BETRUG

DAS WUTBUCH

Über Finanzhaie, Schockanrufer, falsche Polizisten, digitale Fallen - und einen Staat, der seine Bürger besser schützen muss

KEIN SACHBUCH DER KÜHLEN DISTANZ

Dieses Buch ist eine polemische Anklage gegen Betrug und gegen strukturelle Schwächen, die Betrug erleichtern. Personennamen werden bewusst nicht genannt. Fakten, Rechtslage und offene Fragen werden voneinander getrennt.

Stand: 14. September 2026

Hinweis zur Einordnung

Dieses Buch ist ein Wutbuch. Es will nicht neutral klingen, wenn Menschen durch Betrug Ersparnisse, Altersvorsorge, Sicherheit und Vertrauen verlieren. Es ist bewusst scharf formuliert. Scharf bedeutet hier aber nicht schlampig: Wo konkrete Verfahren, Gesetze oder Statistiken angesprochen werden, werden die Tatsachen von Wertungen getrennt.

Personennamen werden vollständig weggelassen. Auch bei öffentlich bekannten Straf- oder Anlagekomplexen geht es hier nicht um persönliche Abrechnung, sondern um Strukturen: um Tatgelegenheiten, technische Lücken, die Geschwindigkeit von Ermittlungen und Gerichten, die Verantwortung von Banken und Plattformen sowie um die Frage, ob Opferschutz in Deutschland denselben politischen Druck erhält wie Täterrechte und Verfahrenssorgfalt.

Die Darstellung eines Ermittlungs- oder Anklagevorwurfs ist keine Feststellung von Schuld. Für Beschuldigte und Angeklagte gilt die Unschuldsvermutung, bis eine rechtskräftige Verurteilung vorliegt. Wo ein öffentlich dokumentierter Fall als Beispiel verwendet wird, wird deshalb beschrieben, was Behörden, Gerichte oder Parlamente mitgeteilt haben - und was gerade noch nicht entschieden ist.

Dieses Buch ersetzt keine Rechtsberatung. Wer aktuell von Betrug betroffen ist, sollte schnell handeln: Bank oder Zahlungsdienstleister kontaktieren, Belege sichern, Passwörter ändern, gegebenenfalls Karten und Konten sperren und Strafanzeige erstatten. Für akute Gefährdungen gilt der Notruf. Eine kompakte Notfallliste steht am Ende dieses Buches.

Inhalt

Teil I - Die Wut: Warum Betrug Lebenszeit stiehlt
1. Das Geld war nicht übrig - es war Lebenszeit
2. Die Täter verkaufen nicht Produkte, sondern Gefühle
3. Scham ist der zweite Diebstahl
4. Zahlen, die jede Gelassenheit verbieten

Teil II - Tatort Telefon
5. Mama, ich hatte einen Unfall
6. Falsche Polizisten und die gestohlene Autorität
7. Call-ID-Spoofing: Die Nummer im Display kann lügen
8. KI-Stimmen, Silent Calls und der nächste Betrugsschub

Teil III - Das große Geld
9. Anlagebetrug: Hochglanz über dem Abgrund
10. Cybertrading, Krypto und die Renditefabrik im Browser
11. Schneeballsysteme: Bezahlt wird mit dem Geld der Nächsten
12. Ein Hamburger Großverfahren und die Frage nach der Zeit

Teil IV - Der digitale Basar der Täuschung
13. Phishing, Smishing und falsche Paketboten
14. Fake-Shops, Marktplätze und Identitätsdiebstahl
15. Romance Scam: Wenn Nähe zur Waffe wird
16. Rechnungsbetrug, Chef-Masche und manipulierte Zahlungswege

Vertiefung - Weitere Betrugswelten, die täglich Geld vernichten
16A. Der falsche Bankmitarbeiter und der Fernzugriff
16B. Recovery Scam: Wenn der Betrug nach dem Betrug weitergeht
16C. Finanzagenten und Money Mules
16D. Job-Scams: Wenn Arbeitssuche zum Einfallstor wird

16E. Gewinnspiele, Abofallen und falsches Inkasso
16F. Erbschaften, Lotterien und der internationale Millionenbrief
16G. Warum Täter so oft im Ausland sitzen
16H. Warum wir Betrug nicht nur nach Schadenssumme bewerten dürfen
16I. Die „Hallo Mama, neue Nummer“-Masche
16J. Tech-Support-Betrug
16K. QR-Code-Betrug
16L. SIM-Swapping und Kontoübernahme
16M. Mietbetrug und falsche Immobilien
16N. Urlaubsbetrug
16O. Geschenkkarten als Betrugszahlung
16P. Falsche Spenden und Katastrophenbetrug
16Q. Die große Lehre: Kein Kanal ist mehr automatisch echt
Teil V - Wo der Staat stärker sein muss
17. Banken: Die letzte Notbremse vor der Übergabe
18. Telekommunikation: Verboten, aber technisch noch möglich
19. Plattformen: Reichweite darf nicht nur Gewinn bedeuten
20. Justiz: Sorgfalt ja - Stillstand nein
21. Offener Vollzug: Resozialisierung braucht belastbare Prognosen
22. Wohnort, Zuständigkeit und der Eindruck vom Wunschgefängnis
Teil VI - Was sich ändern muss
23. Vermögen schneller sichern, Geldströme schneller stoppen
24. Ein nationaler Betrugsschutz mit echter Zuständigkeit
25. Das 20-Punkte-Manifest gegen die Abzocke
26. Schluss: Macht Täter nervös, nicht Opfer
Anhang - Notfallplan, Warnsignale, Gesprächssätze, Quellen

Vier Zahlen, bevor die Wut beginnt

743.472	registrierte Betrugsfälle mit Tatort Deutschland im Jahr 2024.
513.518	zusätzliche Betrugsfälle, die laut BKA aus dem Ausland heraus mit Erfolgsort Deutschland begangen wurden.
nur etwa 20 %	der Betrugsdelikte werden nach BKA-Einschätzung überhaupt angezeigt - das Dunkelfeld ist groß.
61.358	Fälle von Wirtschaftskriminalität 2024; gegenüber 2023 ein Anstieg um 57,6 Prozent in der PKS.

Diese Zahlen stammen aus der Polizeilichen Kriminalstatistik 2024 beziehungsweise aus einer BKA-Auswertung zur Betrugskriminalität. Sie sind kein Beweis dafür, dass heute jeder zweite Anruf ein Betrugsversuch ist. Sie zeigen aber, dass wir nicht über ein Randphänomen reden. Wir reden über ein Massendelikt mit digitaler Infrastruktur, grenzüberschreitender Arbeitsteilung und einem Dunkelfeld, das vermutlich größer ist als das Hellfeld. [Q1][Q2]

TEIL I

DIE WUT

Warum Betrug nicht nur Geld, sondern Lebenszeit stiehlt

1. Das Geld war nicht übrig - es war Lebenszeit

Es gibt eine sterile Sprache für Betrug. Sie spricht von Vermögensschäden, Schadenssummen, Transaktionen, Anlagevolumen und Rückabwicklungen. Diese Sprache ist juristisch notwendig. Menschlich ist sie oft eine Beleidigung. Denn 50.000 Euro sind für einen normalen Haushalt nicht einfach eine Zahl. Sie können zehn Jahre Verzicht sein. Sie können Nachtschichten sein, ein kleineres Auto, ausgelassene Urlaube, ein Leben ohne Luxus und der feste Satz: Im Alter will ich niemandem zur Last fallen.

Wer einem Menschen 50.000 Euro betrügerisch abnimmt, nimmt deshalb nicht nur Geld. Er eignet sich rückwirkend Arbeitszeit an. Er macht aus Stunden, die jemand in einer Werkhalle, im Krankenhaus, im Büro, auf dem Bau, in der Pflege oder im Verkauf verbracht hat, den eigenen Gewinn. Das ist der Kern meiner Wut: Der Täter investiert einige Telefonate, eine präparierte Website, einen falschen Ausweis oder einen überzeugenden Prospekt - das Opfer investierte vielleicht ein halbes Berufsleben.

Besonders brutal wird es im Alter. Ein Dreißigjähriger, der Geld verliert, kann - mit Glück, Gesundheit und Arbeit - neu anfangen. Eine Siebzigjährige kann nicht einfach weitere dreißig Jahre sparen. Ein Betrug im Ruhestand kann endgültig sein. Deshalb ist der Satz „Sie hätte besser aufpassen müssen“ so billig. Er ignoriert die Asymmetrie. Auf der einen Seite steht ein professionelles System, auf der anderen ein Mensch, der nur einmal in seinem Leben genau diese Masche erlebt.

Wir müssen aufhören, Opfer nach ihrer vermeintlichen Naivität zu sortieren. Niemand fragt nach einem Wohnungseinbruch zuerst, ob das Opfer vielleicht ein zu hübsches Sofa im Fenster hatte. Bei Betrug geschieht genau das ständig. War die Rendite nicht zu hoch? Warum hat er das Passwort eingegeben? Warum hat sie das Geld übergeben? Natürlich sind Vorsicht und Aufklärung wichtig. Aber die moralische Hauptlast gehört dorthin, wo sie hingehört: zum Täter.

Der gesellschaftliche Schaden ist größer als die Schadenssumme. Wer betrogen wurde, vertraut danach vielleicht keiner Bank, keiner Nummer, keinem Berater, keiner Online-Anzeige, manchmal nicht einmal mehr der eigenen Urteilskraft. Ein gelungener Betrug erzeugt deshalb einen zweiten Schaden: Er macht Menschen kleiner. Er lässt sie zweifeln, schweigen, sich zurückziehen. Und genau das ist der Punkt, an dem aus privatem Verlust ein öffentliches Problem wird.

WUTSATZ

Wer Ersparnisse stiehlt, stiehlt nicht nur Besitz. Er stiehlt die Zeit, in der dieses Geld verdient wurde.

2. Die Täter verkaufen nicht Produkte, sondern Gefühle

Betrug funktioniert selten, weil eine Lüge besonders kompliziert ist. Er funktioniert, weil sie ein Gefühl im richtigen Moment trifft. Angst. Gier. Scham. Liebe. Autoritätsgläubigkeit. Zeitdruck. Einsamkeit. Hilfsbereitschaft. Der professionelle Betrüger fragt nicht zuerst: Was kann ich dem Opfer verkaufen? Er fragt: Welchen inneren Knopf kann ich drücken?

Der Schockanrufer verkauft keine Kaution. Er verkauft die Hoffnung, das eigene Kind vor dem Gefängnis zu retten. Der Anlagebetrüger verkauft keine Beteiligung. Er verkauft die Sehnsucht nach finanzieller Sicherheit. Der Romance-Scammer verkauft keine Überweisung. Er verkauft Nähe. Der falsche Bankmitarbeiter verkauft keinen Sicherheitscode. Er verkauft die Beruhigung, dass das Konto angeblich gerettet werden kann. Der Phisher verkauft keine Login-Seite. Er verkauft Dringlichkeit.

Das erklärt auch, warum intelligente Menschen Opfer werden. Intelligenz ist kein permanent eingeschalteter Betrugsdetektor. Wer erschrickt, verliebt ist, unter Zeitdruck steht oder glaubt, mit einer Behörde zu sprechen, denkt anders als in einem ruhigen Seminarraum. Täter bauen ihre Geschichten genau um diesen Moment. Sie verhindern Rückfragen. Sie halten das Opfer am Telefon. Sie verbieten Kontakt zu Angehörigen. Sie behaupten, Geheimhaltung sei Teil eines Polizeieinsatzes. Sie erzeugen einen Tunnel.

Wir sollten Betrugsprävention deshalb nicht wie einen IQ-Test behandeln. Die bessere Frage lautet: Welche Schutzschichten bauen wir um Menschen herum, wenn ihr Urteilsvermögen gerade absichtlich angegriffen wird? Banken können ungewöhnliche Bargeldabhebungen hinterfragen. Telekommunikationsanbieter können manipulierte Anruferkennungen stärker filtern. Plattformen können Werbung schneller stoppen. Behörden können schneller warnen. Angehörige können Codewörter vereinbaren.

Die gefährlichste Illusion ist die Vorstellung, man selbst sei zu schlau für Betrug. Genau diese Selbstsicherheit macht unvorsichtig. Professionelle Täter brauchen keinen dummen Menschen. Sie brauchen nur einen klugen Menschen im falschen Moment.

3. Scham ist der zweite Diebstahl

Nach dem Geld kommt oft die Scham. Menschen erzählen ihrer Familie nicht, was passiert ist. Sie gehen zu spät zur Polizei. Sie löschen Nachrichten, weil sie sich nicht noch einmal ansehen wollen, wie sie getäuscht wurden. Sie verschweigen Verluste aus Angst, als naiv, gierig oder senil abgestempelt zu werden. Und damit schenkt die Gesellschaft dem Täter einen zweiten Sieg.

Scham ist für Betrüger wirtschaftlich nützlich. Sie senkt die Anzeigequote, erschwert Warnungen, verzögert Kontosperren und schützt Serien. Wenn Opfer schweigen, kann dieselbe Masche beim nächsten Menschen weiterlaufen. Deshalb muss der Satz nach einem Betrug lauten: „Zeig es an. Sichere alles. Erzähl es.“ Nicht: „Wie konntest du nur?“

Gerade ältere Menschen fürchten zusätzlich, Angehörige könnten ihnen nach einem Betrug die Fähigkeit absprechen, ihre Finanzen selbst zu regeln. Wer glaubt, eine Offenlegung koste Selbstständigkeit, schweigt eher. Prävention muss deshalb würdevoll sein. Sie darf Senioren nicht behandeln, als seien sie Kinder. Sie muss ihnen Werkzeuge geben, nicht Misstrauen gegen die eigene Kompetenz.

Das Gleiche gilt für Anlagebetrug. Wer 100.000 Euro in eine vermeintlich sichere Anlage gesteckt hat, möchte vielleicht nicht hören, dass Außenstehende das Angebot „doch sofort komisch“ gefunden hätten. Hinterher ist jeder Prospekt transparent, jede rote Flagge neonfarben. Vorher sah sie womöglich aus wie ein Siegel, ein Prüfbericht, ein bekannter Markenname oder eine seriöse Veranstaltung.

Opferschutz beginnt deshalb mit Sprache. Betrüger sind verantwortlich für Betrug. Punkt. Wer das Opfer aufklärt, ohne es zu demütigen, erhöht die Chance, dass Straftaten sichtbar werden. Wer spottet, arbeitet unbeabsichtigt für die Täter.

