Enkeltrick 2.0

Wenn Betrüger mit KI anrufen – und wie Sie sich schützen

Mit den Tipps aus meiner Sendung bleiben Sie auch in KI-Zeiten sicher vor Trickbetrügern.

Liebe Teilnehmerinnen und Teilnehmer,

die Masche ist fast so alt wie das Telefon selbst – und doch gefährlicher als je zuvor. Was früher ein stockender Anruf aus einem fernen Callcenter war, ist heute ein täuschend echter Anruf in der Stimme Ihres Enkels oder Ihrer Tochter. Künstliche Intelligenz hat den klassischen Enkeltrick in eine neue Dimension katapultiert.

Das ist aber kein Grund zur Panik, sondern zur Vorbereitung. In unserem Webinar habe ich Ihnen gezeigt, dass der wirksamste Schutz nicht in einem teuren Computerprogramm steckt, sondern in einem einfachen, analogen Trick: dem Familien-Codewort. In dieser Zusammenfassung habe ich alle wichtigen Erkenntnisse, die fünf goldenen Schutzregeln, praktische Smartphone-Einstellungen und die wichtigsten Notfall-Hotlines für Sie aufbereitet.

Herzlichst, Ihr Kaner Etem

Die Realität in Zahlen: Was die Kriminalstatistik 2024 zeigt

Das Bundeskriminalamt (BKA) registrierte in der Polizeilichen Kriminalstatistik (PKS) 2024 in Deutschland **6.656 Fälle** von Enkeltrick und Schockanruf – und das ist nur die Spitze des Eisbergs. Die tatsächliche Dunkelziffer liegt erheblich höher, weil sich viele Opfer aus Scham nicht melden. Allein in Bayern betrug der Schaden durch Schockanrufe im Jahr 2024 rund **4 Millionen Euro**; in Baden-Württemberg verursachte dieses Phänomen Schäden von **18,4 Millionen Euro**.

Hinter den Anrufen stecken keine einzelnen Kleinkriminellen, sondern hochprofessionell organisierte Banden mit eigenen Abteilungen für „Keiler" (die anrufenden Betrüger), „Logistiker" und „Abholer". Im April 2024 zerschlug Europol im Rahmen der **Operation PANDORA** zwölf illegale Callcenter in Albanien, Bosnien-Herzegowina, dem Kosovo und dem Libanon und nahm 21 Personen fest. Der verhütete Schaden lag laut Europol bei über 10 Millionen Euro.

Wichtig zu wissen: Das Narrativ, dass ältere Menschen aus Naivität oder geringer Bildung auf diese Maschen hereinfallen, ist falsch und unfair. Die Täter nutzen ausgeklügelte psychologische Mechanismen – den elterlichen Schutzreflex, Autoritätshörigkeit und künstlich erzeugten Zeitdruck – die bei Menschen jeden Alters und jeder Bildungsstufe wirken. **Opfer sind nicht dumm. Schämen sollen sich die Täter.**

Die neue Gefahr: Wie KI-Voice-Cloning funktioniert

Das Herzstück des modernen Enkeltricks ist das sogenannte **Voice Cloning** – das KI-gestützte Klonen von realen Stimmen. Forscher von Microsoft zeigten bereits 2023 mit ihrem Modell VALL-E, dass bereits **drei Sekunden** einer originalen Sprachaufnahme ausreichen, um eine täuschend echte digitale Kopie einer menschlichen Stimme zu erzeugen. Das benötigte Material finden Kriminelle vollautomatisch auf Social-Media-Plattformen: ein kurzes Instagram-Video, eine WhatsApp-Sprachnachricht oder ein simples „Hallo? Wer ist da?" bei einem Anruf genügen.

Der typische Ablauf eines KI-Schockanrufs

Das psychologische Drehbuch folgt einem streng optimierten Muster, das darauf ausgelegt ist, Ihre Fähigkeit zum rationalen Denken innerhalb von Sekunden auszuschalten:

1. **Der Schock:** Sie hören die Stimme Ihres Enkels – weinend, außer Atem: „Oma, ich hatte einen schweren Unfall, jemand ist verletzt!"
2. **Die Autorität:** Eine „Kommissarin" oder ein „Staatsanwalt" übernimmt das Gespräch. Die Situation wirkt offiziell und unausweichlich.

