



VU

Seniorenunion
vuronline.li

Senior:innen

-leichte Beute für Cyber- und andere Betrügereien?

Betrugsmaschen erkennen und vorbeugen

Freitag, 31. Oktober 2025, 09.00 bis 11.30 Uhr

Treffpunkt: VP Bank, Landstrasse 15, Triesen

Herzlich willkommen!

Begrüßung

Markus Schaper, Präsident der Seniorenunion

**Adrian Schneider, Mitglied der VP Bank-
Gruppenleitung**

Jürgen Eberle, Landespolizei, Abteilung Wirtschaftskriminalität

Zahlen, Fakten und Beispiele aus Liechtenstein





Sicher. Ihre Landespolizei



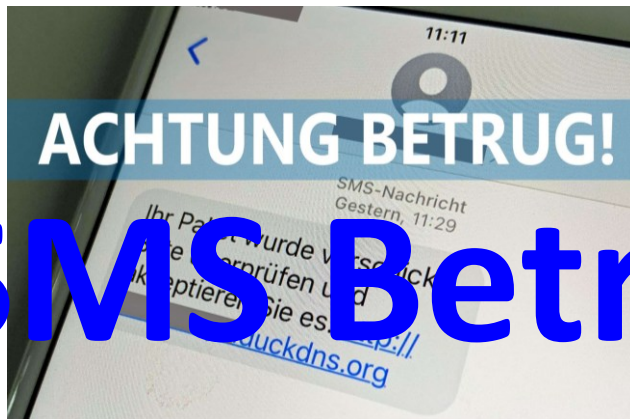


Betrugsphänomene

Falsche Polizisten

Anlagebetrug

SMS Betrug



Liebesbetrug

Massenbetrugsphänomene





Betrugsphänomene

- ▶ Diese Aufzählung von Betrugsphänomenen ist nicht abschliessen. Monatlich kommen neue Betrugsphänomene in neuer oder abgeänderter Form vor.
- ▶ Die Landespolizei oder andere Polizeien versuchen sofort bei bekanntwerden der Betrugsphänomene den Standort oder Täterschaft zu eruieren, um die örtlichen Behörden über die Machenschaften in Kenntnis zu setzen.
- ▶ Eine Information der Betrugsphänomenen erfolgt durch die Landespolizei nach bekanntwerden über die Zeitungen oder Social Media.





Zahlen und Fakten 2023 und 2024

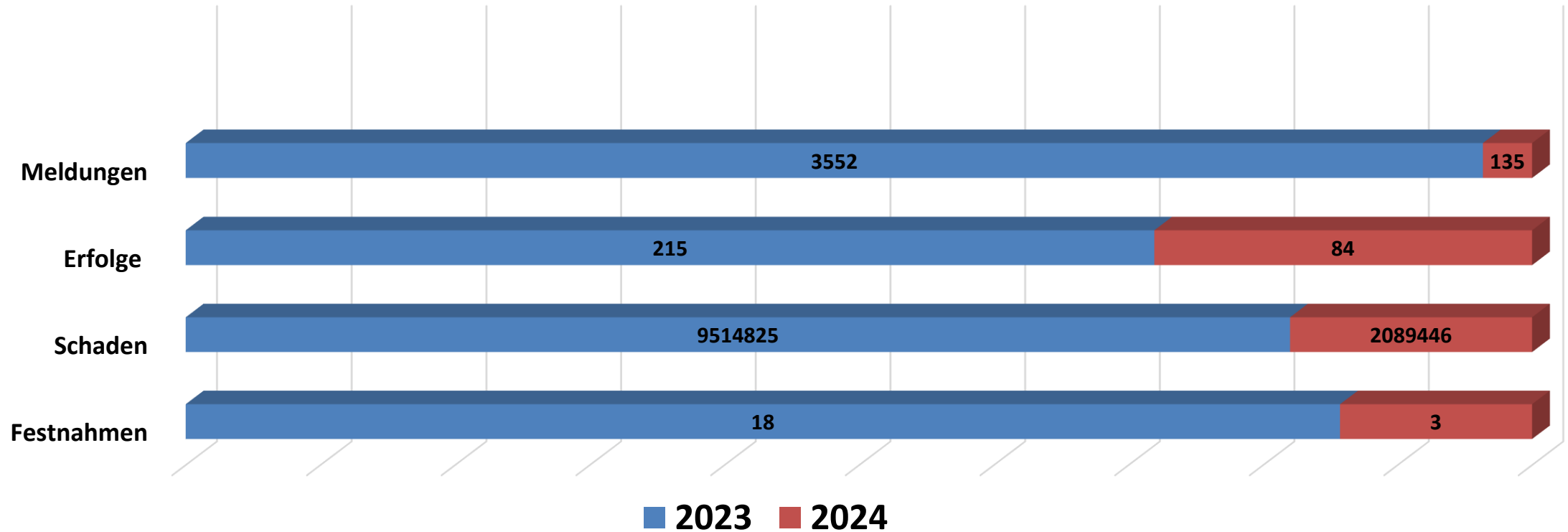
- ▶ Die Bundeskriminalpolizei FedPol in Bern ist zuständig für die organisierte Kriminalität. Sie sammelt und analysiert die in Liechtenstein und der Schweiz vorgefallenen Betrugsphänomene.