4. Zahlen, die jede Gelassenheit verbieten

Das Bundeskriminalamt registrierte für 2024 743.472 Betrugsfälle mit Tatort Deutschland. Hinzu kamen 513.518 Fälle, die aus dem Ausland heraus begangen wurden und ihren Erfolgsort in Deutschland hatten. Gleichzeitig weist das BKA darauf hin, dass nur ungefähr ein Fünftel aller Betrugsdelikte angezeigt wird. [Q1] Schon die amtlich sichtbare Oberfläche ist riesig. Das Dunkelfeld macht jede Selbstberuhigung unseriös.

Die Zahl der registrierten Betrugsdelikte war gegenüber dem Vorjahr zwar leicht rückläufig. Das klingt zunächst beruhigend. Gleichzeitig beschreibt das BKA internationale Tatbegehung und digitale Strukturen als

zentrale Herausforderung. Kriminalität wird skalierbar: Eine Tätergruppe muss nicht mehr in derselben Stadt sitzen wie das Opfer. Sie kann Callcenter, Zahlungswege, Domains, Konten und Kuriere über Länder verteilen.

Besonders auffällig war in der PKS 2024 auch die Wirtschaftskriminalität: 61.358 Fälle, ein Anstieg um 57,6 Prozent gegenüber 2023. [Q2] Statistiken sind immer erklärungsbedürftig; sie hängen von Erfassung, Kontrollen, Großverfahren und Anzeigeverhalten ab. Aber wer aus solchen Zahlen nur den Satz „insgesamt etwas weniger Betrug“ zieht, hat das Problem nicht verstanden.

Das eigentliche Warnsignal ist die industrielle Form. Betrug ist nicht mehr nur der einzelne Hochstapler mit schlechter Visitenkarte. Es gibt Plattformen, Affiliate-Strukturen, Social-Engineering-Skripte, gestohlene Identitäten, KI-generierte Werbung, professionell gestaltete Dashboards, Übersetzer, Kontenkuriere und Geldwäscheketten. Das ist Arbeitsteilung. Nur eben kriminell.

Und deshalb braucht die Antwort ebenfalls Arbeitsteilung: Polizei, Justiz, Finanzaufsicht, Banken, Telekommunikationsunternehmen, Plattformen und Verbraucherschutz. Wer den Bürger alleine in die Mitte stellt und ihm zuruft „Sei wachsam!“, hat aus einem Systemproblem eine private Hausaufgabe gemacht.

TEIL II

TATORT TELEFON

Wie Angst, Autorität und Technik zu einer Waffe werden

5. „Mama, ich hatte einen Unfall“

Das Telefon klingelt. Eine weinende Stimme. Kaum verständlich. „Mama?“ Mehr braucht es manchmal nicht. Das Gehirn ergänzt den Rest. Wer ein Kind hat, kennt diese automatische Bewegung: Erst helfen, dann prüfen. Genau darauf ist der Schockanruf gebaut.

Die Polizeiliche Kriminalprävention beschreibt die Masche klar: Täter geben sich als Angehörige, Polizisten, Rechtsanwälte oder andere Amtspersonen aus, behaupten einen schweren oder tödlichen Unfall und verlangen eine sofortige Kaution, um angeblich Untersuchungshaft zu verhindern. Geld, Gold oder Schmuck sollen übergeben werden. Echte Polizeibeamte verlangen niemals Geld am Telefon. [Q3]

Der raffinierte Teil ist nicht die Geschichte. Der raffinierte Teil ist die Dramaturgie. Das Opfer soll keine Pause bekommen. Es wird im Gespräch gehalten. Es darf niemanden anrufen. Jeder Zweifel wird als Zeitverlust umgedeutet: „Wollen Sie wirklich riskieren, dass Ihre Tochter in Haft kommt?“ Der Täter verwandelt Vernunft in Schuldgefühl.

Wer jetzt sagt, man müsse doch wissen, dass es in Deutschland keine 50.000-Euro-Bar-Kaution für die Tochter beim Telefonpolizisten gibt, unterschätzt den Schock. In einer ruhigen Minute ist die Geschichte absurd. In der Vorstellung, das eigene Kind habe gerade einen Menschen getötet, sieht die Welt anders aus. Professionelle Manipulation lebt davon, dass unser Körper schneller reagiert als unser juristisches Wissen.

Die schäbigste Pointe ist die Übergabe. Ein fremder Mensch erscheint, nimmt einen Umschlag oder Schmuck und verschwindet. Jahre der Ersparnis wechseln in Sekunden den Besitzer. Zurück bleiben Leere, Selbstvorwürfe und eine Familie, die plötzlich nicht nur über Geld, sondern über Vertrauen sprechen muss.

Warum schaffen wir es nicht, diese Masche gesellschaftlich so bekannt zu machen wie „Bei Rot stehen“? Jeder ältere Mensch sollte einen einzigen Satz auswendig kennen: Polizei und Staatsanwaltschaft holen keine Kaution in bar oder Schmuck an der Haustür ab. Und jede Bank sollte denselben Satz sichtbar am Schalter haben.

MERKSATZ

Ein echter Notfall verträgt eine Rückfrage. Ein Betrüger hasst die Pause.

6. Falsche Polizisten und die gestohlene Autorität

Es ist besonders widerwärtig, wenn Täter Vertrauen in den Staat selbst als Werkzeug benutzen. Uniform, Amtsdeutsch, Aktenzeichen, Dienststelle, Staatsanwalt, Haftbefehl - all diese Begriffe sind soziale Abkürzungen. Sie signalisieren: Hier spricht jemand mit Befugnis. Der falsche Polizist missbraucht nicht nur den einzelnen Menschen, sondern ein öffentliches Vertrauensgut.

Die Maschen variieren. Mal seien Einbrecher in der Nachbarschaft festgenommen worden, bei denen angeblich eine Liste mit dem Namen des Opfers gefunden wurde. Mal sei das Bankkonto unsicher. Mal müsse Bargeld „überprüft“ werden. Mal werde behauptet, Bankmitarbeiter seien Teil einer Bande. Das Ziel ist stets ähnlich: Das Opfer soll Werte herausgeben und gleichzeitig jeden echten Kontrollweg meiden.

Besonders perfide ist die Anweisung, niemandem etwas zu sagen. Geheimhaltung klingt in Krimis professionell. Im wirklichen Leben ist sie ein Warnsignal. Betrüger versuchen, den sozialen Schutzkreis abzuschalten. Kein Sohn, keine Nachbarin, kein Bankberater, keine echte Polizeidienststelle soll die Geschichte hören, bevor das Geld weg ist.

Hier kann Prävention konkret werden. Familien sollten nicht nur sagen „Pass auf Betrüger auf“. Sie sollten Szenarien durchspielen. Was tust du, wenn jemand behauptet, ich sei in Haft? Wen rufst du an? Welche Nummer wählst du selbst? Welches Familien-Codewort kennen nur wir? Wo liegt die Nummer der örtlichen Polizeidienststelle?

Und Banken müssen verstehen, dass manche Kunden am Schalter bereits Teil einer psychologischen Geiselnahme sind. Ein Opfer kann ausdrücklich behaupten, das Geld sei für ein Auto oder eine Renovierung, weil der Täter genau diese Ausrede vorgegeben hat. Ein gutes Warnsystem fragt deshalb nicht nur nach dem Verwendungszweck. Es fragt nach Druck, Geheimhaltung und Telefonkontakt.

7. Call-ID-Spoofing: Die Nummer im Display kann lügen

Wir haben Menschen jahrzehntelang beigebracht, auf die Nummer im Display zu schauen. Dann haben wir eine Telekommunikationswelt gebaut, in der genau diese Nummer manipuliert werden kann. Willkommen in einem technischen Widerspruch, den Kriminelle lieben.

Die Bundesnetzagentur beschreibt ausdrücklich, dass angezeigte Rufnummern gefälscht werden können. Es können reale Nummern unbeteiligter Dritter oder sogar Fantasienummern aufgesetzt werden. Die eigentliche Identität des Anrufers wird verschleiert. Diese Praxis wird als Call-ID-Spoofing bezeichnet und ist in den einschlägigen Konstellationen gesetzlich verboten. [Q4]

Noch frustrierender ist die technische Realität: Die Bundesnetzagentur erklärt selbst, dass sie keine eigenen technischen Verhinderungsmöglichkeiten besitzt. Eingriffsmöglichkeiten liegen bei Netzbetreibern und Telekommunikationsanbietern. In bestimmten Fällen ist sogar aus Verbindungsdaten nicht zuverlässig rekonstruierbar, woher der Anruf tatsächlich kam. [Q4]

Ja, es gibt Schutzregeln. Ja, seit Jahren wurden Vorgaben verschärft, gerade für aus dem Ausland kommende Anrufe mit aufgesetzten deutschen Rufnummern. Ja, die Bundesnetzagentur ordnet Abschaltungen an und veröffentlicht Maßnahmenlisten. [Q5] Das ist wichtig. Aber die Verbraucherfrage bleibt brutal einfach: Warum zeigt mein Telefon eine Identität an, die ich nicht als Identität behandeln darf?

Wir brauchen eine technische Vertrauensstufe. Eine verifizierte Nummer muss im Display anders aussehen als eine bloß übermittelte Absenderinformation. Banken, Behörden, Krankenhäuser, Versicherungen und Telekommunikationsanbieter sollten kryptografisch verifizierbare Anruferkennungen nutzen können. Der Verbraucher darf nicht gezwungen werden, in jeder Sekunde Telekommunikationsforensiker zu spielen.

Der Satz „Rufen Sie über die offizielle Nummer zurück“ ist richtig. Er ist aber eine Reparaturanweisung für ein System, dessen Anzeige zu leicht missverstanden werden kann. Sicherheit sollte nicht davon abhängen, ob eine erschrockene Achtzigjährige technische Metadaten misstrauischer bewertet als die Stimme eines angeblichen Polizeibeamten.

8. KI-Stimmen, Silent Calls und der nächste Betrugsschub

Der klassische Schockanruf brauchte Schauspiel. Die nächste Generation braucht möglicherweise nur wenige Sekunden Audiomaterial. Moderne Sprachsynthese kann Stimmen imitieren. Damit wird aus „Mama, ich hatte einen Unfall“ im schlimmsten Fall nicht mehr irgendeine weinende Stimme, sondern eine Stimme, die tatsächlich wie das eigene Kind klingt.

Das bedeutet nicht, dass jeder aktuelle Schockanruf bereits mit künstlicher Intelligenz arbeitet. Es bedeutet, dass eine alte Masche ein neues Werkzeug erhält. Die psychologische Architektur bleibt identisch: Schock, Zeitdruck, Autorität, Isolation. KI senkt lediglich die Produktionskosten der Glaubwürdigkeit.

Ähnlich funktionieren sogenannte Silent Calls. Das Telefon klingelt, am anderen Ende ist Stille. Solche Anrufe können unterschiedliche Ursachen haben; im Betrugskontext können sie dazu dienen, aktive Anschlüsse zu prüfen oder automatisierte Systeme vorzubereiten. Die Polizeiprävention warnte 2026 erneut vor solchen Erscheinungen. [Q6]

Die richtige gesellschaftliche Antwort kann nicht lauten: „Dann darf man eben keiner Stimme mehr glauben.“ Eine Gesellschaft, in der jede Stimme verdächtig ist, hat technisch kapituliert. Wir brauchen neue Gewohnheiten: Rückruf über bekannte Nummern, Familiencodewörter, verifizierte Kommunikationskanäle und klare Regeln für Banken und Behörden.

Vor allem brauchen wir Geschwindigkeit. Betrugsprävention darf nicht erst zwei Jahre nach einer neuen Technik reagieren. Kriminelle führen keine Konsultationsverfahren durch. Sie warten nicht auf DIN-Normen. Sie testen, was funktioniert, und skalieren es sofort. Staat und Wirtschaft müssen lernen, dass Missbrauchsschutz Teil der Produkteinführung ist, nicht ein Kapitel für später.

TEIL III

DAS GROSSE GELD

Wenn Hochglanz, Rendite und Vertrauen zum Tatwerkzeug werden

9. Anlagebetrug: Hochglanz über dem Abgrund

Anlagebetrug ist die elegante Schwester des Schockanrufs. Er schreit nicht. Er trägt Sakko. Er hat Diagramme. Er spricht von Sachwerten, Risikostreuung, exklusivem Zugang, garantierten Prozessen und konservativen Annahmen. Während der Schockanruf Angst beschleunigt, betäubt der Anlagebetrug Skepsis mit Seriosität.

Es gibt ein fatales Missverständnis: Menschen glauben, Betrug müsse billig aussehen. Schlechte Grammatik, dubiose Domain, aggressiver Verkäufer. In Wahrheit investieren professionelle Täter genau in die Oberfläche. Sie kopieren Marken, verwenden gestohlene Fotos, fälschen Bewertungen, bauen Kundenportale und beschäftigen Menschen, die souverän erklären können, warum gerade diese Anlage „anders“ sei.

Die Finanzaufsicht warnt regelmäßig vor unerlaubt betriebenen Plattformen, Identitätsmissbrauch und angeblichen Investmentangeboten. Sie rät, Anbieter zu prüfen, Warnmeldungen zu suchen und nichts zu kaufen, was man nicht versteht. [Q7] Das ist richtig. Aber es offenbart auch die Informationsasymmetrie: Der Verbraucher soll in einer Stunde prüfen, was eine Tätergruppe in Monaten gebaut hat.

Besonders gefährlich ist das Wort „sicher“. Eine Anlage kann real ein Risiko haben und dennoch seriös sein. Betrug beginnt dort, wo Risiken verschleiert, Tatsachen erfunden, Erlaubnisse vorgetäuscht oder Gelder anders verwendet werden als zugesagt. Hohe Rendite ist nicht automatisch Betrug. Aber hohe Rendite plus angebliche Sicherheit plus Zeitdruck plus intransparente Struktur ist eine Sirene, die man hören sollte.

Wir brauchen in der Finanzwerbung mehr Reibung. Wer risikoreiche oder komplexe Produkte an Kleinanleger vertreibt, sollte nicht nur einen zehnseitigen Risikohinweis irgendwo im PDF verstecken. Die Kernrisiken müssen so sichtbar sein wie der Zinssatz. Und Plattformen, die Finanzanzeigen verkaufen, sollten nicht so tun dürfen, als sei die Prüfung des Werbekunden ein fremdes Problem.

