den klassischen Postweg.

Eine E-Mail, SMS oder WhatsApp-Nachricht kann echt sein, aber sie verdient immer eine Prüfung.



Dieselben fünf Warnsignale tauchen überall auf

DRUCK
„heute“, „sofort“, „letzte Chance“

GEHEIMNIS
„Sagen Sie niemandem etwas“

Inne-Halten!

DATEN
Passwort, PIN, TAN, Ausweis

KANALWECHSEL
E-Mail → Telefon → Fernzugriff

GELDWEG
Vorkasse, Gutscheine, Krypto

Prüfen Sie über einen zweiten, selbst gewählten Weg

NACHRICHT	≠	PRÜFUNG
Link, Nummer oder QR-Code aus der Nachricht		eigener Favorit, Karte, Vertrag, alte Nummer

Beispiel: SMS von der „Bank“ → Bank-App selbst öffnen oder Nummer von der Karte wählen.

Wenn etwas passiert ist: stoppen, sichern, melden

1	**STOPPEN**	Nichts weiter eingeben; Überweisung/Freigabe abbrechen.
2	**TRENNEN**	Bei Fernzugriff oder Schadsoftware Internetverbindung trennen.
3	**SICHERN**	Screenshots, Nummern, Zeiten und Zahlungsdaten notieren.
4	**ÄNDERN**	Passwörter über sauberes Gerät ändern; Sitzungen abmelden.
5	**MELDEN**	Bank, Anbieter, Polizei und betroffene Kontakte informieren.

Hilfen: 116 116 (Sperr-Notruf, Voraussetzungen beachten) · 110 nur bei akuter Gefahr

MITMACHEN

Welche Nachricht ist verdächtig?

A „Ihr Paket konnte nicht zugestellt werden. 1,99 € zahlen: kurzer-link …“

B „Deine neue Rechnung liegt im Kundenportal. Öffne die App wie gewohnt.“

C „Neue Nummer. Bitte überweise heute 1.480 € — ich erkläre später alles.“

Antwort: A und C sind deutlich verdächtig.
B kann echt sein, wird aber unabhängig in der App geprüft.

SECHS KLEINE SCHRITTE

Ihre persönliche Schutzroutine ab heute

- ✓ **Bank-, E-Mail- und Messenger-App immer aktuell halten**
- ✓ **Zwei-Faktor-Schutz für E-Mail und Banking aktivieren**
- ✓ **Bildschirmsperre und Geräte-PIN aktivieren**
- ✓ **Familien-Codewort vereinbaren**
- ✓ **Einzigartige Passwörter im Passwortmanager speichern**
- ✓ **Wichtige Nummern auf Papier bereithalten**

Empfohlene Nummern: Bank · Angehörige · Sperr-Notruf 116 116 · örtliche Polizei

Drei Sätze, die Sie ab morgen schützen

1 „Ich entscheide nicht unter Zeitdruck.“

2 „Ich rufe über eine bekannte Nummer zurück.“

3 „Ich gebe Passwörter, PIN und TAN niemals weiter.“

Im Zweifel gilt: abbrechen, prüfen, Hilfe holen.

STAND: SEPTEMBER 2026

Quellen und Hilfen

BSI: Phishing, Passwörter, Deepfakes, sichere Geräte
www.bsi.bund.de

Polizeiliche Kriminalprävention: Telefon-, Messenger- und Supportbetrug
www.polizei-beratung.de

Bundeskriminalamt: Bundeslagebilder Cybercrime
www.bka.de

Verbraucherzentrale: Smishing, Fake-Shops, Rechnungen
www.verbraucherzentrale.de

BaFin: Schutz vor Banking- und Anlagebetrug
www.bafin.de

Sperr-Notruf: 116 116 · Akute Gefahr: 110
www.sperr-notruf.de

Hinweis: Täter ändern ihre Geschichten. Die Schutzprinzipien bleiben: Pause, unabhängige Prüfung, keine Geheimnisse, keine Freigabe auf Zuruf.