# Sicher im Netz:
# Ein Leitfaden für ältere Menschen und ihre Familien

*Schockanruf, Enkeltrick und KI-Stimmklon: Wie diese Maschen wirklich funktionieren*

*Herausgegeben von der aediaevum Stiftung · Mühltal · Juni 2026*

Für ältere Menschen, ihre Angehörigen und alle, die sie schützen wollen

> Im Mai 2026 verlor ein Senior in Schleswig-Holstein durch einen einzigen Schockanruf **113.000 Euro**. Im selben Monat erbeuteten Kriminelle in Haan EC-Karten, PINs und Wertsachen bei Bewohnern Ende achtzig und Anfang neunzig — indem sie sich als Bankmitarbeiter und Handwerker ausgaben. Das sind keine Einzelfälle. Das ist eine Industrie.
>
> *Quelle: Börse Express, Mai 2026*

Dieser Leitfaden erklärt, wie diese Maschen funktionieren — damit sie nicht funktionieren.

## 1. Warum ältere Menschen gezielt angesprochen werden

Das hat nichts mit Naivität zu tun und nichts mit mangelnder Intelligenz. Kriminelle wählen ihre Zielgruppe nach klaren Kriterien:

**Vermögen, das ein Leben lang aufgebaut wurde.** Wer jahrzehntelang gearbeitet und gespart hat, hat im Alter oft bedeutende Rücklagen — Ersparnisse, Schmuck, Eigenheim. Diese Rücklagen sind das eigentliche Ziel.

**Stärker ausgeprägte Autoritätsorientierung.** Menschen, die in einer Zeit aufgewachsen sind, in der Behörden, Polizei und Ärzte unangezweifelte Autorität besaßen, reagieren auf entsprechende Anrufe mit einer anderen inneren Haltung als jüngere Generationen — und genau das nutzen Täter aus.

**Soziale Isolation.** Wer allein lebt und wenig Kontakt hat, dem fehlt die Person, die beim Verdacht schnell zurückfragt: „War das wirklich mein Enkel¿‘

**Vertrautheit mit persönlichem Kontakt.** Wer Vertrauen aus jahrzehntelangen persönlichen Begegnungen kennt, fällt auf simuliertes Vertrauen am Telefon anders herein als jemand, der mit digitaler Grundskepsis aufgewachsen ist.

Keines dieser Merkmale ist eine Schwäche. Sie alle sind das Ergebnis eines langen, gelebten Lebens. Die Kriminellen missbrauchen das.

## 2. Die fünf Maschen — und wie man sie in Sekunden erkennt

### Der Schockanruf

Eine aufgeregte Stimme am Telefon: „Ihre Tochter hatte einen schweren Unfall. Es wird sofort Geld für die Operation benötigt." Manchmal ist es kein Unfall — sondern ein angebliches Verbrechen, eine Festnahme, eine Kaution.

Die Täter haben Ihre Telefonnummer, oft aus öffentlichen Telefonbüchern oder zugekauften Listen. Sie wissen: Wer pausiert, wartet darauf, dass das Opfer selbst einen Namen nennt. „Ist es die Maria¿' — und schon haben die Täter den Namen, den sie für das weitere Gespräch brauchen.

> **Das einzige zuverlässige Gegenmittel:** Auflegen. Sofort. Dann direkt über die Ihnen bekannte Nummer zurückrufen — die gespeicherte Nummer in Ihrem Handy, nicht die Nummer, die der Anrufer nennt. Eine echte Notlage übersteht diesen kurzen Moment. Eine erfundene Notlage zerbricht genau daran.

*Quelle: BMI, Straftaten zum Nachteil älterer Menschen*

### Der klassische Enkeltrick — und seine KI-Variante

„Rate mal, wer hier sprichti' Ein Anruf, der darauf abzielt, dass Sie selbst den Namen eines Enkels, Kindes oder Bekannten nennen.

**Die KI-Variante:** Kriminelle benötigen nur **drei Sekunden** Audiomaterial aus einem Social-Media-Video, um eine täuschend echte Stimmkopie zu erstellen (Quelle). Die Stimme am Telefon klingt wie Ihr Enkel. Die Betonung ist richtig. Und dennoch ist es eine Maschine.

**Gegenmittel: Das Familien-Codewort**

Vereinbaren Sie heute noch mit Ihren nächsten Angehörigen ein **Codewort** — ein beliebiges Wort, das kein Fremder kennt. Wer es bei einem Hilferuf nicht nennen kann, ist nicht, wer er vorgibt zu sein.

### Die WhatsApp-Masche: „Mama, ich hab eine neue Nummer"

Eine Nachricht von einer unbekannten Nummer: „Hallo Mama, mein Handy ist kaputt, das ist meine neue Nummer. Kannst du mir kurz helfen¿' Dann kommt die Bitte um eine dringende Überweisung.