3. **Der Druck:** Es wird striktes Stillschweigen befohlen. Kein Gespräch mit der Familie, nicht die Bank anrufen, nicht die Polizei.
4. **Die Übergabe:** Ein „Bote" oder „Kurier" soll Bargeld oder Schmuck abholen, oder es wird eine sofortige Überweisung gefordert.

Der erste polizeilich bestätigte KI-Schockanruf in Deutschland ereignete sich am **5. September 2025 in Lichtenfels** (Oberfranken). Eine ältere Seniorin hörte am Telefon die – korrekt geklonte – Stimme ihrer weinenden Tochter, die angeblich einen tödlichen Unfall verursacht hatte. Eine vermeintliche „Kommissarin" forderte 45.000 Euro Kaution. Die Familie erkannte den Betrug rechtzeitig; kein Geld floss. Andere Fälle gingen weniger glimpflich aus: Ein Ehepaar in Düsseldorf verlor 230.000 Euro, eine 60-jährige Frau in Pfaffenhofen übergab 60.000 Euro auf einem Supermarktparkplatz.

Weitere KI-gestützte Maschen, die Sie kennen sollten

- **Deepfake-Investmentvideos:** Prominente wie Günther Jauch, Dieter Bohlen oder Thomas Gottschalk werben in gefälschten Videos für angeblich revolutionäre Krypto-Plattformen.
- **WhatsApp-Enkeltrick „Neue Nummer":** „Mama, mein Handy ist kaputt, das ist meine neue Nummer." – kombinierbar mit einer geklonten Sprachnachricht in der Stimme des echten Kindes.
- **“Romance Scam”:** Vermeintlich attraktive Frauen buhlen auf Social Media um Ihre Gunst. Eine Woche später passiert ein vermeintlich schlimmer Unfall, sie benötigen dringend Geld. Hinter den weiblichen Profilen stecken Trickbetrüger.
- **Stumme Anrufe:** Manche Betrüger rufen nur an, um Ihr „Hallo?" aufzunehmen – als Stimmprobe für spätere Klonierungsversuche.
- **Falscher Microsoft-Support:** „Ihr Computer ist mit einem gefährlichen Virus infiziert" – Ziel ist es, Fernzugriff auf Ihren PC zu erhalten.

Das Schutzschild: Die 5 goldenen Verhaltensregeln

Da gefälschte Stimmen und Bilder nicht mehr zuverlässig erkannt werden können, muss der Schutz durch klare Verhaltensregeln entstehen – nicht durch technische Erkennungsversuche.

1. **Auflegen ist nicht unhöflich – es ist klug.** Bei jedem Anruf mit einer Geldforderung, einer Schocknachricht oder einer angeblichen Behörde legen Sie sofort auf. Echte Verwandte verstehen das und rufen zurück. Echte Polizisten fordern niemals am Telefon Geld oder Kaution.
2. **Selbst zurückrufen – über die bekannte Nummer.** Wählen Sie die Nummer Ihrer Tochter, Ihres Enkels oder der Polizei (110) direkt aus Ihrem Adressbuch. Verwenden Sie niemals die Rückruftaste, da diese aufgrund von Call-ID-Spoofing direkt wieder zu den Betrügern führen kann.

3. **Das Familien-Codewort vereinbaren.** Dies ist die wirksamste Einzelmaßnahme. Mehr dazu im nächsten Abschnitt.
4. **Niemals Bargeld oder Schmuck übergeben.** Keine Behörde der Welt schickt Boten, um Wertsachen abzuholen. Wer das tut, ist ein Betrüger – punkt.
5. **Bei Druck und Eile: Vertrauensperson einschalten.** „Ich kläre das mit meiner Familie und rufe zurück" ist ein Recht, das Sie immer haben. Echte Notlagen halten 10 Minuten Verzögerung aus. Wer das nicht akzeptiert, will Sie täuschen.

Das Familien-Codewort: Ihre wichtigste Waffe

Das Familien-Codewort ist überraschend simpel und dabei von unschlagbarer Wirksamkeit. Eine Künstliche Intelligenz kann keine Gedanken lesen und kein Geheimwissen erraten. Vereinbaren Sie beim nächsten Familientreffen – persönlich, nicht per Messenger – ein Wort oder eine kurze Frage, die keinen logischen Bezug zu Ihrer Familie hat und nicht aus Ihren sozialen Netzwerken ableitbar ist.

