

Betrugsversuche erkennen

und sicher kommunizieren mit dem Smartphone

23.02.2026

Julia Hentschel

Inhalt

- Verschiede Betrugsarten
- Warnhinweise
- Betrug mit KI – Deepfakes
- Wie kann ich mich schützen?
- Signal Messenger
- Weitere Möglichkeiten und Informationen
- Fragen

Verschiede Betrugsarten

Klassische Betrugsversuche

- **Per Telefon** → Anrufe, bei denen nicht gesprochen wird oder sich jemand als Polizei oder Kind/Enkel ausgibt
- **Per SMS oder WhatsApp** → „Hallo Mama, ich habe mein Handy verloren“, „Ihr Paket konnte nicht zugestellt werden“
- **Per E-Mail** → Echtwirkende Mitteilungen von Finanzamt, ÖGK* etc.
- **Lovescam** → Emotionale Zuneigung wird vorgegaukelt, um finanzielle Vorteile daraus zu ziehen; meist auf Social Media

Betrugsversuche mit KI

- Einerseits sogenannte Deepfakes (Video) → echte Fotos/Videos werden in anderen Kontext gesetzt
- Stimmen werden aufgenommen und genutzt (Anrufe von nahestehenden Personen)
- Fake News → KI generierte Inhalte, die gezielt für politische Zwecke genutzt werden

Beispiel Betrugsmail



Beispiel Betrugsmail

Ihre Auszahlung steht bereit

Sehr geehrte Kundin, sehr geehrter Kunde,

wir freuen uns, Ihnen mitteilen zu können, dass eine Rückerstattung in Höhe von **479,45 Euro** für Sie bereitsteht. Um den Prozess für Sie so einfach wie möglich zu gestalten, haben wir ein digitales

Bitte beachten Sie: Die Beantragung sollte zeitnah erfolgen, um eine schnelle Bearbeitung zu gewährleisten.

Jetzt fortfahren

Hinweis: Der gesamte Vorgang dauert weniger als 2 Minuten.

Mit freundlichen Grüßen,
Ihr Serviceteam

Deepfakes erkennen

Deepfakes sind realistisch wirkende Bilder oder Videos, die durch KI erzeugt, abgeändert oder verfälscht wurden.

Woran erkennt man Deepfakes?

- Übergänge oft unscharf oder schlecht gemacht
- unnatürliche Bewegungen, kein Blinzeln (Videogeschwindigkeit verlangsamen)
- unnatürliche Sprache oder schlecht synchronisierte Sprache
- Fehlerhafte Körperteile (Hände, Zähne, Augen)
- Unterschiedliche Qualitätsstufen

Wie kann man ein Bild/Video überprüfen?

- DeepFake-o-meter, Deepware, Deepfake Detection von DuckDuckGoose
- umgekehrte Bildersuche z.B. mit Google Bildersuche oder TinEye

Warnhinweise auf Betrugsversuche

- Zeitdruck („Sofort reagieren!“)
- Drohungen („Ihr Konto wird gesperrt!“)
- Geldforderungen
- Unbekannten Links
- Ungewöhnlichen Absendern oder neuen Nummern
- Schlechter Rechtschreibung oder untypischer Ansprache