10. Cybertrading, Krypto und die Renditefabrik im Browser

Online-Anlagebetrug hat eine besondere Qualität: Das Opfer sieht sein Geld scheinbar wachsen. Ein Dashboard zeigt grüne Zahlen. Ein persönlicher „Broker“ gratuliert. Kleine Auszahlungen am Anfang schaffen Vertrauen. Dann wird die Einzahlung größer. Danach kommt die Steuer, die Freigabegebühr, die Sicherheitsleistung, die angebliche Geldwäscheprüfung - immer noch eine Zahlung, bevor das große Guthaben ausgezahlt werden könne.

Genau hier liegt die Magie des falschen Dashboards. Menschen glauben Zahlen auf einem Bildschirm, weil unser Alltag auf Zahlen auf Bildschirmen basiert. Onlinebanking ist real. Depots sind real. Börsenkurse sind real. Warum sollte ausgerechnet dieses professionell aussehende Konto erfunden sein? Weil die Anzeige nichts beweist. Eine Website kann jede Zahl darstellen, die ihr Betreiber eingibt.

BaFin und Strafverfolgungsbehörden warnen vor dubiosen Online-Handelsplattformen, die außergewöhnliche Gewinne versprechen. [Q8] Häufig erfolgt die Ansprache über Social Media, Werbung oder vermeintliche Prominentenempfehlungen. Die erste Einzahlung ist bewusst klein. Aus 250 Euro soll psychologisch eine Beziehung entstehen, nicht sofort ein Großschaden.

Danach beginnt das sogenannte „Butchering“: Vertrauen wird gemästet, bevor es geschlachtet wird. Der Begriff ist brutal, die Logik noch brutaler. Der Täter investiert Zeit in das Opfer, weil ein gut gepflegtes Opfer mehr zahlt. Beratungsgespräche, tägliche Anrufe, Marktkommentare, angebliche Sonderchancen - alles kann Teil des Skripts sein.

Und selbst nach dem Verlust ist die Jagd nicht vorbei. Dann melden sich angebliche Rückholfirmen, Rechtsberater oder Ermittler, die versprechen, das verschwundene Geld gegen eine Vorausgebühr wiederzubeschaffen. Recovery Scam nennt man diese zweite Ernte. Wer bereits verletzt ist, wird noch einmal angegriffen, diesmal mit Hoffnung statt Rendite.

11. Schneeballsysteme: Bezahlt wird mit dem Geld der Nächsten

Ein Schneeballsystem kann lange wie Erfolg aussehen. Ausschüttungen kommen pünktlich. Frühere Anleger berichten begeistert. Vermittler zeigen Kontoauszüge. Veranstaltungen sind gut besucht. Genau das ist das Problem: Solange neues Geld zufließt, kann eine Fassade erstaunlich stabil wirken.

Der fundamentale Unterschied zu einem tragfähigen Geschäftsmodell lautet: Woher kommt die Rendite? Aus echter wirtschaftlicher Leistung - oder aus dem Geld späterer Teilnehmer? Wenn die Antwort unklar ist, sollte jede weitere Frage lauter werden. Welche Vermögenswerte existieren? Wer verwahrt sie? Welche unabhängigen Prüfungen gibt es? Wie werden Rückzahlungen finanziert? Welche Erlaubnisse braucht das Geschäftsmodell?

Schneeballsysteme leben außerdem von sozialem Beweis. „Mein Nachbar bekommt seine Zinsen doch auch.“ Genau. Bis er sie nicht mehr bekommt. Frühzeitige Auszahlungen beweisen nicht die Gesundheit des Systems; in einem betrügerischen Modell können sie gerade die Werbung dafür sein.

Besonders tragisch sind Vertriebsnetzwerke, in denen Vermittler selbst gutgläubig sein können. Ein Mensch vertraut einem Berater, der wiederum einem Produktgeber vertraut. Wenn oben gelogen wird, verteilt sich die Täuschung durch eine Kette aus echten Beziehungen. Deshalb müssen Aufsicht und Produktprüfung dort greifen, wo der einzelne Anleger keine realistische Chance mehr hat, die Wahrheit zu verifizieren.

Und wenn das System zusammenbricht, folgt das juristische Nachleben: Insolvenz, Forderungsanmeldung, Anfechtung, Prospekthaftung, Strafverfahren, Zivilklagen. Für Geschädigte beginnt nach dem finanziellen Verlust eine zweite Vollzeitbeschäftigung - Papier, Fristen, Anwälte, Hoffnung. Auch das gehört zur Schadensbilanz.

12. Ein Hamburger Großverfahren und die Frage nach der Zeit

Es gibt Fälle, die zu Symbolen werden, weil sie eine größere Frage sichtbar machen. Ein solcher Fall ist ein Hamburger Anlagekomplex, bei dem über Jahre Gelder für Beteiligungsmodelle eingeworben wurden. Personennamen spielen hier keine Rolle. Entscheidend ist die Chronologie, die der Hamburger Senat selbst öffentlich dokumentiert hat.

Die Anklageschrift datiert vom 3. Juli 2020 und wurde am 8. Juli 2020 an das Landgericht Hamburg übersandt. Vier Personen wurde im Zusammenhang mit einem Fonds gemeinschaftlicher banden- und gewerbsmäßiger Betrug in 1.730 tateinheitlichen Fällen vorgeworfen; vier weiteren Beihilfe. Nach Darstellung der Anklage entstand in den angeklagten Fällen ein Vermögensschaden von mindestens rund 41 Millionen Euro. [Q9]

Der Umfang ist außergewöhnlich: Nach Senatsangaben wuchs die Hauptakte auf mehr als 5.500 Seiten, hinzu kamen 142 Umzugskartons mit Unterlagen, eine 235-seitige Anklageschrift, acht Angeschuldigte,

zahlreiche Verteidiger und Adhäsionskläger. [Q9] Niemand kann seriös behaupten, das sei ein Fall, den man an einem Freitagnachmittag zwischen zwei Bußgeldsachen erledigt.

Aber genau deshalb ist die Zeitfrage so explosiv. Am 4. April 2025 teilte der Hamburger Senat auf eine erneute parlamentarische Anfrage mit: Das Landgericht habe noch nicht über die Eröffnung des Hauptverfahrens entschieden. Für Wirtschaftsstrafkammern lag die durchschnittliche Dauer vom Eingang bis zum Eröffnungsbeschluss 2024 laut derselben Drucksache bei acht Monaten. [Q10] Der konkrete Großfall lag da seit fast fünf Jahren.

Das ist kein Beweis für Faulheit. Es ist kein Beweis für Rechtsbruch. Es ist ein Warnsignal über Kapazität, Komplexität und Priorisierung. Der Senat verwies auf die hohe Belastung des Strafbereichs, unter anderem durch aufwendige EncroChat-Verfahren. [Q10] Das mag erklären. Aber Erklärung ist nicht dasselbe wie Akzeptanz.

Für einen geschädigten Anleger lautet die Erfahrung nicht „komplexes Zwischenverfahren“. Sie lautet: Ich warte. Vielleicht seit dem Ende meiner Berufstätigkeit. Vielleicht mit einer Forderung, die mein gesamtes Erspartes betrifft. Der Rechtsstaat hat selbstverständlich die Pflicht, sorgfältig zu prüfen, ob eine Anklage zur Hauptverhandlung zugelassen wird. Er hat aber ebenso die Pflicht, Verfahren so auszustatten, dass Sorgfalt nicht zu jahrelanger Schwebe wird.

Besonders wichtig ist die sachliche Korrektur einer oft wiederholten Behauptung: In diesem Komplex ist nicht „bis heute keine Anklage zustande gekommen“. Die Anklage wurde 2020 erhoben. Der Kritikpunkt ist gerade schärfer: Die Anklage lag jahrelang beim Gericht, ohne dass über die Eröffnung entschieden war. Wer Kritik präzise formuliert, macht sie unangreifbarer.

In Medienberichten war für das weitere Firmengeflecht von mehreren Tausend Anlegern und Summen bis zu 200 Millionen Euro die Rede; die öffentlich dokumentierte Anklage selbst betrifft jedoch einen engeren Komplex. [Q11] Genau diese Trennung muss man einhalten. Wut braucht keine Übertreibung. Die belegten Dimensionen reichen völlig.

FRAGE AN DEN RECHTSSTAAT

Wie lange darf ein wirtschaftsstrafrechtliches Verfahren dauern, bevor seine Dauer selbst Vertrauen zerstört - auch wenn jede einzelne Verzögerung juristisch erklärbar ist?

TEIL IV

DER DIGITALE BASAR DER TÄUSCHUNG

Vom Paket-Link bis zur gestohlenen Identität

13. Phishing, Smishing und falsche Paketboten

Eine SMS: „Ihr Paket konnte nicht zugestellt werden.“ Ein Link. Zwei Euro Nachporto. Wer gerade tatsächlich auf ein Paket wartet - und wer wartet nicht ständig auf irgendein Paket? - hat den perfekten Moment. Der Betrag ist klein, die Handlung plausibel, das Risiko wirkt lächerlich. Genau deshalb funktioniert es.

Smishing verbindet SMS und Phishing. Das Ziel kann sein, Zugangsdaten abzugreifen, Schadsoftware zu installieren, Karteninformationen zu stehlen oder Abofallen auszulösen. Verbraucherzentralen warnen regelmäßig vor Nachrichten im Namen von Paketdiensten, Banken, Finanzämtern oder Gerichten. [Q12][Q13]

Das Muster ist immer ähnlich: eine vertraute Marke, ein plausibler Anlass, eine kleine Frist. „Ihr Konto wird gesperrt.“ „Ihre TAN-App muss aktualisiert werden.“ „Ihre Steuererstattung wartet.“ „Es gibt eine offene Forderung.“ Der Betrüger muss nicht beweisen, dass die Geschichte stimmt. Er muss nur erreichen, dass Sie schneller klicken als denken.

Besonders problematisch ist, dass echte Unternehmen uns jahrelang an Links in Nachrichten gewöhnt haben. Banken sagen zwar oft, sie würden nie bestimmte Daten per Mail abfragen - gleichzeitig schicken Unternehmen Marketinglinks, Loginlinks, Trackinglinks und App-Links. Sicherheit wird dadurch zu einer Stilfrage, die Laien erraten sollen.

Die bessere Regel lautet: Unerwartete Nachricht, eigener Weg. Nicht auf den Link tippen. App selbst öffnen. Adresse selbst eintippen. Telefonnummer selbst heraussuchen. Das klingt umständlich. Genau diese Umständlichkeit ist Sicherheitsgewinn. Betrug liebt Komfort ohne Pause.

14. Fake-Shops, Marktplätze und Identitätsdiebstahl

Der Fake-Shop ist die perfekte Karikatur des Onlinehandels: schöne Bilder, günstiger Preis, Countdown, Gütesiegel, „nur noch drei Stück“, deutsche Sprache, vielleicht sogar ein Impressum. Nur die Ware existiert nicht - oder der Betreiber ist nicht der, für den er sich ausgibt.

Verbraucherzentralen weisen darauf hin, dass Betrüger gestohlene oder manipulierte Fotos und Videos verwenden, bekannte Marken nachahmen und gefälschte Plattformen bauen. Fehlendes oder widersprüchliches Impressum, auffällige Domains und riskante Zahlungsarten sind Warnsignale. [Q14] Aber auch hier gilt: Ein professioneller Fake kann viele dieser Anfängerfehler vermeiden.

Noch schlimmer wird es beim Identitätsdiebstahl. Dann ist nicht nur Geld weg. Der eigene Name wird zum Tatwerkzeug. Verträge, Bestellungen, Konten oder Anzeigen tauchen auf. Das Opfer muss beweisen, dass es etwas nicht getan hat. Eine bizarre Umkehr: Der ehrliche Mensch verbringt Stunden damit, seine eigene Unschuld gegenüber automatisierten Mahnsystemen zu dokumentieren.

Plattformbetreiber müssen deshalb mehr Verantwortung für Identitätsprüfungen, Händlerhistorien und verdächtige Muster übernehmen. Wer tausende Transaktionen vermittelt und daran verdient, ist nicht bloß eine digitale Pinnwand. Er ist Teil der Infrastruktur. Infrastruktur hat Pflichten.

Auch Verbraucher brauchen pragmatische Regeln: Vorkasse bei unbekannten Shops ist ein Risiko. Extreme Preisabweichungen sind keine Einladung, sondern eine Frage. Gütesiegel müssen anklickbar und verifizierbar sein. Bewertungen dürfen nicht wie Naturgesetze behandelt werden. Und wenn ein Angebot nur noch 90 Sekunden gültig ist, ist die beste Reaktion oft, es 91 Sekunden lang zu ignorieren.

15. Romance Scam: Wenn Nähe zur Waffe wird

Beim Romance Scam ist die Tatwaffe keine Drohung, sondern Zuwendung. Nachrichten morgens und abends. Interesse an Details. Komplimente. Gemeinsame Zukunft. Vielleicht ein Beruf, der Entfernung erklärt: Militär, Medizin, Offshore, internationales Geschäft. Nähe wird sorgfältig dosiert, bis Vertrauen entsteht.

Dann kommt die Krise. Ein Zollproblem. Eine Operation. Ein blockiertes Konto. Eine Reise. Ein Paket. Eine Investitionschance. Geld wird nicht als Geld verlangt, sondern als Beweis der Beziehung. Wer Zweifel äußert, wird emotional bestraft: „Du vertraust mir also nicht?“

Das macht diese Form des Betrugs so zerstörerisch. Das Opfer verliert nicht nur Geld, sondern eine Beziehung, die psychologisch real war. Außenstehende sehen ein erfundenes Profil. Das Opfer erlebt Monate echter Gefühle. Spott ist hier besonders grausam und besonders kontraproduktiv.

Neuere Varianten verbinden Romance Scam mit Investmentbetrug. Die vermeintliche Partnerin oder der vermeintliche Partner empfiehlt eine Handelsplattform, angeblich aufgrund familiärer Kontakte oder eigener Erfahrung. So verschmelzen Intimität und Rendite. Der Täter muss nicht mehr kalt verkaufen; er empfiehlt als Vertrauensperson.

Prävention muss deshalb Beziehungen respektieren und trotzdem prüfen. Nie Geld an Menschen schicken, die man nicht sicher persönlich kennt. Keine Investmentplattform aufgrund einer Online-Beziehung nutzen. Bilder rückwärts suchen. Videotelefonie verlangen - wobei auch Video heute kein absoluter Echtheitsbeweis mehr ist. Vor allem: Angehörige nicht verspotten, wenn sie verliebt sind. Wer verspottet wird, erzählt beim nächsten Geldwunsch gar nichts mehr.