So geht es richtig:

- Beim persönlichen Treffen besprechen – nie per E-Mail, SMS oder WhatsApp
- Nicht der Name des Haustieres, der auf Facebook sichtbar ist
- Nirgendwo aufschreiben, wo andere es finden könnten
- Beispiel: Berlin2000

Die eiserne Regel: Bevor auch nur ein Gedanke an finanzielle Hilfe verschwendet wird, fragen Sie nach dem Codewort. Kann die anrufende Stimme es nicht sofort nennen, legen Sie auf – unabhängig davon, wie überzeugend die Stimme klingt.

Technische Helfer: Spam-Anrufe automatisch blockieren

Moderne Smartphones bieten kostenlose, eingebaute Schutzfunktionen, die einen Großteil der automatisierten Betrugsanrufe still und lautlos aussortieren, bevor Ihr Telefon überhaupt klingelt.

Apple iPhone (iOS)

Gehen Sie zu **Einstellungen** → **Telefon** → **„Unbekannte Anrufer stummschalten"** und aktivieren Sie die Funktion. Anrufe von Nummern, die nicht in Ihrem Adressbuch stehen, klingeln nicht mehr, sondern werden direkt an die Mailbox weitergeleitet. Sie sehen sie später still in Ihrer Anrufliste. Wichtig: Speichern Sie alle relevanten Nummern (Arzt, Apotheke, Handwerker) im Adressbuch, damit diese Sie weiterhin erreichen können.

Android-Smartphones (Google, Samsung, Xiaomi)

Öffnen Sie die Telefon-App, tippen Sie auf das Menü (drei Punkte), wählen Sie **Einstellungen** → **Anrufer-ID & Spam** und aktivieren Sie die Funktion. Google prüft eingehende Nummern in Echtzeit gegen eine riesige Datenbank bekannter Betrugs-Nummern und markiert verdächtige Anrufe deutlich mit einem roten Warnhinweis.

Browser-Schutz gegen Phishing-Webseiten

- **Google Chrome:** Einstellungen → Datenschutz und Sicherheit → Sicherheit → *Erweiterter Schutz* aktivieren
- **Microsoft Edge:** Der Microsoft Defender SmartScreen ist standardmäßig aktiv und blockiert bekannte Betrugsseiten automatisch
- **Apple Safari:** Einstellungen → Safari → *Betrugswarnung* aktivieren

Zwei-Faktor-Authentifizierung (2FA)

Aktivieren Sie für Ihr E-Mail-Konto und Ihr Online-Banking die Zwei-Faktor-Authentifizierung. Selbst wenn Betrüger Ihr Passwort stehlen, können sie ohne den zweiten Faktor (z. B. einen Code per SMS) nicht auf Ihr Konto zugreifen. Laut dem BSI-Cybersicherheitsmonitor nutzen weniger als 40 Prozent der deutschen Internetnutzer 2FA – hier liegt enormes ungenutztes Schutzpotenzial.

Erste Hilfe im Ernstfall: Was sofort zu tun ist

Trotz aller Vorsichtsmaßnahmen kann es passieren. Die größte Gefahr in dieser Situation ist die Scham, die schnelles Handeln verhindert. Denken Sie daran: Sie sind Opfer hochprofessioneller Krimineller – nicht naiv.

Die goldene Stunde: Bei einer Überweisung zählt jede Minute. Je schneller Sie Ihre Bank informieren, desto größer die Chance, dass das Geld noch gestoppt werden kann.

Schritt 1 – Kommunikationsabbruch: Legen Sie sofort auf, ohne den Betrüger zu konfrontieren. Schließen Sie keine Browser-Tabs und löschen Sie keine Nachrichten – das sind spätere Beweise.

Schritt 2 – Bank sofort anrufen: Fordern Sie einen **Recall** (Überweisungsrückruf) an. Bei klassischen SEPA-Überweisungen besteht innerhalb von 24 Stunden eine realistische Chance, die Transaktion noch zu stoppen. Wurde mit Kreditkarte bezahlt, leiten Sie einen **Chargeback** ein (Frist: bis zu 120 Tage). Karten sperren: zentrale Notrufnummer **116 116** (24/7, kostenfrei).

