

Die Betrugsmaschen-Erkennungskarte

Die zehn häufigsten Maschen — mit dem typischen Köder, den Warnzeichen und der richtigen Reaktion. Zum Ausdrucken und neben das Telefon legen.

Du musst dir nicht jede Zahl merken. Du musst nur eines können: das Muster erkennen und im richtigen Moment auflegen. Fast jede Masche funktioniert gleich — sie erzeugt **Druck, Angst oder Gier** und will, dass du **sofort** handelst. Genau da liegt dein Schutz: Kein seriöser Anrufer, keine echte Bank und keine echte Behörde verlangt jemals eine Entscheidung in derselben Minute.

Wichtiger Hinweis: Diese Karte ist eine Orientierungshilfe, keine Rechtsberatung. Stand 2026, Zahlen aus Deutschland (BKA, Bitkom, Verbraucherzentralen, Landespolizeien). Mit ⚠ markierte Zahlen sind Schätzungen von Verbraucherschützern, keine amtliche Statistik.

So funktioniert (fast) jede Masche

Über 6 von 10 Internetnutzern waren 2025 von Cyberkriminalität betroffen (Bitkom 2025). Der Durchschnittsschaden liegt bei rund 180–219 € — aber bei Schock- und Anlagebetrug geht es schnell um fünf- bis sechststellige Summen. Neu ist: Durch KI verschwinden die alten Warnzeichen. Schlechtes Deutsch, holprige Anrede — das war einmal. Heute klingt die Stimme am Telefon wie dein Enkel, weil sie aus wenigen Sekunden eines Social-Media-Videos geklont wurde. KI-gestützter Betrug ist seit 2023 um über 300 % gestiegen ⚠ (geschätzt, Verbraucherzentrale-Financen 2026).

Deshalb schützt dich nicht das Wissen über die Technik, sondern ein trainierter Reflex: auflegen, selbst zurückrufen, nie unter Zeitdruck zahlen.

Die Erkennungskarte

Masche	Typischer Satz / Köder	Warnzeichen	Deine richtige Reaktion
Schockanruf	„Mama, ich hatte einen schweren Unfall ... du musst sofort eine Kautions zahlen, sonst komme ich ins Gefängnis.“ (weinende Stimme)	Extreme Emotion, Zeitdruck, Geheimhaltung („sag es niemandem“), Übergabe von Bargeld/Wertsachen.	Auflegen. Familienmitglied selbst über die bekannte Nummer anrufen. Codewort abfragen. Niemals Geld übergeben.
Falscher Polizist / Staatsanwalt	„Hier Kriminalpolizei. In Ihrer Nähe wurde eingebrochen — Ihr Geld ist auf der Bank nicht mehr sicher. Wir holen es zur Sicherheit ab.“	Angebliche Amtsautorität, Angst, Aufforderung, Geld/Gold „in Sicherheit“ zu bringen.	Auflegen. Echte Polizei fordert nie Bargeld oder Wertsachen. Über 110 selbst zurückrufen (nie die angezeigte Nummer).
„Hallo Mama / Hallo Papa“ (WhatsApp/SMS)	„Hallo Papa, das ist meine neue Nummer. Mein altes Handy ist kaputt. Kannst du kurz eine Rechnung für mich überweisen? Ich komm grad nicht ins Banking.“	Neue, unbekannte Nummer; „kein Zugriff aufs Online-Banking“; drängt auf schnelle Überweisung.	Nicht überweisen. Alte, gespeicherte Nummer anrufen oder eine Sprachnachricht verlangen. Eine Frage stellen, die nur das echte Kind beantworten kann.
Phishing (E-Mail)	„Ihr Konto wurde gesperrt. Bestätigen Sie sofort Ihre Daten über den folgenden Link, sonst wird Ihr Zugang gelöscht.“	Dringlichkeit, Link zum „Bestätigen“, Abfrage von Passwort/TAN. Bank und Behörde fragen so etwas NIE per Mail.	Nicht klicken. Bank-App öffnen oder Adresse selbst eintippen. Im Zweifel Bank über die Nummer auf der Karte anrufen.
Smishing (Paket-SMS)	„DHL: Ihr Paket wartet. Bitte begleichen Sie die offene Zollgebühr von 2,99 € über diesen Link.“	SMS mit Zahlungs-Link, angebliche „Gebühr“ oder „falsche Adresse“, teils absichtliche Tippfehler.	Nicht klicken. Paketdienste verlangen nie Vorab-Zahlung per SMS-Link. SMS löschen, Sendung nur in der offiziellen App prüfen.
Quishing (QR-Code)	Aufgeklebter QR-Code am Parkautomaten oder an der Ladesäule: „Hier bequem per Handy bezahlen.“	Überklebter/beigelegter QR-Code führt auf eine gefälschte Bezahlseite, die Kreditkartendaten abgreift.	QR-Codes aus unerwarteten Mails, Briefen oder von überklebten Automaten nie scannen . Vor Ort am Automaten selbst zahlen.