Zahlen und Fakten 2023 und 2024

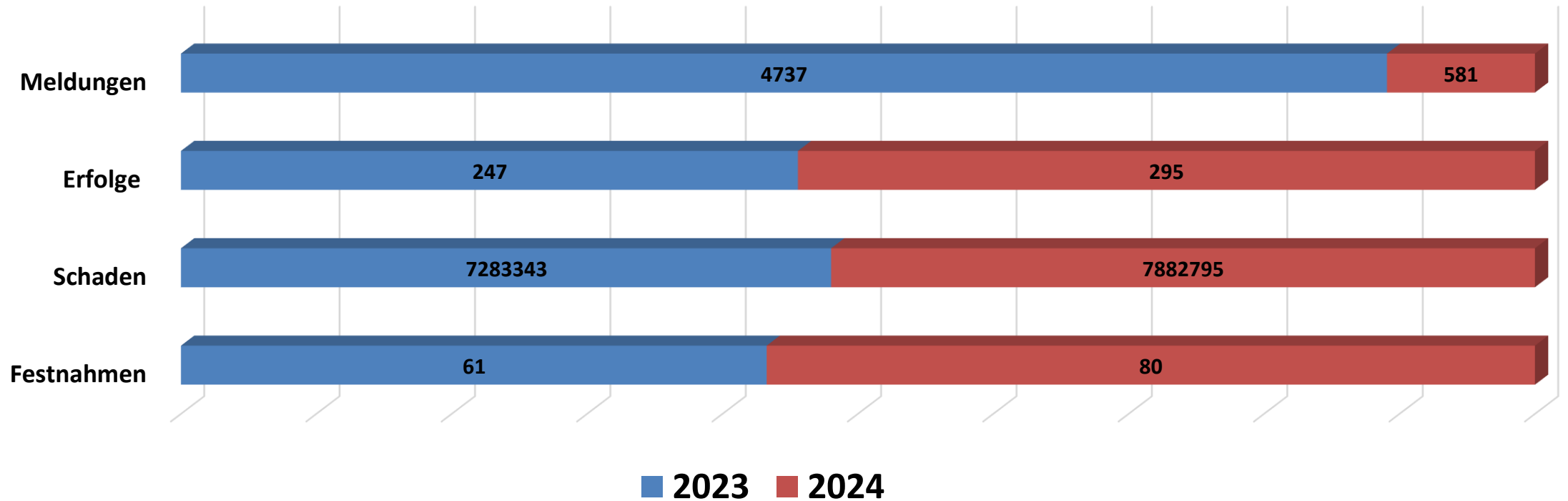
Betrugsphänomen Enkeltrick





Zahlen und Fakten 2023 und 2024

Betrugsphänomen Falsche Polizisten



Die Arbeit der Polizei

- Wieso ist es fast unmöglich eine Täterschaft zu ermitteln oder zu verhaften?



- Die Täterschaft tritt am Telefon, in Schreiben oder E-Mails immer mit gefälschten Namen, Adressen, etc. auf und hat den Sitz meistens im Ausland (Polen, Rumänien oder Türkei).