Schritt 3 – Polizei: Erstatten Sie Strafanzeige – persönlich auf jeder Dienststelle, telefonisch (110 bei akuter Gefahr) oder online unter portal.onlinewache.polizei.de. Notieren Sie die Vorgangsnummer.

Schritt 4 – Beweise sichern: Sichern Sie alle Chatverläufe, E-Mails (inkl. technischer Kopfzeilen), Rufnummern der Täter und Überweisungsbelege. Screenshots allein reichen vor Gericht oft nicht aus; exportieren Sie originale Dateien.

Schritt 5 – Passwörter ändern: Wechseln Sie von einem sicheren, nicht infizierten Gerät aus alle Passwörter der betroffenen Konten und aktivieren Sie 2FA.

Wichtige Hotlines und Anlaufstellen auf einen Blick

Rufnummer / Adresse	Einrichtung & Leistung
110	Polizei-Notruf – bei akuter Gefahr oder laufendem Betrug
116 116	Zentraler Sperr-Notruf – EC-/Kreditkarte & Online-Banking sofort sperren (24/7, kostenfrei)
116 006	WEISSER RING – Opfer-Telefon, tägl. 7–22 Uhr, kostenfrei & anonym. Rechtliche Beratung, psychologische Unterstützung, über 400 Außenstellen bundesweit
portal.onlinewache.polizei.de	Online-Strafanzeige – bequem von zu Hause, inkl. Beweis-Upload
bsi.bund.de	BSI – Cybersicherheits-Lotse, kostenloser Newsletter „Einfach Cybersicher", Phishing-Checkliste (PDF)
verbraucherzentrale.de	Verbraucherzentrale – Phishing-Radar, Fakeshop-Finder, Beratung vor Ort

Rückbuchungsfristen: Was noch zu retten ist

Zahlungsart	**Frist & Möglichkeit**
SEPA-Überweisung (klassisch)	**Innerhalb 24 Std.** → Recall-Antrag bei der Bank möglich
SEPA-Echtzeit-Überweisung	Praktisch nicht rückholbar (Sekunden bis Gutschrift)
SEPA-Lastschrift (autorisiert)	**8 Wochen** – ohne Begründung rückbuchbar
SEPA-Lastschrift (unautorisiert)	**13 Monate (!)** – ohne Begründung rückbuchbar
Kreditkartenzahlung	**Bis zu 120 Tage** – Chargeback bei der kartenausgebenden Bank
PayPal	**180 Tage** – Käuferschutz bei Nicht-Lieferung (nicht bei „Geld an Freunde″)
Kryptowährungen	Praktisch nicht rückholbar

Die 3 wichtigsten Merksätze

1. Auflegen und über die bekannte Nummer selbst zurückrufen – bei jedem Anruf mit Geldforderung oder Schocknachricht.

2. Codewort abfragen – kann die Stimme das Wort nicht nennen, legen Sie auf. Kein Geld, kein Schmuck, kein Bargeld.

3. Im Notfall sofort handeln: 110 (Polizei) · 116 116 (Kartensperrung) · 116 006 (WEISSER RING)

Sprechen Sie heute noch mit Ihrer Familie über das Codewort – beim nächsten Essen, beim nächsten Telefongespräch. Es ist die einfachste und wirksamste Schutzmaßnahme, die es gibt. Ich wünsche Ihnen Sicherheit, Gelassenheit und dass Sie das Gelernte hoffentlich nie brauchen werden.

Impressum: Computerwissen, ein Unternehmensbereich der VNR Verlag für die Deutsche Wirtschaft AG, Theodor-Heuss-Straße 2–4, 53177 Bonn · Vorstand: Richard Rentrop · Redaktionell Verantwortlicher: Sven Udert · Redaktion & Moderation: Kaner Etem, München · www.computerwissen.de

Alle Angaben ohne Gewähr. Stand: Mai 2026.

Quellenangaben: BKA Polizeiliche Kriminalstatistik 2024, BSI-Cybersicherheitsmonitor 2026, Europol-Operation PANDORA, Microsoft VALL-E (arXiv 2023), WEISSER RING e.V.