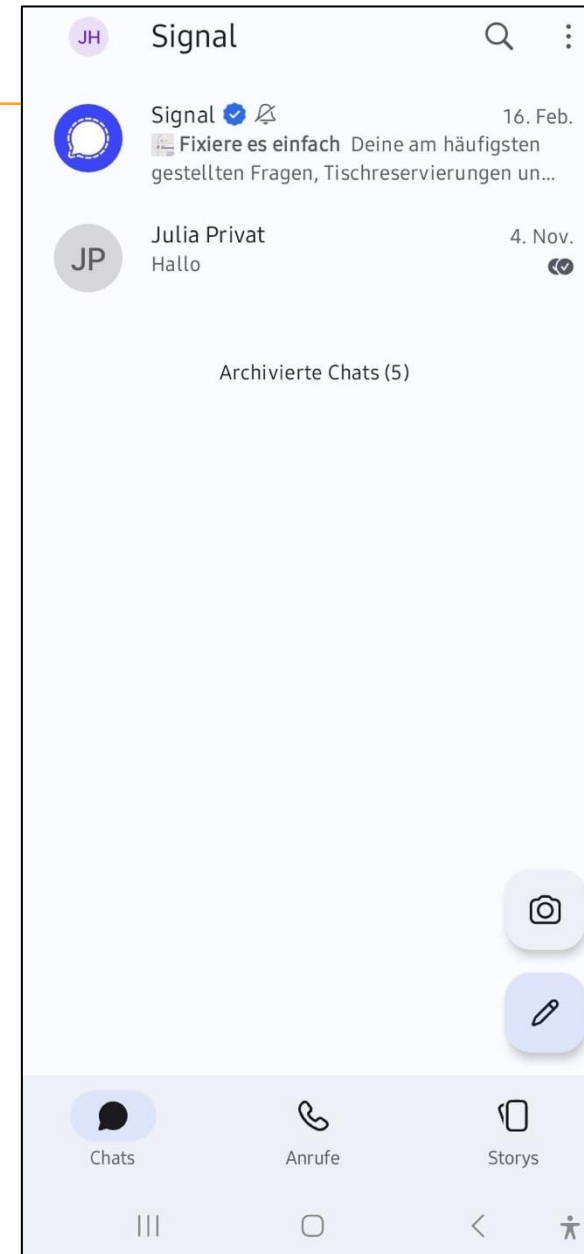
!!! Wenn eine Nachricht Angst macht oder drängt – zuerst prüfen, nicht klicken !!!

Wie kann ich mich schützen?

- Keine sensiblen Daten per SMS oder Messenger versenden
- Keine unbekannten Links anklicken → Banken, Finanzamt u.ä. schicken niemals Links per SMS aus
→ Bei Benachrichtigungen über neue Nachrichten z.B. in „Mein Postkorb“ oder Finanzamt immer direkt auf die Plattform gehen und nicht über den Link im Mail
- Niemals TANs oder Passwörter weitergeben
- Bei Geldforderungen immer persönlich nachfragen
- Im Zweifelsfall Nachricht ignorieren und löschen
- Regelmäßig Updates durchführen
- Zwei-Faktor-Authentifizierung aktivieren

Signal Messenger

- Kann über Playstore/Appstore heruntergeladen werden
- Speichert ausgesprochen wenige Nutzerdaten
- Wird von einer gemeinnützigen Stiftung betrieben und verdient kein Geld mit Nutzerdaten
- Bedienoberfläche und Nutzungsumfang ähnlich wie bei WhatsApp
- Keine KI integriert
- Nachrichten werden Ende-zu-Ende verschlüsselt



Weitere Möglichkeiten und Informationen

- Threema (Messenger) - schweizer Anbieter, kann ohne Telefonnummer genutzt werden, einmalige Zahlung erforderlich
- www.ombudsstelle.at – Plattform bei Internetbetrug
- www.watchlist-internet.at – Informationsplattform für aktuelle Betrugsversuche
- www.mimikama.org – Plattform zur Information über Fake News
- www.tineye.com – Rückwärtsbildersuche zur Überprüfung
- KI Videos:
https://www.instagram.com/reel/DU3aRWnCOPn/?utm_source=ig_web_copy_link&igsh=MzRIODBiNWFIZA==
- https://youtube.com/shorts/ogP2tXebbqs?si=0YuEdH7vNmgdKE_B

Offene Fragen?



Bis zum nächsten Mal!

09. März 2026

17.00 Uhr

Gesunder Lebensstil – wie das Smartphone
unterstützen kann