16. Rechnungsbetrug, Chef-Masche und manipulierte Zahlungswege

Nicht jeder Betrug zielt auf Senioren. Unternehmen sind genauso attraktiv. Beim Rechnungsbetrug wird eine echte Rechnung abgefangen oder nachgebaut und lediglich die Bankverbindung geändert. Beim CEO-Fraud erhält die Buchhaltung eine angebliche Nachricht der Geschäftsführung: streng vertraulich, dringend, hoher Betrag, keine Rückfragen.

Diese Maschen funktionieren, weil Unternehmen Effizienz trainieren. Rechnungen sollen schnell bezahlt, Hierarchien respektiert, Projekte vertraulich behandelt werden. Der Betrüger benutzt Unternehmensdisziplin gegen das Unternehmen. Ein gut gefälschter Mail-Thread kann stärker wirken als jede plumpe Drohung.

Die Gegenmaßnahme ist banal und deshalb unbeliebt: Vier-Augen-Prinzip. Rückruf. Getrennte Freigaben. Änderung einer Bankverbindung nie ausschließlich aufgrund einer E-Mail akzeptieren. Hohe Überweisung plus Geheimhaltung plus Zeitdruck ist kein Premiumservice, sondern ein Alarm.

Auch hier wird KI den Druck erhöhen. Texte werden sprachlich sauberer, Übersetzungen besser, Stimmen imitierbar. Das klassische Erkennungsmerkmal „schlechtes Deutsch“ verschwindet. Sicherheit muss von Inhaltsgefühl auf Prozesse wechseln. Nicht „klingt die Mail echt?“, sondern „wurde die Zahlung über einen zweiten Kanal verifiziert?“

Das ist eine zentrale Lektion dieses Buches: Wenn Täuschungen besser werden, dürfen Schutzsysteme nicht vom Erkennen der Täuschung abhängen. Sie müssen so gebaut sein, dass selbst eine perfekte Täuschung an einem unabhängigen Kontrollschritt scheitert.

VERTIEFUNG: Weitere Betrugswelten, die täglich Geld vernichten

Betrug ist kein einzelnes Deliktbild, sondern ein Baukasten. Dieselben psychologischen Bauteile - Autorität, Zeitdruck, Vertrauen, Geheimhaltung und künstliche Verknappung - tauchen in immer neuen Kombinationen auf. Die folgenden Kapitel vertiefen Maschen, die im Alltag besonders häufig miteinander verschmelzen.

16A. Der falsche Bankmitarbeiter und der Fernzugriff

Der Anruf klingt professionell: Auf Ihrem Konto gebe es eine verdächtige Überweisung. Zum Glück habe die Sicherheitsabteilung sie entdeckt. Jetzt müsse nur schnell gehandelt werden. Wer in diesem Moment erleichtert ist, hat bereits den ersten psychologischen Schritt gemacht: Der Täter erscheint nicht als Gefahr, sondern als Retter.

Als Nächstes kommt die angebliche Sicherheitsprüfung. TAN vorlesen. Push-Freigabe bestätigen. App installieren. Bildschirm teilen. Eine Software für Fernwartung laden. Was beim echten IT-Support sinnvoll sein kann, wird in der Hand eines Betrügers zur Fernbedienung des Kontos. Der Täter sieht, was das Opfer sieht, gibt Überweisungen ein oder führt es durch Freigaben, die als „Stornierung“ oder „Sicherheitsbuchung“ verkauft werden.

Die entscheidende Regel lautet: Eine Bank braucht nicht Ihre TAN, um Sie vor einer fremden Überweisung zu schützen. Freigabecodes sind keine Ausweisdokumente, die ein Mitarbeiter kontrolliert. Sie sind Schlüssel. Wer sie verlangt, will eine Tür öffnen. Und wer Sie auffordert, eine Fernzugriffssoftware zu installieren, gehört aus dem Gespräch - nicht auf Ihren Rechner.

Besonders gefährlich ist die Kombination mit Spoofing. Auf dem Display kann eine bekannte Nummer erscheinen. Vielleicht sogar die der Bank. Genau deshalb ist der einzige sichere Rückruf der selbst initiierte: Gespräch beenden, offizielle Banking-App öffnen oder Nummer von der Bankkarte beziehungsweise Website selbst wählen. Nicht Rückruftaste, nicht Nummer aus der SMS, nicht Nummer, die der Anrufer diktiert.

Banken sollten diese Regeln nicht im Kleingedruckten verstecken. Jede Freigabe-App könnte bei hohen oder ungewöhnlichen Transaktionen klar anzeigen: „Ein Bankmitarbeiter wird Sie niemals auffordern, diese Freigabe am Telefon zu bestätigen.“ Technik kann warnen, bevor der Finger tippt.

16B. Recovery Scam: Wenn der Betrug nach dem Betrug weitergeht

Wer Geld verloren hat, sucht Hoffnung. Genau in diesem Moment tauchen „Rückholer“ auf: angebliche Kanzleien, Ermittler, Blockchain-Spezialisten, Behördenkontakte oder Recovery-Agenturen. Sie wissen erstaunlich genau, wie der erste Betrug ablief. Manchmal deshalb, weil dieselben Daten verkauft oder innerhalb des Täterumfelds weitergegeben wurden.

Die Geschichte klingt diesmal seriöser. Das Geld sei gefunden. Eine Wallet sei eingefroren. Eine internationale Behörde habe eine Rückzahlung genehmigt. Es fehle nur noch eine Steuer, eine Freischaltungsgebühr, eine Versicherung, eine notarielle Bestätigung oder eine Anti-Geldwäsche-Kaution. Wer schon 80.000 Euro verloren hat, zahlt vielleicht weitere 2.000, um die 80.000 zu retten.

Das ist psychologisch perfide, weil der Verlust selbst zum Druckmittel wird. Menschen handeln nach dem Prinzip: Jetzt darf ich nicht aufgeben. Der Täter nennt das nicht „noch einmal zahlen“, sondern „den letzten Schritt“. Danach kommt regelmäßig der wirklich letzte Schritt. Und danach der allerletzte.

Eine seriöse Rückgewinnung kann Kosten verursachen. Aber sie sollte überprüfbare Identitäten, schriftliche Mandate, nachvollziehbare Gebühren und realistische Erfolgsaussichten haben. Niemand kann verlorene Kryptowerte allein deshalb garantieren, weil er eine angebliche Transaktions-ID vorzeigt. Wer vor der Auszahlung immer neue Gebühren verlangt, ist ein Alarmfall.

Die Aufklärung über Recovery Scams muss automatisch Teil jeder Betrugsanzeige sein. Wer einmal Opfer wurde, hat ein erhöhtes Risiko für den zweiten Angriff - nicht weil er „leichtgläubig“ ist, sondern weil Täter wissen, dass Hoffnung nach Verlust besonders gut verkauft werden kann.

16C. Finanzagenten und Money Mules: Der Mensch als Durchlaufkonto

Betrug braucht Geldwege. Gestohlenes Geld soll nicht auf einem Konto liegen bleiben, das direkt mit der Tätergruppe verbunden ist. Deshalb werden sogenannte Finanzagenten oder Money Mules angeworben: Menschen, die ihr Konto zur Verfügung stellen, Zahlungen empfangen und weiterleiten.

Manche wissen, was sie tun. Andere glauben an einen Nebenjob. „Zahlungsabwickler“, „Testkunde“, „Account Manager“, „Krypto-Assistent“ - die Berufsbezeichnungen klingen modern, die Aufgabe ist alt: fremdes Geld weiterreichen. Als Lohn darf ein kleiner Prozentsatz behalten werden.

Für Betrugsopfer ist diese Kette fatal. Sobald Geld weiterverteilt, abgehoben oder in Kryptowerte getauscht wurde, sinkt die Chance auf Rückholung. Für den Finanzagenten kann es ebenfalls böse enden: Konto gesperrt, Ermittlungsverfahren, Rückforderungsansprüche, Schufa- und Bankprobleme.

Hier müssen Banken Muster früher erkennen. Viele Zahlungseingänge von unbekannten Personen, sofortige Weiterleitungen, plötzlich stark verändertes Kontoverhalten - das sind Signale. Gleichzeitig muss Aufklärung klar sagen: Kein seriöser Arbeitgeber braucht Ihr Privatkonto, damit Sie Kundengelder für ihn „weiterleiten“.

Betrugsbekämpfung bedeutet deshalb nicht nur, den Anrufer zu finden. Sie bedeutet, das Ökosystem zu zerstören: Konten, Kuriere, SIM-Karten, Domains, Zahlungsdienste, Krypto-Offramps und Werbekanäle. Eine Bande ist nur so schnell wie ihre Infrastruktur.

16D. Job-Scams: Wenn Arbeitssuche zum Einfallstor wird

Wer einen Job sucht, ist offen für Kontakt. Genau das nutzen Betrüger. Eine Nachricht verspricht einfache Heimarbeit, gute Bezahlung und flexible Zeiten. Erst sollen Produkte bewertet, Zahlungen getestet, Pakete weitergeschickt oder Konten „verifiziert“ werden. Später wird Geld verlangt oder die eigene Identität missbraucht.

Besonders perfide sind sogenannte Task-Scams. Das Opfer erledigt kleine digitale Aufgaben und sieht in einer App ein wachsendes Guthaben. Für höher bezahlte Aufgaben müsse es eigenes Geld „vorstrecken“. Anfangs kann sogar eine kleine Auszahlung erfolgen. Dann werden die Aufgaben teurer, das angebliche Guthaben größer - und die Auszahlung blockiert.

Andere Job-Scams zielen auf Ausweisdaten. Ein vermeintlicher Arbeitgeber verlangt Vorder- und Rückseite des Personalausweises, Selfie, Bankverbindung und Videoident. Später werden mit diesen Daten Konten eröffnet, Verträge geschlossen oder weitere Opfer getäuscht.

Arbeitsplattformen müssen Stellenanzeigen deshalb nicht nur auf politische oder diskriminierende Inhalte prüfen, sondern auf Betrugsindikatoren. Arbeitgeberidentität, Domainalter, Zahlungsaufforderungen und massenhafte identische Anzeigen sind technisch prüfbar.

Für Bewerber gilt: Ein Arbeitgeber zahlt Ihnen Geld; Sie finanzieren nicht erst seine Geschäftsabläufe. Wer vor Arbeitsbeginn Gebühren, Kryptokäufe, Gutscheinkarten oder Zahlungen an „Lieferanten“ verlangt, bietet wahrscheinlich keinen Job, sondern sucht ein Opfer.

16E. Gewinnspiele, Abofallen und falsches Inkasso

„Herzlichen Glückwunsch, Sie haben gewonnen.“ Dieser Satz ist eine der ältesten Eintrittskarten in den Betrug. Der Gewinn existiert angeblich, aber vor der Auszahlung fehlen Bearbeitungsgebühr, Steuer, Transport, Versicherung oder eine kostenpflichtige Mitgliedschaft. Ein Gewinn, für den man immer wieder bezahlen muss, ist vor allem eines: teuer.

Abofallen arbeiten subtiler. Ein Probeangebot, ein Streamingdienst, eine Datingseite, ein Gewinnspiel oder ein vermeintlicher Gutschein führt zu einem Vertrag, den der Verbraucher so nicht erwartet hat. Danach kommen Rechnungen und Mahnungen. Nicht jede streitige Rechnung ist Betrug - aber Täter imitieren bewusst die Sprache seriösen Forderungsmanagements.

Falsches Inkasso setzt auf Angst vor Schufa, Gerichtsvollzieher und Gerichtsverfahren. Die Forderung ist klein genug, dass viele lieber zahlen als prüfen. Genau diese Bequemlichkeit wird monetarisiert. Deshalb gilt: Forderungsgrund, Gläubiger, Vertragsdatum, Aktenzeichen und Bankverbindung prüfen. Nicht unter Zeitdruck auf Links in SMS klicken.

Der Staat muss bei massenhaften falschen Forderungen schneller gegen Zahlungswege und Kommunikationsinfrastruktur vorgehen. Tausend einzelne Verbraucherbeschwerden sind kein tausendfaches Einzelfallproblem, sondern ein Muster.

Und Unternehmen sollten ihre Marken aktiv verteidigen. Wenn Betrüger regelmäßig im Namen eines Paketdienstes, Zahlungsdienstes oder Händlers auftreten, ist Betrugsprävention Teil des Markenschutzes. Wer Vertrauen als Geschäftsgrundlage nutzt, muss auch investieren, wenn dieses Vertrauen missbraucht wird.

16F. Erbschaften, Lotterien und der internationale Millionenbrief

Die klassische Vorschussbetrugsmasche ist beinahe Folklore: Ein unbekannter Anwalt, Banker, Prinz, Erbe oder Regierungsbeamter braucht Hilfe, um Millionen außer Landes zu bringen. Dafür soll der Empfänger einen Anteil erhalten. Vorher fallen nur kleine Gebühren an. Dann größere. Dann sehr große.

Was heute lächerlich klingt, war nie auf maximale Plausibilität angewiesen. Betrug ist ein Filtergeschäft. Eine extrem unglaubwürdige Geschichte sortiert skeptische Menschen früh aus. Wer antwortet, ist aus Sicht des Täters interessanter. Danach beginnt persönliche Bearbeitung.

Moderne Varianten sind besser. Sie verwenden echte Kanzleinamen, gestohlene Briefköpfe, nachgebaute Websites und plausibel klingende Erbfälle. Vielleicht existiert sogar ein realer Verstorbener gleichen Nachnamens. Das Internet liefert genug Daten, um Zufall wie Schicksal aussehen zu lassen.

Die Grundregel bleibt: Eine echte Erbschaft verlangt nicht, dass ein zufällig angeschriebener Fremder Gebühren an private Konten, Geldtransferdienste oder Kryptoadressen zahlt. Lotterien zahlen Gewinnern Geld; sie verkaufen nicht im Nachhinein die Freigabe des Gewinns.

Diese alten Maschen sind wichtig, weil sie zeigen: Technik ändert die Verpackung, nicht die menschlichen Hebel. Hoffnung auf Reichtum, Angst vor Verlust, Respekt vor Autorität und Wunsch nach Zugehörigkeit sind älter als das Internet - und deshalb werden Betrüger sie auch nach der nächsten technischen Revolution benutzen.

16G. Warum Täter so oft im Ausland sitzen - und warum das keine Ausrede sein darf

Das BKA weist auf die enorme Zahl von Betrugsfällen hin, die aus dem Ausland heraus mit Erfolgsort Deutschland begangen werden. [Q1] Das ist für Ermittler ein reales Problem: Daten liegen bei ausländischen Providern, Konten in anderen Rechtsordnungen, Callcenter wechseln Standorte, Rechtshilfe kostet Zeit.