Die Arbeit der Polizei

- ▶ Verhaftet werden zu meist nur Abholer, die über dubiose Jobangebote z.B. Kurierfahrer angeworben. Die Abholer haben meistens keine Angaben des Auftraggebers.
- ▶ Ergaunertes Geld wird mittels Money Mule (sogenannter Geldesel, Personen die ihr Konto zur Verfügung stellen und Geld weiterüberweisen) an die Täterschaft übermittelt.



Die Landespolizei rät:



Übergeben Sie niemals Geld oder Wertgegenstände an unbekannte Personen!

- ▶ Seien Sie misstrauisch, wenn sich Personen am Telefon nicht mit Namen melden, sondern diesen erraten lassen. - Enkeltrickbetrug
- ▶ Seien Sie misstrauisch, wenn Sie von angeblichen Polizeibeamten mit ausländischen Akzent, meist sehr gutes Hochdeutsch, angerufen werden. (ACHTUNG neu können auch KI unterstützte Anrufe mit Dialekt geführt werden) – Falsche Polizisten



Die Landespolizei rät:



- ▶ Informieren Sie sofort die Polizei, wenn Ihnen eine Kontaktaufnahme oder Situation verdächtig vorkommt die Notrufnummer **117** oder **236 71 11** der Landespolizei wird ihnen helfen.
- ▶ Lassen Sie sich gegebenenfalls aus dem Telefonbuch streichen oder zumindest Ihren Vornamen abkürzen.



Die Landespolizei rät:



- ▶ **Nehmen Sie Warnungen von Bankangestellten ernst.**
- ▶ Telefonbetrüger warnen ihre Opfer vor unbequemen Fragen von Bankmitarbeitenden. Denn diese kennen die Merkmale des Telefonbetrugs. Sie haben in der Vergangenheit wiederholt solche Straftaten erkannt und verhindert. Nehmen Sie Warnungen von Bankangestellten ernst. Lassen Sie Unterstützung und Hilfe zu.



Die Landespolizei rät:



**Bei Verdacht –
Anruf!**

117

**Wir sind jederzeit
für Sie da!**

Sicher. Ihre Landespolizei



Und der letzte Rat der Landespolizei

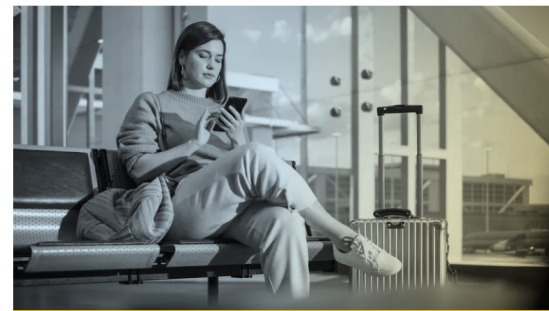
CYBERCRIMEPOLICE.CH

Alle Fälle Häufige Phänomene Warnliste

- Besuchen Sie die Internetplattform der **Cybercrimepolice.ch**, diese Internetseite ist ein Engagement der Polizei, welche aktuell zu den Internetbetrügen informiert und Tipps gibt, wie man sich davor schützen kann.

Cybercrimepolice.ch – ein Engagement Ihrer Polizei.

Wir informieren unabhängig und aktuell zu Internetbetrug und geben Tipps, wie man sich schützen kann.



17.09.2025 | Missbrauch von Online-Zahlungssyst./Wertkarten oder einer fremden Identität, um einen Betrug zu begehen

Phishing-Mail zielt auf Miles & More Kreditkarten-Login



Warnliste

Verdächtige Onlineplattformen

stingray.ink
avotrend.org
vibeshopy.com

Verdächtige Kryptoadressen

ltc1qqwq7gs7l2008zg2hlzmjgq5xzusxy0r5znha
1KEYrM9pri7qnNWyzE5yXpb63G5Xy5eEs
13KT5QPMWQrWuuiNmMXpRc46vbfGsgQDY

Verdächtige Immobilienplattformen

immo-pure.com
theprofitsupp.net
reallia-properties.com

www.cybercrimepolice.ch



Danke für Ihre Aufmerksamkeit!