> **Gegenmittel:** Rufen Sie bei jeder unbekannten Nummer, die behauptet, Ihre Tochter oder Ihr Sohn zu sein, unter der bekannten, gespeicherten Nummer zurück. Wenn das Handy angeblich kaputt ist, gibt es andere Wege zur Erreichbarkeit.

*Quelle: mimikama.org*

### Der falsche Polizist

Ein angeblicher Polizeibeamter ruft an und erklärt, Ihre Ersparnisse seien in Gefahr — Ihr Geld müsse zur sicheren Verwahrung abgeholt werden.

**Was Sie wissen müssen**

Die Polizei holt **niemals** Bargeld, Schmuck oder Wertsachen zur „sicheren Verwahrung" ab. Kein Polizist wird Sie jemals bitten, Geld abzuheben und an eine fremde Person zu übergeben. Wenn Sie auch nur den geringsten Zweifel haben: Legen Sie auf und rufen Sie den Notruf **110** an — nicht die Nummer, die der Anrufer Ihnen nennt.

### Gefälschte technische Unterstützung

Eine Fehlermeldung auf dem Computer oder ein Anruf von „Microsoft": Ihr Computer sei infiziert, Sie müssten sofort handeln. Man bittet um Fernzugriff auf Ihren Computer oder um die Installation eines Programms.

> **Gegenmittel:** Kein seriöses Unternehmen nimmt unaufgefordert Kontakt auf, um Ihnen mitzuteilen, dass Ihr Computer einen Fehler hat. Legen Sie auf. Schließen Sie die Seite. Fragen Sie eine vertraute Person.

## 3. Drei Gewohnheiten, die langfristig schützen

**Gewohnheit 1: Das Codewort in der Familie.** Vereinbaren Sie heute noch mit Ihren nächsten Angehörigen ein Codewort — ein beliebiges Wort, das kein Fremder kennt. Wer es bei einem Hilferuf nicht nennen kann, ist nicht Ihr Kind oder Ihr Enkel.

**Gewohnheit 2: Niemals sofort handeln.** Jede Anfrage, die Dringlichkeit erzeugt — „Sie müssen sofort überweisen", „Sie haben nur zwei Stunden" — ist ein Warnsignal. Echte Notlagen können warten, bis Sie eine vertraute Person gefragt haben. Erfundene Notlagen können das nicht.

**Gewohnheit 3: Eine Vertrauensperson benennen.** Benennen Sie in Ihrem Umfeld eine Person — ein Kind, eine Nachbarin, ein Freund —, der Sie bei unklaren Situationen sofort anrufen. Nicht morgen. Sofort, bevor Sie etwas tun.

## 4. Was Familien tun können — das Gespräch, das schützt

Das Wirksamste, was Sie als Angehöriger tun können, ist ein offenes Gespräch — ohne Herablassung, ohne die Haltung „Ich erkläre dir jetzt etwas".

**Sprechen Sie konkret.** Nicht „Sei vorsichtig mit dem Internet", sondern: „Wenn jemand anruft und sagt, ich sitze im Gefängnis und brauche Geld — leg sofort auf und ruf mich an." Ein konkretes Szenario bleibt besser in Erinnerung als eine abstrakte Warnung.

**Vereinbaren Sie das Codewort.** Sagen Sie Ihrer Mutter, Ihrem Vater, Ihrer Großmutter: „Wenn ich jemals wirklich in einer Notlage bin, nenne ich dieses Wort." Dann nennen Sie es — und nur Sie beide kennen es.

**Sprechen Sie auch mit dem Bankberater.** Viele Banken informieren ihr Personal gezielt über diese

Maschen. Wer einer älteren Person erklärt, warum eine ungewöhnliche Barabhebung kurz hinterfragt wird, verhindert damit Schäden im fünfstelligen Bereich.

## Was dieses Wissen in der Welt bewirkt

Senioren-Betrug trifft selten nur eine Person — oft betrifft er ganze Familien. Der finanzielle Verlust ist das Eine. Das Gefühl, hereingefallen zu sein, das Misstrauen gegenüber dem eigenen Urteilsvermögen, die Scham — das ist das Andere, das oft länger anhält.

Wissen, das vor dem Betrug ankommt, verhindert beides. Teilen Sie diesen Leitfaden — mit Eltern, Großeltern, Nachbarn. Nicht als Warnung, sondern als Information: So funktioniert es. So erkennt man es. So legt man einfach auf.

### Quellen

BMI: Straftaten zum Nachteil älterer Menschen — Enkeltrick und Schockanrufe
mimikama.org: Senioren-Betrug erkennen: Enkeltrick, Schockanruf & WhatsApp-Fakes
Börse Express: Digitale Teilhabe: Europas Senioren zwischen KI und Cyberkriminalität, Mai 2026
borncity.com: KI-Anrufe: Drei Sekunden Audio reichen für perfekten Stimmklon