Für den Bürger darf „Ausland“ trotzdem nicht zum Synonym für „unlösbar“ werden. Banken arbeiten global in Sekunden. Plattformen schalten global Werbung in Millisekunden. Telekommunikationsnetze routen global. Strafverfolgung muss wenigstens in den wichtigsten Betrugsphänomenen vergleichbare Schnellkanäle entwickeln.

Erfolgreiche Bekämpfung braucht Joint Investigation Teams, standardisierte Datenerhaltung, schnelle Providerkontakte, koordinierte Kontensperren und spezialisierte Staatsanwälte. Es ist ineffizient, wenn jedes örtliche Revier denselben internationalen Sachverhalt von Null aus entdeckt.

Gleichzeitig sollte Deutschland dort ansetzen, wo es Hoheit hat: deutsche Empfängerkonten, hiesige Werbekunden, SIM-Karten, Hosting, Domainregistrare, Bargeldkuriere und Finanzagenten. Eine internationale Bande braucht lokale Brücken. Diese Brücken sind angreifbar.

Internationalität erklärt Schwierigkeit. Sie darf aber nicht zur rhetorischen Endstation werden. Organisierte Kriminalität plant grenzüberschreitend. Rechtsstaaten müssen das ebenfalls tun.

16H. Warum wir Betrug nicht nur nach Schadenssumme bewerten dürfen

Ein Schaden von 5.000 Euro kann für einen Millionärgeringer sein als 500 Euro für eine Rentnerin mit Grundsicherung. Strafrecht muss objektive Maßstäbe verwenden. Opferschutz darf trotzdem die subjektive Lebenswirkung sehen.

Betrug kann Miete gefährden, medizinische Ausgaben verhindern, Familien zerstreiten und psychische Krisen auslösen. Manche Opfer verlieren Schlaf, Selbstvertrauen und soziale Kontakte. Andere entwickeln Angst vor Technik oder geben selbstständige Finanzentscheidungen auf.

Deshalb sollte Opferhilfe bei schweren Vermögensdelikten nicht als Luxus gelten. Beratungsstellen, psychosoziale Unterstützung und verständliche Verfahrensbegleitung können genauso wichtig sein wie die Frage, ob ein Teil des Geldes zurückkommt.

Gerade ältere Opfer brauchen eine Ansprache, die Selbstständigkeit schützt. Hilfe darf nicht bedeuten, ihnen pauschal die Kontrolle über ihre Finanzen zu entziehen. Besser sind abgestufte Schutzinstrumente:

Überweisungslimits, Vertrauenspersonen, Benachrichtigungen, Rückrufregeln und freiwillige Sperrmechanismen.

Der Staat zählt Euro. Das ist notwendig. Aber eine humane Gesellschaft zählt auch, was diese Euro im konkreten Leben bedeutet haben.

16I. Die „Hallo Mama, neue Nummer“-Masche

Die Nachricht ist unspektakulär: „Hallo Mama, mein Handy ist kaputt. Das ist meine neue Nummer.“ Kein dramatischer Unfall, kein Polizist, keine Sirene. Gerade deshalb ist die Masche so gefährlich. Sie beginnt mit Alltag.

Nach ein paar Nachrichten folgt die Bitte: Das Onlinebanking funktioniere noch nicht, eine Rechnung müsse aber heute bezahlt werden. Könntest du kurz überweisen? Das Geld komme morgen zurück. Der Betrag ist oft so gewählt, dass er für einen echten Angehörigen plausibel wirkt.

Der Trick lebt von sprachlicher Anpassung. Täter übernehmen Namen, Familienrollen und manchmal Informationen aus sozialen Netzwerken. Sie müssen nicht perfekt schreiben. Familienkommunikation ist informell; Tippfehler wirken sogar authentisch. Wer jeden Tag kurze Messenger-Nachrichten verschickt, erwartet keine notariell beglaubigte Grammatik.

Die Gegenregel ist einfach: Neue Nummer plus Geldwunsch bedeutet Rückruf über die alte bekannte Nummer oder Kontakt über einen zweiten Kanal. Wenn das angeblich nicht geht, kommt die Familienfrage oder das Codewort. Betrüger hassen Fragen, deren Antwort nicht öffentlich recherchierbar ist.

Messenger-Anbieter könnten zusätzlich deutlicher warnen, wenn eine neue Nummer erstmals einen Kontakt anschreibt und kurz darauf Zahlungsdaten verschickt. Sicherheit darf nicht nur im Hilfecenter stehen; sie muss im Moment des Risikos auftauchen.

16J. Tech-Support-Betrug: Erst wird das Problem erfunden, dann die Lösung verkauft

Ein Pop-up behauptet, der Computer sei mit Viren verseucht. Eine Telefonnummer verspricht Hilfe. Oder ein angeblicher Mitarbeiter eines großen Technologieunternehmens ruft direkt an. Der Computer müsse dringend geprüft werden. Ohne Eingriff seien Fotos, Bankdaten oder sogar das ganze Netzwerk in Gefahr.

Dann soll Fernwartungssoftware installiert werden. Der Täter erhält Kontrolle über Bildschirm, Maus und Tastatur. Manchmal zeigt er harmlose Systemmeldungen als Beweis einer Infektion. Manchmal öffnet er das Onlinebanking. Manchmal fordert er eine angebliche Erstattung durch eine absichtlich manipulierte Anzeige und behauptet danach, das Opfer habe zu viel Geld erhalten und müsse es zurückzahlen.

Diese Masche nutzt technischen Respekt. Viele Menschen wissen, dass sie ihren Computer nicht vollständig verstehen. Der Täter inszeniert sich als Fachmann und macht aus normaler Unsicherheit eine Hierarchie. Je weniger das Opfer versteht, desto mehr soll es gehorchen.

Die wichtigste Regel: Unaufgeforderte technische Hilfe ablehnen. Kein seriöser Hersteller überwacht zufällig Ihren privaten Windows-Rechner und ruft an, weil er heute besonders besorgt ist. Pop-ups mit Telefonnummern schließen, Browser notfalls beenden, Gerät vom Netz trennen und Hilfe über einen selbst gewählten Dienstleister suchen.

Auch Browser und Betriebssysteme müssen aggressive Warnseiten stärker isolieren. Wenn eine Website versucht, Vollbild, Alarmton und Blockadegefühl zu erzeugen, ist das kein gewöhnliches Designproblem. Es ist eine bekannte Social-Engineering-Technik.

16K. QR-Code-Betrug: Wenn selbst der Aufkleber auf der Parkuhr lügen kann

QR-Codes sind bequem, weil sie Text unsichtbar machen. Genau das ist ihr Sicherheitsproblem. Bei einer Webadresse sieht man wenigstens, wohin man klickt. Beim QR-Code sieht man nur ein Muster. Der Mensch vertraut dem Aufkleber, dem Tischschild, der Parkuhr oder dem Brief.

Kriminelle können echte QR-Codes überkleben und auf Phishing-Seiten umleiten. Dort werden Kartendaten, Login-Daten oder Zahlungen abgefragt. Besonders perfide ist der physische Angriff: Der Ort ist real und seriös, nur der kleine Aufkleber wurde manipuliert.

Wer einen QR-Code scannt, sollte deshalb die aufgelöste Adresse prüfen, bevor er Daten eingibt. Bei Behörden, Banken oder Parkdiensten ist die offizielle App oder selbst eingegebene Website sicherer. Ein QR-Code ist kein Echtheitssiegel.

Betreiber öffentlicher Systeme müssen ihre Codes manipulationssicherer gestalten: Plomben, spezielle Etiketten, regelmäßige Sichtkontrolle, digitale Signaturen und klare Hinweise auf die erwartete Domain. Wenn jeder beliebige Aufkleber dieselbe Autorität besitzt wie das Original, ist die Gestaltung selbst Teil des Problems.

Quishing zeigt exemplarisch, wohin Betrug geht: Er vermischt physische und digitale Welt. Der Bürger kann nicht mehr sagen „Online bin ich vorsichtig, draußen ist es echt“. Sicherheitsdenken muss kanalübergreifend werden.

16L. SIM-Swapping und Kontoübernahme: Wenn plötzlich das eigene Handy verstummt

Bei SIM-Swapping versuchen Täter, die Mobilfunknummer des Opfers auf eine von ihnen kontrollierte SIM oder eSIM übertragen zu lassen. Gelingt das, können SMS-Codes, Passwort-Resets und Anrufe beim Täter landen. Das Opfer merkt manchmal erst etwas, wenn das eigene Telefon plötzlich keinen Empfang mehr hat.

Die Masche zeigt, wie gefährlich eine Telefonnummer als universeller Identitätsanker geworden ist. Banken, E-Mail-Dienste, soziale Netzwerke und Behörden nutzen dieselbe Nummer zur Wiederherstellung. Wer sie übernimmt, erhält potenziell Schlüssel zu mehreren Türen.

Mobilfunkanbieter müssen deshalb besonders strenge Identitätsprüfungen für SIM-Tausch und Rufnummernübertragung anwenden. Ein erfolgreicher Social-Engineering-Anruf beim Provider darf nicht reichen, um das digitale Leben eines Kunden umzuleiten.

Verbraucher sollten, wo möglich, App-basierte Zwei-Faktor-Verfahren oder Hardware-Schlüssel nutzen statt SMS allein. Und wenn das Handy ohne erklärbaren Grund Netz verliert, während gleichzeitig Passwort-Reset-Nachrichten eintreffen, ist Eile geboten: Provider und Banken sofort kontaktieren.

Der Fall zeigt eine allgemeine Wahrheit: Sicherheit ist nur so stark wie der schwächste Wiederherstellungsweg. Das beste Passwort nützt wenig, wenn ein Callcenter-Mitarbeiter durch eine überzeugende Geschichte zur Herausgabe der Identität gebracht werden kann.

16M. Mietbetrug und falsche Immobilien: Die Wohnung, die nie existierte

Wohnungsnot ist ein idealer Nährboden für Betrug. Eine schöne Wohnung, überraschend günstige Miete, sofort verfügbar. Der angebliche Vermieter sei im Ausland, könne aber den Schlüssel nach Zahlung einer Kaution schicken. Oder eine bekannte Buchungsplattform werde als Treuhänder genannt - über einen Link, der nur so aussieht.

Wer verzweifelt sucht, akzeptiert Bedingungen, die er sonst ablehnen würde. Genau hier ersetzt Knappheit den klassischen Zeitdruck. „Es gibt zehn weitere Interessenten." „Heute noch reservieren." „Kaution vor Besichtigung." Die emotionale Botschaft lautet: Prüfen kostet dich die Wohnung.

Eine Wohnung, die man nicht besichtigt hat, ein Vermieter, dessen Identität nicht verifiziert ist, und eine Zahlung an ein ausländisches Konto oder einen Geldtransferdienst sind eine gefährliche Kombination. Auch Ausweiskopien des vermeintlichen Vermieters beweisen wenig - sie können gestohlen sein.

Plattformen für Immobilienanzeigen sollten verifizierte Eigentümer- oder Makleridentitäten stärker kennzeichnen und Serienanzeigen schneller erkennen. Wer dieselbe Traumwohnung in fünf Städten anbietet, darf nicht erst nach der fünften Opferanzeige auffallen.

Mietbetrug zeigt, warum Betrugspolitik auch Sozialpolitik berührt. Je größer die Verzweiflung auf einem Markt, desto leichter kann sie monetarisiert werden.

16N. Urlaubsbetrug: Ferienhaus, Flug und Ticket als Fata Morgana

Die Ferienwohnung sieht perfekt aus. Meerblick, gute Bewertungen, erstaunlich günstiger Preis. Der Vermieter bittet nur darum, außerhalb der Plattform zu zahlen, um Gebühren zu sparen. Wer das tut, spart manchmal tatsächlich Gebühren - und verliert gleichzeitig den Schutz der Plattform.

Betrüger kopieren echte Inserate, stehlen Fotos und bauen eigene Buchungsseiten. Auch Konzerttickets, Flüge, Mietwagen oder Reisegutscheine können gefälscht sein. Der emotionale Hebel ist Vorfreude: Menschen wollen buchen, nicht ermitteln.

Besonders wirksam ist künstliche Knappheit: „Nur noch ein Zimmer", „15 Personen sehen dieses Angebot", „Preis gilt noch 7 Minuten". Nicht jede solche Anzeige ist Betrug, aber sie trainiert Verbraucher darauf, Geschwindigkeit über Prüfung zu stellen. Das ist ein Geschenk an Täter.

Zahlung innerhalb etablierter Plattformen, überprüfbare Anbieter, Kreditkarten mit möglichen Rückbuchungsmechanismen und Skepsis bei ungewöhnlichen Zahlungswegen sind wichtige Schutzfaktoren. Wer Gutscheinkarten, Krypto oder Überweisung an Privatkonten verlangt, sollte die Reise sehr schnell beenden - zumindest die finanzielle.

Auch hier müssen Plattformen Verantwortung übernehmen: Sie kennen Kopien, Geräte, IP-Muster, Zahlungswege und Wiederholungstäter. Ein Nutzer sieht ein Inserat. Die Plattform sieht das Netzwerk.

16O. Geschenkkarten: Das perfekte Geld für Betrüger

„Kaufen Sie bitte Gutscheinkarten und lesen Sie mir die Codes vor.“ Dieser Satz sollte in Deutschland denselben Alarm auslösen wie „Übergeben Sie Bargeld an einen Fremden“. Geschenkkarten sind für Betrüger attraktiv, weil Codes schnell übertragen und weiterverkauft werden können.

Die Geschichten wechseln: angebliche Steuerzahlung, Chef-Anweisung, Gewinnfreigabe, technischer Support, Familiennotfall. Warum sollte eine Behörde eine Strafe mit Gaming-Gutscheinen verlangen? In ruhiger Minute ist die Absurdität offensichtlich. Unter Autoritätsdruck handeln Menschen trotzdem.

Einzelhändler können helfen. Hohe Mengen von Gutscheinkarten, besonders bei älteren Kunden oder nervösem Verhalten, sind ein Warnsignal. Kassensysteme könnten kurze Hinweise anzeigen: „Hat Sie jemand am Telefon aufgefordert, diese Karten zu kaufen? Dann brechen Sie den Kauf ab.“

Ein Code ist Bargeld mit Tarnkappe. Sobald er übermittelt ist, kann die Spur schnell weitergehen. Prävention muss daher vor dem Kauf oder spätestens an der Kasse greifen.