Masche	Typischer Satz / Köder	Warnzeichen	Deine richtige Reaktion
Tech-Support-Scam	Pop-up: „Windows-Sicherheitswarnung! Ihr PC ist infiziert. Rufen Sie sofort die Microsoft-Hotline an.“ Dann: „Der Ingenieur braucht Fernzugriff.“	Angebliche Warnung mit Rufnummer, Bitte um Fernwartung (AnyDesk/TeamViewer), Zahlung „Wartungspaket“ (bis ~400 €).	Microsoft ruft NIE unaufgefordert an. PC vom Internet trennen, niemandem Fernzugriff geben, keine Zahlung. Danach Passwörter ändern.
Anlagebetrug (Cybertrading)	„Garantierte Rendite. Sehen Sie selbst, wie Ihr Depot wächst — legen Sie einfach noch etwas nach.“ (oft über WhatsApp, mit Deepfake-Promi-Video)	„Garantierte“ hohe Gewinne, Druck zum Nachschießen, Anwerbung per WhatsApp/Anruf, gefälschtes Depot mit Scheingewinnen.	Nichts einzahlen. Niemand Seriöses wirbt per WhatsApp um Geldanlagen. Anbieter in der BaFin-Warnliste prüfen.
Romance Scam („Pig Butchering“)	„Ich habe mich in dich verliebt. Lass uns eine gemeinsame Zukunft aufbauen — ich zeige dir, wie wir zusammen investieren können.“	Schnelle Gefühle, nie ein echter Videocall, ständig neue Ausreden, am Ende immer ein Geld- oder Anlagethema.	Kein Geld an nie persönlich getroffene Kontakte. Auf Videocall bestehen. Mit einer Vertrauensperson darüber sprechen.
Gewinnversprechen	„Herzlichen Glückwunsch! Sie haben 50.000 € gewonnen. Zur Auszahlung überweisen Sie bitte nur die Bearbeitungsgebühr.“	„Gewinn“ für ein Gewinnspiel, an dem du nie teilgenommen hast; Vorkasse für „Gebühr“ oder „Steuer“.	Nicht zahlen, nicht antworten. Echte Gewinne verlangen nie eine Vorab-Gebühr. ⚠️ geschätzter Jahresschaden >50 Mio. €.

Die 3 goldenen Regeln (gilt für ALLE Zeilen oben)

1. **Auflegen.** Auflegen ist nie unhöflich. Es schließt das Stressfenster, das die Täter brauchen.
2. **Selbst zurückrufen** — über die echte, bekannte Nummer. Niemals über die Nummer im Display oder aus der Nachricht.
3. **Niemals unter Zeitdruck** Geld überweisen, Bargeld übergeben oder Daten/TAN herausgeben.

Wenn du nur eine Sache aus diesem Kurs mitnimmst, dann diese drei Sätze. Häng die Karte neben das Telefon. Im Ernstfall zählt nicht, was du weißt — sondern was du reflexartig tust.

Dein Schritt heute: Druck diese Karte aus und leg sie neben das Telefon. Häng eine zweite Kopie an den Kühlschrank deiner Eltern oder Großeltern.