Wenn eine Zahlung nur deshalb gewählt wird, weil sie schwer rückholbar ist, sollten Verbraucher fragen: Wer profitiert eigentlich von dieser Irreversibilität? Bei Betrug fast nie das Opfer.

16P. Falsche Spenden und Katastrophenbetrug: Mitgefühl als Geschäftsmodell

Nach Katastrophen, Kriegen oder persönlichen Schicksalen steigt die Spendenbereitschaft. Das ist menschlich. Und genau deshalb tauchen gefälschte Spendenaufrufe, kopierte Hilfsorganisationen und erfundene Einzelschicksale auf.

Der Täter muss hier keine Gier wecken, sondern Mitgefühl. Bilder werden gestohlen, Geschichten kopiert, Konten schnell eingerichtet. Social Media beschleunigt die Verbreitung, weil emotionales Teilen schneller ist als institutionelle Prüfung.

Wer spenden möchte, sollte Organisationen selbst aufrufen, nicht über zufällige Links zahlen, und bei privaten Sammelaktionen nachvollziehen, wer organisiert, für wen gesammelt wird und wie Mittel verwendet werden. Bei großen Ereignissen sind bekannte Hilfswerke der sicherere Weg.

Plattformen sollten bei viralen Spendenkampagnen Identitäten und Empfänger stärker prüfen. Es ist schwer erträglich, wenn Hilfsbereitschaft zum Risikofaktor wird. Wer Mitgefühl ausbeutet, beschädigt nicht nur ein Opfer, sondern die Bereitschaft der Gesellschaft, beim nächsten echten Notfall zu helfen.

Das ist ein wiederkehrendes Muster: Betrug verbraucht soziales Kapital. Jeder falsche Polizist schwächt Vertrauen in echte Polizei. Jede falsche Spendenaktion schwächt Vertrauen in echte Hilfe. Jeder falsche Berater macht seriöse Beratung schwieriger.

16Q. Die große Lehre: Kein Kanal ist mehr automatisch echt

Telefonnummern können gefälscht sein. Absendernamen in E-Mails können täuschen. Websites können kopiert werden. Stimmen können imitiert, Videos manipuliert, Bewertungen gekauft und Dokumente digital nachgebaut werden. Das bedeutet nicht, dass nichts mehr glaubwürdig ist. Es bedeutet, dass Echtheit einen zweiten Faktor braucht.

Dieser zweite Faktor kann ein Rückruf über eine bekannte Nummer sein, eine selbst eingegebene Website, eine App, ein Codewort, eine persönliche Begegnung oder eine zweite Person. Sicherheit entsteht nicht mehr allein durch die Qualität eines Signals, sondern durch unabhängige Bestätigung.

Das ist unbequem. Aber die Alternative wäre universelles Misstrauen. Eine Gesellschaft kann nicht funktionieren, wenn jeder Anruf, jede Rechnung und jede Nachricht grundsätzlich als feindlich behandelt wird. Deshalb müssen Systeme verifizierbare Vertrauensanker schaffen.

Behörden und Unternehmen sollten ihre Kommunikation so gestalten, dass Bürger sie unabhängig prüfen können. Klare Domains, keine widersprüchlichen Linkpraktiken, verifizierte Absender, nachvollziehbare Aktenzeichen und öffentlich bekannte Rückrufwege. Wer Sicherheit verlangt, muss selbst sicher kommunizieren.

Der Satz der Zukunft lautet nicht „Glaub nichts“. Er lautet: „Bestätige Wichtiges über einen zweiten Weg.“ Das ist weniger romantisch als Vertrauen - aber besser als die totale Kapitulation vor Täuschung.

TEIL V

WO DER STAAT STÄRKER SEIN MUSS

Banken, Netze, Plattformen, Justiz und Vollzug

17. Banken: Die letzte Notbremse vor der Übergabe

Banken sind keine Vormünder. Erwachsene Menschen dürfen über ihr Geld verfügen, auch unvernünftig. Diese Freiheit ist wichtig. Aber Freiheit bedeutet nicht, dass ein Institut Warnsignale ignorieren muss, wenn eine typische Betrugssituation vor ihm steht.

Eine Kundin hebt normalerweise 200 Euro ab und verlangt plötzlich 35.000 Euro in bar. Sie wirkt nervös. Sie sagt, sie dürfe niemandem erklären, wofür. Vielleicht telefoniert sie währenddessen. Das ist keine gewöhnliche Transaktion. Es ist ein Muster, das jeder Bankangestellte kennen sollte.

Die Schwierigkeit: Täter trainieren ihre Opfer. Sie geben Ausreden vor - Autokauf, Renovierung, Familiengeschenk. Deshalb reicht die Frage „Wofür brauchen Sie das Geld?“ nicht. Besser sind konkrete Sicherheitsfragen: Hat Sie jemand telefonisch zu dieser Abhebung aufgefordert? Hat jemand gesagt, Sie müssten darüber schweigen? Soll das Geld an eine fremde Person übergeben werden? Hat jemand behauptet, Polizei oder Staatsanwaltschaft zu sein?

Banken sollten für besonders hohe Bargeldabhebungen älterer Kunden standardisierte Betrugswarnungen anbieten, ohne sie zu entmündigen. Ein zweiter Mitarbeiter kann kurz gegenprüfen. Eine freiwillige Vertrauensperson kann hinterlegt werden. Bei Überweisungen an neue Empfänger können klare Warnungen erscheinen. Entscheidend ist die Tonlage: nicht „Wir glauben Ihnen nicht“, sondern „Wir sehen diese Betrugsmasche jeden Tag und möchten verhindern, dass jemand Sie unter Druck setzt.“

Und wenn ein Institut erkennt, dass ein Konto regelmäßig als Durchlaufstation für Betrugsgelder genutzt wird, muss es handeln. Geldwäscheprävention ist keine lästige Compliance-Übung. Sie ist Opferschutz. Jede Stunde, in der Geld auf einer bekannten Mule-Struktur weiterwandert, senkt die Chance auf Rückholung.

18. Telekommunikation: Verboten, aber technisch noch möglich

Es ist ein Lieblingszustand moderner Regulierung: etwas ist verboten, aber technisch weiterhin bequem möglich. Call-ID-Spoofing ist dafür das perfekte Beispiel. Die Rechtslage sagt: so nicht. Die Technik sagt: kommt darauf an.

Die Bundesnetzagentur erklärt, dass sie bei manipulierten Absenderinformationen keine eigenen technischen Verhinderungsmöglichkeiten hat und dass technische Einwirkungen bei Netzbetreibern und Telekommunikationsanbietern liegen. [Q4] Das ist keine Kleinigkeit. Es bedeutet, dass die wirksamste Prävention dort stattfinden muss, wo die Signalisierung verarbeitet wird.

Wir brauchen deshalb verbindliche technische Standards, die Echtheit sichtbar machen. Eine Rufnummer sollte nicht nur als Textfeld übertragen werden. Für sensible Branchen muss eine verifizierte Identität möglich sein. Wer „Polizei“, „Bank“, „Versicherung“ oder „Behörde“ behauptet, sollte sich technisch stärker authentifizieren müssen als irgendein Werbeanrufer.

Außerdem braucht es bessere grenzüberschreitende Kooperation. Ein großer Teil der Betrugskommunikation kommt aus internationalen Strukturen. Nationale Abschaltungen helfen, aber Täter rotieren Nummern, Provider, Accounts und Domains. Abwehr muss ebenso automatisiert und grenzüberschreitend werden wie der Angriff.

Und wir sollten die Verbraucheroberfläche ändern. Statt nur eine Nummer anzuzeigen, könnte das Gerät zwischen „verifiziert“, „nicht verifiziert“ und „verdächtig“ unterscheiden. E-Mail hat über Jahre Mechanismen

wie SPF, DKIM und DMARC aufgebaut - nicht perfekt, aber besser als blindes Vertrauen. Telefonie braucht denselben Ehrgeiz.

19. Plattformen: Reichweite darf nicht nur Gewinn bedeuten

Viele moderne Betrugsopfer treffen ihren Täter zuerst nicht am Telefon, sondern in einer Anzeige. Promi-Video, Investmenttipp, Gewinnspiel, Jobangebot, romantisches Profil. Die Plattform verkauft Reichweite. Der Täter kauft sie. Das Opfer zahlt am Ende den eigentlichen Preis.

Natürlich können Plattformen nicht jede Lüge vorab erkennen. Aber sie sehen mehr als der einzelne Nutzer: Wer schaltet hunderte ähnliche Anzeigen? Welche Domains werden ständig gewechselt? Welche Konten werden nach Beschwerden neu angelegt? Welche Zahlungsdaten, Geräte oder Kampagnenmuster wiederholen sich?

Wer diese Daten besitzt und gleichzeitig am Anzeigenumsatz verdient, hat eine besondere Verantwortung. „Wir haben nach Meldung gelöscht“ ist bei seriellen Kampagnen zu wenig. Nach dem zehnten Klon einer Betrugsanzeige muss die Frage lauten: Warum konnte Nummer elf überhaupt live gehen?

Verbraucherzentralen warnen vor gefälschten Anzeigen, Shops und Anlageplattformen, die mit geklauten oder veränderten Promi-Bildern Vertrauen erzeugen. [Q14] Gerade KI senkt die Kosten solcher Täuschungen. Plattformen müssen deshalb Herkunft, Werbekunden und Zahlungsströme stärker prüfen - besonders bei Finanzprodukten.

Das Argument „Wir sind nur Vermittler“ ist gesellschaftlich verbraucht. Wer eine Autobahn betreibt, ist nicht für jeden Fahrer verantwortlich. Aber wenn dieselbe Ausfahrt jeden Abend für Raubüberfälle genutzt wird, darf er nicht behaupten, die Fahrbahnmarkierung sei seine einzige Zuständigkeit.

20. Justiz: Sorgfalt ja - Stillstand nein

Wer über langsame Justiz spricht, bekommt schnell die richtige Antwort: Rechtsstaat braucht Zeit. Akten müssen gelesen, Beweise geprüft, Verteidigungsrechte gewahrt werden. Absolut. Niemand sollte wegen öffentlicher Wut schneller verurteilt werden. Das wäre keine Gerechtigkeit, sondern Lynchlogik im Anzug.

Aber aus diesem richtigen Satz folgt nicht, dass jede Verfahrensdauer automatisch hinzunehmen ist. Der Europäische Rechtsstaat schuldet nicht nur ein faires, sondern auch ein Verfahren in angemessener Zeit. Und selbst dort, wo keine konkrete Rechtsverletzung festgestellt ist, kann extreme Dauer Vertrauen zerstören.

Wirtschaftsstrafverfahren sind besonders anfällig. Terabytes Daten, internationale Rechtshilfe, komplexe Gesellschaften, Sachverständige, viele Beschuldigte, viele Verteidiger, parallele Insolvenzen. Genau deshalb braucht dieser Bereich Spezialisierung. Wer einen Flughafen bauen will, stellt auch nicht fest, dass Beton kompliziert ist, und wartet dann zehn Jahre auf einen zusätzlichen Bauingenieur.

Wir brauchen Schwerpunktstaatsanwaltschaften, spezialisierte Wirtschaftsstrafkammern, digitale Aktenführung, forensische Buchhalter, Datenanalysten und verbindliche Eskalationsmechanismen für Verfahren, die jahrelang im Zwischenstadium stehen. Richterliche Unabhängigkeit bedeutet nicht organisatorische Gleichgültigkeit.

Vor allem brauchen Geschädigte bessere Information. Nicht zu jedem Ermittlungsdetail - Geheimhaltung und Persönlichkeitsrechte gelten. Aber ein Opfer, das Jahre wartet, sollte nachvollziehen können, in welchem

Stadium sich ein Verfahren befindet, welche grundsätzlichen Gründe für Verzögerungen bestehen und welche nächsten Schritte anstehen. Schweigen produziert Gerüchte. Transparenz produziert wenigstens Verständnis.

Ein Staat, der Parkverstöße automatisiert in Wochen bearbeitet, darf sich bei Millionenverfahren nicht damit abfinden, dass Zeit ein Naturgesetz sei. Natürlich ist der Vergleich juristisch schief. Genau deshalb ist er politisch so wirksam: Bürger erleben Verwaltung als schnell, wenn sie etwas von ihnen will, und als langsam, wenn sie Schutz erwarten.

21. Offener Vollzug: Resozialisierung braucht belastbare Prognosen

Offener Vollzug ist kein Geschenk und kein Wellnessprogramm. Er ist ein Instrument des Strafvollzugs. Die Idee ist vernünftig: Wer geeignet ist, soll schrittweise Verantwortung unter weniger gesicherten Bedingungen übernehmen können, um Rückkehr in ein legales Leben vorzubereiten.

Das Strafvollzugsgesetz formuliert als Grundgedanken: Eine Unterbringung im offenen Vollzug kommt in Betracht, wenn der Gefangene den besonderen Anforderungen genügt und insbesondere nicht zu befürchten ist, dass er flieht oder die Möglichkeiten des offenen Vollzuges zu Straftaten missbrauchen wird. [Q15] Genau dieser letzte Halbsatz ist politisch entscheidend.

Wenn die Öffentlichkeit von einem Fall erfährt, in dem jemand trotz mehrjähriger Freiheitsstrafe sehr früh offenen Vollzug erhält, entsteht automatisch die Frage: Wie wurde die Missbrauchsgefahr geprüft? Diese Frage ist legitim. Sie ist nicht gleichbedeutend mit der Forderung, jeden Menschen maximal hart einzusperren.

Der richtige Maßstab ist nicht Empörung über Lockerung, sondern Qualität der Prognose. Welche Deliktsart liegt vor? Wie war das Verhalten im Vollzug? Gibt es Einsicht, Schadenswiedergutmachung, stabile Lebensverhältnisse? Besteht Zugang zu denselben Strukturen, mit denen Straftaten begangen wurden? Wie wird kontrolliert?

Bei Vermögensdelikten muss außerdem verstanden werden, dass Tatmittel oft kein Brecheisen sind. Es sind Telefon, Laptop, Geschäftskontakte, Vertrieb, Social Media und Überzeugungskraft. Wer Missbrauchsgefahr bewertet, muss deshalb digitale und wirtschaftliche Tatmöglichkeiten genauso ernst nehmen wie Fluchtgefahr.

Und falls jemand während Lockerungen tatsächlich neue Straftaten begeht oder konkrete Verstöße zeigt, muss das System schnell reagieren. Resozialisierung lebt von Vertrauen. Vertrauen ohne Konsequenz bei Missbrauch wäre keine Humanität, sondern Naivität.

22. Wohnort, Zuständigkeit und der Eindruck vom Wunschgefängnis

Die Vorstellung, ein Verurteilter könne einfach umziehen und sich dadurch eine angenehmere Haftanstalt aussuchen, ist in dieser Pauschalität falsch. Die örtliche und sachliche Zuständigkeit wird durch Vollstreckungspläne der Landesjustizverwaltungen geregelt. § 152 Strafvollzugsgesetz beschreibt genau dieses System. [Q16]

Gleichzeitig kann Wohnortnähe im Vollzug eine Rolle spielen, etwa aus Gründen von Behandlung, Eingliederung und Entlassungsvorbereitung. Das ist sinnvoll: Wer nach der Haft in eine Region zurückkehrt, profitiert von sozialen Kontakten, Arbeitsperspektiven und Behördenwegen dort.

Aber genau weil solche Faktoren existieren, muss die Verwaltung verhindern, dass daraus strategische Gestaltung entsteht. Ein kurzfristiger oder rein taktischer Wohnortwechsel darf nicht automatisch zu einer bevorzugten Unterbringung führen. Zuständigkeit muss nachvollziehbar und überprüfbar bleiben.

Die beste Antwort auf den öffentlichen Verdacht eines „Wunschgefängnisses“ ist Transparenz über Regeln, nicht Geheimniskrämerei. Welche Kriterien entscheiden? Welche Behörde entscheidet? Welche Rolle spielen Wohnsitz, Strafdauer, Deliktsart, Sicherheitsbewertung und Belegung? Je klarer das System, desto weniger Raum für Legenden.

Und auch hier gilt: Kritik sollte exakt sein. Wer behauptet, jeder könne durch Umzug die Haftform bestimmen, schießt übers Ziel. Wer fragt, ob Zuständigkeitsregeln gegen taktische Gestaltung ausreichend abgesichert sind, stellt eine berechtigte rechtsstaatliche Frage.

TEIL VI

WAS SICH ÄNDERN MUSS

Ein Manifest gegen die organisierte Abzocke

23. Vermögen schneller sichern, Geldströme schneller stoppen

Bei Betrug entscheidet Zeit. Geld bewegt sich heute in Sekunden. Strafverfahren bewegen sich naturgemäß langsamer. Diese Asymmetrie ist der Traum jedes Täters. Eine Überweisung kann über mehrere Konten, Zahlungsdienste und Kryptowerte weitergeleitet sein, bevor das Opfer überhaupt realisiert, was passiert ist.

Deshalb muss die erste staatliche und wirtschaftliche Reaktion auf Betrug stärker auf Sicherung ausgerichtet sein. Banken brauchen rund um die Uhr erreichbare Fraud-Teams. Meldungen zwischen Instituten müssen standardisiert sein. Verdächtige Empfängerkonten müssen schneller geprüft und gegebenenfalls eingefroren werden können - selbstverständlich mit rechtsstaatlichen Sicherungen.

Auch die Rückgewinnung von Vermögen verdient mehr Priorität. Ein Urteil nach Jahren ist wichtig. Für das Opfer ist zusätzlich entscheidend, ob noch etwas da ist. Kriminalpolitik misst Erfolg zu oft in Verurteilungen. Vermögensabschöpfung und Rückführung sind für Betrugsopfer mindestens genauso real.

International braucht es schnellere Rechtshilfe für Kontodaten, Domaininhaber, Plattformaccounts und Kommunikationsdaten. Betrugsnetzwerke wählen Jurisdiktionen nicht aus romantischem Fernweh, sondern weil Grenzen Reibung erzeugen. Der Staat muss diese Reibung auf seiner Seite reduzieren.

Und wir brauchen bessere Warnketten. Wenn eine Behörde eine Betrugsdomain erkennt, sollten Suchmaschinen, soziale Netzwerke, Browseranbieter und Banken automatisiert gewarnt werden können. Warum sollte ein Verbraucher eine Seite noch problemlos finden, wenn mehrere Behörden sie bereits als Teil einer laufenden Betrugswelle identifiziert haben?

24. Ein nationaler Betrugsschutz mit echter Zuständigkeit

Deutschland liebt Zuständigkeiten. Für komplexe Betrugsfälle ist das manchmal ein Sicherheitsrisiko. Telekommunikationsrecht hier, Finanzaufsicht dort, Strafanzeige bei der Polizei, Plattformbeschwerde beim Anbieter, Bankrückruf beim Institut, Verbraucherschutz an anderer Stelle. Der Bürger, der gerade 30.000 Euro verloren hat, bekommt ein Verwaltungsseminar.

Ich plädiere für eine zentrale, rund um die Uhr erreichbare Betrugsnotfallstelle - digital und telefonisch. Nicht als Ersatz für Polizei oder Banken, sondern als koordinierende erste Tür. Der Betroffene schildert den Fall einmal. Das System gibt priorisierte Schritte aus, erzeugt standardisierte Meldungen und leitet an zuständige Stellen weiter.

Bei akuten Zahlungsvorgängen zählt jede Minute. Eine solche Stelle könnte mit Banken, Zahlungsdiensten und Strafverfolgung definierte Schnellkanäle nutzen. Kein Bürger sollte in der ersten Stunde nach einem Betrug googeln müssen, welche Abteilung heute zuständig ist.

Gleichzeitig braucht es ein nationales Lagebild, das Betrugsmaschen nicht nur nach Straftatbeständen, sondern nach Kampagnen clustert. Dieselbe Tätergruppe kann telefonieren, SMS versenden, Fake-Websites schalten und Geld über identische Konten abziehen. Behörden müssen diese Signale zusammenführen.

Das Ziel ist einfach: Aus tausend einzelnen Opfern soll für den Staat ein einziges Muster werden. Täter skalieren. Der Staat muss ebenfalls skalieren.

25. Das 20-Punkte-Manifest gegen die Abzocke

1. Verifizierte Anruferkennung für Banken, Behörden und andere sensible Einrichtungen verbindlich vorantreiben.
2. Call-ID-Spoofing technisch stärker filtern und internationale Provider bei Missbrauch konsequent sperren oder drosseln.
3. Eine bundesweit einheitliche Betrugsnotfallstelle mit 24/7-Schnellwegen zu Banken und Polizei schaffen.
4. Banken zu standardisierten Warnfragen bei auffälligen hohen Bargeldabhebungen und neuen Hochrisikoempfängern verpflichten.
5. Konten, die als Geldwäsche- oder Durchlaufkonten auffallen, schneller institutübergreifend kennzeichnen und prüfen.
6. Vermögenssicherung und Rückgewinnung als zentrale Erfolgskennzahl in Betrugsverfahren behandeln.
7. Spezialisierte Wirtschaftsstrafkammern und Staatsanwaltschaften personell und technisch dauerhaft stärken.
8. Verfahren mit außergewöhnlicher Dauer organisatorisch eskalieren, ohne richterliche Unabhängigkeit anzutasten.
9. Geschädigten regelmäßige, verständliche Statusinformationen über lange Verfahren ermöglichen.
10. Finanzwerbung auf Plattformen nur nach überprüfbarer Identität des Werbekunden und erhöhten Prüfstandards zulassen.
11. Wiederkehrende Klonanzeigen, Fake-Domains und identische Kampagnenmuster plattformübergreifend schneller sperren.
12. Prominenten-Deepfakes und manipulierte Finanzwerbung mit sichtbaren Herkunfts- und Manipulationshinweisen versehen.
13. Verbraucherbildung zu Betrug fest in Schulen, Volkshochschulen, Seniorenarbeit und betrieblicher Weiterbildung verankern.
14. Familiencodewörter und Rückrufregeln in öffentlichen Präventionskampagnen zum Standard machen.
15. Bankmitarbeiter, Taxifahrer, Pflegekräfte und andere Berufsgruppen mit häufigem Kontakt zu gefährdeten Personen regelmäßig schulen.
16. Bei offenem Vollzug die deliktspezifische digitale und wirtschaftliche Missbrauchsgefahr ausdrücklich in Prognosen einbeziehen.
17. Vollstreckungs- und Zuständigkeitsregeln so transparent machen, dass der Eindruck einer taktischen „Wunschgefängnis“-Wahl gar nicht erst entsteht.
18. Recovery-Scams nach vorangegangenem Anlagebetrug als eigene Präventionspriorität behandeln.
19. Behördenwarnungen technisch schneller in Browser, Suchmaschinen, App-Stores und Plattformen einspeisen.
20. Opfer öffentlich nicht belehren, sondern unterstützen: Scham ist ein Ermittlungshemmnis.

DER KERN

Prävention darf nicht bedeuten, dass der einzelne Bürger zum alleinigen Sicherheitsbeauftragten einer globalen digitalen Infrastruktur erklärt wird.

26. Schluss: Macht Täter nervös, nicht Opfer

Dieses Buch ist aus Wut geschrieben. Aber Wut ist nur dann nützlich, wenn sie eine Richtung hat. Meine Richtung ist nicht Rache. Sie ist Funktionsfähigkeit. Ich will keinen Staat, der Menschen vorsorglich einsperrt.

Ich will einen Staat, der bekannte Betrugsmuster schnell erkennt, Tatmittel erschwert, Geld sichert, Verfahren zügig führt und Opfer nicht jahrelang im Nebel stehen lässt.

Ich will Banken, die nicht erst nach der Überweisung erklären, dass man vorsichtig sein müsse. Ich will Telekommunikationsanbieter, die eine Rufnummernanzeige nicht wie eine unverbindliche Dekoration behandeln. Ich will Plattformen, die für bezahlte Reichweite auch bezahlte Verantwortung übernehmen. Ich will Finanzaufsicht, die Warnungen so sichtbar macht wie Werbung. Ich will eine Justiz, deren Sorgfalt nicht mit Stillstand verwechselt werden kann.

Und ich will, dass wir aufhören, Opfer zu verhöhnen. Ein Mensch, der betrogen wurde, hat nicht bewiesen, dass er dumm ist. Er hat bewiesen, dass ein Täter einen Moment gefunden hat, in dem eine Lüge funktioniert hat. Das kann uns allen passieren. Unterschiedlich wahrscheinlich, unterschiedlich leicht - aber niemand ist immun.

Betrug wird nie vollständig verschwinden. Aber seine Rentabilität ist politisch beeinflussbar. Je schwerer Identitäten zu fälschen sind, je schneller Geld eingefroren wird, je besser Plattformen Kampagnen erkennen, je professioneller Ermittlungen laufen und je schneller Gerichte verhandeln können, desto schlechter wird das Geschäftsmodell.

Die entscheidende Frage lautet nicht: „Warum ist der Verbraucher darauf hereingefallen?“ Die entscheidende Frage lautet: „Warum konnte der Täter diese Infrastruktur so leicht benutzen?“

Macht Täter nervös. Macht ihre Konten kurzlebig, ihre Domains wertlos, ihre Nummern unverlässlich, ihre Geldwege sichtbar, ihre Verfahren zügig und ihre Gewinne rückholbar. Und gebt Opfern das zurück, was Betrug neben Geld am schnellsten zerstört: das Gefühl, dass der Staat auf ihrer Seite handlungsfähig ist.

LETZTER WUTSATZ

Ein Rechtsstaat ist nicht daran zu messen, wie viele Warnbroschüren er druckt, sondern wie schwer er es Betrügern macht, aus fremder Angst ein Geschäftsmodell zu bauen.

TEIL ANHANG

NOTFALL UND QUELLEN

Was Betroffene sofort tun können - und worauf die Fakten im Buch beruhen

A. Der 15-Minuten-Notfallplan nach einem Betrug

21. Zahlung stoppen: Bank, Kartenanbieter oder Zahlungsdienst sofort über die offizielle Nummer oder App kontaktieren. Rückruf, Recall oder Sperre verlangen.
22. Konten und Karten sichern: Zugang sperren, Karten blockieren, Onlinebanking prüfen, unbekannte Geräte und Sitzungen abmelden.
23. Passwörter ändern: zuerst E-Mail-Konto, dann Bank, Shops und andere wichtige Dienste. Wo möglich Zwei-Faktor-Authentifizierung aktivieren.
24. Beweise sichern: Screenshots, Rufnummern, Chatverläufe, E-Mails, Überweisungsbelege, Wallet-Adressen, Domains, Namen und Uhrzeiten nicht löschen.
25. Strafanzeige erstatten. Bei laufender Gefahr oder Übergabe sofort Polizei verständigen. Bei Telefonbetrug niemals die vom Anrufer genannte Rückrufnummer verwenden.
26. Angehörige informieren. Scham kostet Zeit. Ein zweites Paar Augen erkennt Folgeangriffe häufig schneller.
27. Bei Anlagebetrug auch BaFin-Warnungen und Unternehmensdatenbank prüfen; bei Rufnummernmissbrauch Beschwerdemöglichkeiten der Bundesnetzagentur nutzen.
28. Vor Recovery-Scams schützen: Niemandem eine weitere Vorauszahlung leisten, nur weil er behauptet, verlorenes Geld „sicher“ zurückholen zu können.

B. Zehn Sätze, die man am Telefon sagen darf

„Ich entscheide nichts am Telefon. Ich rufe selbst zurück.“

„Nennen Sie mir keine Rückrufnummer. Ich suche die offizielle Nummer selbst heraus.“

„Ich übergebe weder Bargeld noch Schmuck an fremde Personen.“

„Wenn Sie von der Polizei sind, kläre ich das über 110 beziehungsweise meine örtliche Dienststelle.“

„Ich gebe keine TAN, PIN, Passwörter oder Freigabecodes weiter.“

„Ich bespreche das zuerst mit meiner Familie.“

„Ich installiere keine Software auf Anweisung eines Anrufers.“

„Ich tätige keine Zahlung unter Zeitdruck.“

„Wenn es wirklich dringend ist, verträgt es eine unabhängige Prüfung.“

„Das Gespräch ist beendet.“

C. Warnsignale bei Geldanlagen

- Ungewöhnlich hohe Rendite bei gleichzeitig angeblich geringem oder keinem Risiko.
- Zeitdruck, künstliche Verknappung oder „nur heute“ verfügbare Konditionen.
- Unaufgeforderte Kontaktaufnahme über Telefon, Messenger oder Social Media.
- Unklare Unternehmensidentität, wechselnde Domains oder fehlende Erlaubnis.
- Einzahlung auf ausländische oder ständig wechselnde Konten ohne nachvollziehbaren Grund.
- Professionelles Dashboard, aber keine unabhängige Verwahrstelle und keine überprüfbaren Transaktionen.
- Probleme bei Auszahlungen; vor Auszahlung werden weitere Gebühren, Steuern oder Sicherheitsleistungen verlangt.
- Prominentenwerbung, die sich nicht auf offiziellen Kanälen bestätigen lässt.
- Berater fordert Fernzugriff auf Computer oder Smartphone.

- Nach einem Verlust meldet sich plötzlich ein „Rückholservice“ und verlangt Vorkasse.

D. Kleines Wörterbuch der Abzocke

Account Takeover: Übernahme eines Onlinekontos durch gestohlene Zugangsdaten oder manipulierte Wiederherstellung.

Call-ID-Spoofing: Manipulation der angezeigten Anrufernummer, um eine andere Identität vorzutäuschen.

CEO-Fraud: Betrug, bei dem Beschäftigte angeblich im Auftrag der Unternehmensleitung dringende Zahlungen ausführen sollen.

Chargeback: Rückbelastungsverfahren bei Kartenzahlungen; Möglichkeiten hängen vom konkreten Fall und Kartenverfahren ab.

Cybertrading-Betrug: Scheinbare Online-Handelsplattformen, auf denen Gewinne angezeigt werden, obwohl das Geld nicht real investiert wird.

Deepfake: Künstlich erzeugtes oder verändertes Audio-, Bild- oder Videomaterial, das eine reale Person täuschend imitieren kann.

Finanzagent / Money Mule: Person, deren Konto zum Empfang und Weiterleiten kriminell erlangter Gelder benutzt wird.

FOMO: Fear of Missing Out - Angst, eine einmalige Chance zu verpassen; häufig bewusst durch Zeitdruck erzeugt.

Identitätsdiebstahl: Missbrauch personenbezogener Daten, um im Namen des Opfers Verträge, Konten oder andere Handlungen vorzunehmen.

Phishing: Täuschungsversuch, Zugangsdaten oder andere sensible Informationen über gefälschte Nachrichten oder Websites zu erlangen.

Quishing: Phishing über manipulierte QR-Codes.

Recovery Scam: Folgebetrug, bei dem nach einem ersten Verlust gegen Vorauszahlung eine angebliche Rückholung des Geldes versprochen wird.

Remote Access: Fernzugriff auf Computer oder Smartphone; legitime Technik, die bei Betrug zur Kontrolle des Geräts missbraucht wird.

Romance Scam: Aufbau einer vorgetäuschten Liebes- oder Vertrauensbeziehung mit dem Ziel finanzieller Ausbeutung.

Schockanruf: Telefonbetrug mit erfundener Notlage, meist Unfall, Haft oder medizinischer Krise eines Angehörigen.

SIM-Swapping: Übertragung einer Mobilfunknummer auf eine vom Täter kontrollierte SIM/eSIM.

Smishing: Phishing per SMS oder Messenger-Nachricht.

Social Engineering: Manipulation von Menschen, damit sie Informationen preisgeben oder Handlungen ausführen, die dem Täter nutzen.

Task Scam: Scheinjob mit digitalen Aufgaben, bei dem das Opfer später eigenes Geld einsetzen soll, um angebliche Gewinne freizuschalten.

Vishing: Phishing über Sprachanrufe.

E. Fünfzig Fragen, die Politik und Wirtschaft beantworten sollten

29. Warum gibt es noch keine allgemein sichtbare, verifizierte Anruferidentität für sensible Einrichtungen?
30. Welche technischen Mindeststandards müssen Netzbetreiber gegen Spoofing erfüllen?
31. Wie schnell können missbrauchte Ursprungsrufnummern heute tatsächlich abgeschaltet werden?
32. Warum sehen Verbraucher nicht, ob eine angezeigte Nummer verifiziert oder nur übermittelt wurde?
33. Wie viele Schockanruf-Kampagnen werden als zusammenhängende Serien erkannt statt als Einzelfälle?
34. Wie viele Banken nutzen verbindliche Warnprozesse bei ungewöhnlichen Bargeldabhebungen?
35. Welche Rückholquote wird bei unmittelbar gemeldeten Betrugsüberweisungen erreicht?
36. Warum gibt es keinen einheitlichen bundesweiten Fraud-Notfallkanal zwischen Banken und Polizei?

37. Wie schnell werden bekannte Geldwäschekonten institutübergreifend erkannt?
38. Welche Verantwortung tragen Zahlungsdienstleister bei wiederkehrenden Betrugsempfängern?
39. Wie viele Anlageanzeigen werden vor Veröffentlichung auf Anbieteridentität und Erlaubnis geprüft?
40. Wie oft dürfen gesperrte Werbekunden mit neuer Domain oder neuem Account zurückkehren?
41. Warum werden bekannte Betrugsdomains nicht schneller browser- und suchmaschinenweit gewarnt?
42. Welche Plattformen veröffentlichen transparente Zahlen über entfernte Betrugsanzeigen?
43. Wer trägt die Kosten, wenn Plattformwerbung ein Opfer gezielt zu einer Betrugsseite führt?
44. Wie werden Deepfake-Werbungen technisch erkannt und gekennzeichnet?
45. Warum ist Betrugsprävention kein verpflichtender Bestandteil digitaler Verbraucherbildung?
46. Wie viele Schulen vermitteln praktisch, wie Phishing, Fake-Shops und Anlagebetrug funktionieren?
47. Wie werden Senioren erreicht, die keine Online-Warnkampagnen sehen?
48. Warum gibt es keine flächendeckenden Familien-Codewort-Kampagnen?
49. Wie werden Pflegeeinrichtungen, Banken und Taxibetriebe in Schockanrufprävention eingebunden?
50. Welche personellen Standards brauchen Schwerpunktstaatsanwaltschaften für Wirtschaftskriminalität?
51. Wie viele Wirtschaftsstrafverfahren liegen länger als zwei, drei oder fünf Jahre im Zwischenverfahren?
52. Welche organisatorischen Alarmmechanismen greifen bei außergewöhnlicher Verfahrensdauer?
53. Wie werden Geschädigte über den Stand langwieriger Verfahren informiert?
54. Warum ist digitale Forensik in manchen Behörden noch immer ein Engpass?
55. Wie schnell können internationale Kontodaten in dringenden Betrugsfällen gesichert werden?
56. Welche Rechtshilfewege könnten durch standardisierte Notfallverfahren beschleunigt werden?
57. Wie stark wird Vermögensabschöpfung als Erfolgskriterium gemessen?
58. Wie viel beschlagnahmtes Vermögen gelangt tatsächlich zu Geschädigten zurück?
59. Wie werden Recovery-Scams nach einem Erstbetrug systematisch verhindert?
60. Warum werden Opferdaten nicht stärker als besonders schutzbedürftig behandelt, nachdem sie in Täterlisten aufgetaucht sind?
61. Welche Regeln verhindern, dass Money-Mule-Konten lange aktiv bleiben?
62. Wie schützen Mobilfunkanbieter SIM-Tausch und eSIM-Prozesse gegen Social Engineering?
63. Wie schnell werden gestohlene Identitäten zwischen betroffenen Unternehmen signalisiert?
64. Warum akzeptieren manche Unternehmen weiterhin unsichere Identitätsprüfung per leicht kopierbarer Dokumente?
65. Wie werden QR-Codes an öffentlichen Zahlungspunkten gegen Überkleben geschützt?
66. Welche Standards gelten für verifizierte digitale Rechnungen und Bankverbindungsänderungen?
67. Warum ist ein zweiter Kommunikationskanal bei hohen Unternehmenszahlungen nicht überall Standard?
68. Wie werden Beschäftigte gegen CEO-Fraud und Deepfake-Stimmen geschult?
69. Welche deliktspezifischen Kriterien gelten bei der Eignungsprüfung für offenen Vollzug?
70. Wie wird bei Vermögensdelikten die Möglichkeit digitaler Wiederholungstaten bewertet?
71. Wie transparent sind Vollstreckungspläne und Zuständigkeitsregeln für die Öffentlichkeit?
72. Welche Sicherungen verhindern taktische Wohnsitzgestaltung zur Beeinflussung der Vollzugszuständigkeit?
73. Wie oft werden Lockerungen nach neuen Risikohinweisen überprüft?
74. Welche psychosoziale Hilfe steht Opfern großer Vermögensdelikte zur Verfügung?
75. Warum werden Vermögensdelikte häufig als weniger traumatisch behandelt als körperliche Delikte?
76. Wie kann Scham als Anzeigehemmnis systematisch reduziert werden?
77. Welche Behörde besitzt am Ende die Gesamtverantwortung für nationale Betrugsprävention?
78. Und die wichtigste Frage: Wer fühlt sich zuständig, bevor das Geld weg ist - nicht erst danach?

F. Quellen und Anmerkungen

[Q1] Bundeskriminalamt: „Betrugskriminalität 2024: Rückgang bei Fallzahlen - große Herausforderungen durch internationale Tatbegehungen“, 25.04.2025. 743.472 Inlandstaten, 513.518 Auslandstaten mit Erfolgsort Deutschland; Hinweis auf großes Dunkelfeld. https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/250425_Entwicklung_Betrugskriminalit%C3%A4t.html

[Q2] Bundeskriminalamt: Polizeiliche Kriminalstatistik 2024, ausgewählte Zahlen. Wirtschaftskriminalität 61.358 Fälle, +57,6 % gegenüber 2023. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2024/FachlicheBroschueren/Flyer.pdf

[Q3] Polizeiliche Kriminalprävention: Schockanrufe. Beschreibung von Unfall-/Kautionsmaschen und Hinweis, dass echte Polizeibeamte kein Geld am Telefon fordern. https://www.polizei-beratung.de/themen-und-tipps/betrug/schockanrufe/

[Q4] Bundesnetzagentur: Manipulation von Rufnummern. Erläuterung von Call-ID-Spoofing, realen und fiktiven aufgesetzten Nummern sowie technischen Grenzen der Behörde. https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Manipulation/start.html

[Q5] Bundesnetzagentur: Maßnahmenliste Rufnummernmissbrauch 2026. Dokumentiert u. a. Abschaltungen ermittelter Ursprungsrufnummern bei Rufnummernmanipulation. https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Aktuelles/Ma%C3%9Fnahmen/start_RM.html

[Q6] Polizeiliche Kriminalprävention: Aktuelle Warnungen 2026, unter anderem zu Silent Calls und KI-gestützten Betrugsrisiken. https://www.polizei-beratung.de/aktuelles/

[Q7] BaFin: Warnungen und Verbraucherschutz zu Anlagebetrug und unerlaubten Geschäften; laufende Warnmeldungen zu Plattformen und Identitätsmissbrauch. https://www.bafin.de/DE/Verbraucher/Finanzbetrug/finanzbetrug_node.html

[Q8] BaFin/BKA: Warnung vor Abzocke bei Geldanlagen im Internet und dubiosen Online-Handelsplattformen. https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/dl_schreiben_warnung_bafin_bka.pdf

[Q9] Bürgerschaft Hamburg, Drs. 22/15168 vom 10.05.2024: Angaben zur Anklage vom 03.07.2020, Übersendung am 08.07.2020, 1.730 tateinheitlichen Betrugsfällen, Schadensdarstellung und außergewöhnlichem Aktenumfang. https://www.buergerschaft-hh.de/parldok/dokument/87306/zahlreiche_betrugsopfer_warten_seit_jahren_auf_gerechtigkeit_funktioniert_der_rechtsstaat_noch.pdf

[Q10] Bürgerschaft Hamburg, Drs. 23/38 vom 04.04.2025: Landgericht hatte noch nicht über Eröffnung des Hauptverfahrens entschieden; Durchschnitt Wirtschaftsstrafkammer 2024: 8,0 Monate; Hinweis auf hohe Belastung. https://www.buergerschaft-hh.de/parldok/dokument/90632/23_00038_zahlreiche_lombardium_betrugsopfer_warten_seit_jahren_auf_gerechtigkeit_funktioniert_der_rechtsstaat_noch

[Q11] dpa/n-tv vom 24.08.2020: Berichte über 1.730 angeklagte Fälle und mehr als 50 Mio. Euro; Medienberichte zum weiteren Firmengeflecht nannten 7.000 Anleger und bis zu 200 Mio. Euro. https://www.n-tv.de/regionales/hamburg-und-schleswig-holstein/Pfandhausbetreiber-muss-sich-wegen-Betrugs-verantworten-article21992260.html

[Q12] Verbraucherzentrale: Fake-SMS zu Online-Banking, Steuerbescheiden und Gerichtsverfahren, Stand 29.05.2026. https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/fakesms-zu-onlinebanking-steuerbescheiden-und-gerichtsverfahren-67038

[Q13] Verbraucherzentrale: Paketdienst-SMS - Vorsicht, Abzocke!, Stand 22.07.2026. https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/paketdienstsms-vorsicht-abzocke-58988

[Q14] Verbraucherzentrale: Fälschungen im Netz - So entlarven Sie Betrüger:innen, Stand 11.02.2026. https://www.verbraucherzentrale.de/wissen/digitale-welt/soziale-netzwerke/faelschungen-im-netz-so-entlarven-sie-betruegerinnen-90402

[Q15] Strafvollzugsgesetz § 10: Offener Vollzug; Eignung insbesondere bei fehlender Flucht- und Missbrauchsgefahr. https://www.gesetze-im-internet.de/stvollzg/__10.html

[Q16] Strafvollzugsgesetz § 152: Vollstreckungsplan; örtliche und sachliche Zuständigkeit der Justizvollzugsanstalten wird durch die Landesjustizverwaltung geregelt. https://www.gesetze-im-internet.de/stvollzg/__152.html

G. Schlussnotiz zur Sprache

Die Ausdrucksweise dieses Buches ist absichtlich scharf. Sie richtet sich gegen Betrugsmaschen, kriminelle Strukturen und erkennbare Systemschwächen. Sie soll keine Person ohne rechtskräftige Feststellung als Täter brandmarken. Deshalb wurden Personennamen vollständig weggelassen.

Die schärfste Kritik wird dort am glaubwürdigsten, wo sie exakt bleibt. Anklage ist nicht Verurteilung. Offener Vollzug ist nicht automatisch „leichte Haft“. Eine Rufnummernmanipulation ist nicht deshalb erlaubt, weil sie technisch möglich ist. Und ein langes Verfahren ist nicht automatisch rechtswidrig. Aber all diese

Themen dürfen öffentlich hart gefragt werden - gerade weil Vertrauen in den Rechtsstaat von nachvollziehbarer Funktionsfähigkeit lebt.