Landespolizei des Fürstentums Liechtenstein
Gewerbeweg 4
FL-9490 Vaduz

+423/ 236 71 11

117

info@landespolizei.li

www.landespolizei.li





Ein Fall Beispiel

- ▶ 11:05 Uhr, bei Herrn MUSTER Max klingelt das Haustelefon. Die Anrufer Identifikation zeigt unbekannte Rufnummer an.
- ▶ Die Betrüger versuchen mit der Betrugsmasche Falsche Polizisten und das ein Familienmitglied ein schwerer Verkehrsunfall verursachte das Opfer zu Bargeldzahlungen zu verleiten.
- ▶ Herr MUSTER nimmt den Anruf entgegen und wird von einem angeblich hochdeutschsprechenden Polizisten in Kenntnis gesetzt, dass seine Schwester in Bregenz einen Verkehrsunfall mit tödlichem Ausgang verursacht habe.



Ein Fall Beispiel

- ▶ Herr MUSTER nimmt ihm Hintergrund des Telefonats eine weinende Frauenstimme war, welche er angeblich seiner Schwester zuordnete.
- ▶ Die Betrüger konnten mit dem Sachverhalt, dass seine Schwester aufgrund des tödlichen Verkehrsunfalls in Gefängnis muss, Herrn MUSTER so weit bringen, dass er bereit war eine Bargeldkaution für seine Schwester zu bezahlen, sodass diese nicht ins Gefängnis muss.



Ein Fall Beispiel

- ▶ Die Täterschaft gab an, dass nur der Anrufende Polizist, Staatsanwalt oder Richter die Möglichkeit habe seine Schwester vom Gefängnis zu bewahren und wenn das Gespräch von seiner Seite unterbrochen würde, so könne man nichts mehr für seine Schwester tun.
- ▶ Herr MUSTER gab in der Folge seine Mobilrufnummer an und stand von ca. 12:15 Uhr bis ca. 19:15 Uhr in ständigem telefonischen Kontakt mit der Täterschaft.



Ein Fall Beispiel

- ▶ Was passierte in der Zeit von ca. 12:15 Uhr bis ca. 19:15 Uhr?
- ▶ Herr MUSTER gab der Täterschaft seine Mobilrufnummer bekannt und stand von ca. 12:15 Uhr bis ca. 19:15 Uhr mit seinem Mobiltelefon in ständigen telefonischen Kontakt mit der Täterschaft. So konnte die Täterschaft stetigen Druck auf Herrn MUSTER ausüben und mit hören, mit wem MUSTER spricht.
- ▶ So konnte die Täterschaft MUSTER dazu bewegen auf die Bank zu gehen und einen Betrag in der der Höhe von CHF 50'000.00 abzuheben.



Ein Fall Beispiel

- ▶ Der Versuch bei einer weiteren Bank ebenfalls einen hohen Bargeldbetrag abzuheben konnte durch die Bankangestellte verhindert werden.
- ▶ Nachdem die Täterschaft mit allen Möglichen Mitteln versucht hat, Herrn MUSTER um sein Vermögen zu bringen, musste Herr MUSTER mit seinem Personenwagen eine ca. 1½-stündige Irrfahrt durch Liechtenstein bis nach Feldkirch über sich ergehen lassen, immer mit der Absicht, seine Schwester vor dem Gefängnis zu bewahren.



Ein Fall Beispiel

- ▶ In Feldkirch kam es um ca. 19:15 Uhr auf einem Parkplatz zur Bargeldübergabe an einen Herrn MUSTER unbekannte Person.
- ▶ Zu Hause angekommen dämmerte es Herrn MUSTER und er rief seine Schwester an, die ihm erklärte, dass bei ihr alles in Ordnung sei und er betrogen worden war.

Ein Fall Beispiel

- ▶ Die Landespolizei überprüfte die täterische Rufnummer über den Provider, welche sich als Prepaid Mobilnummer aus Norwegen herausstellte. – Keine weiteren Ermittlungsansätze.
- ▶ Mit dem Landeskriminalamt Vorarlberg wurden sämtliche Kameras in der Umgebung der Geldübergab gesichtet, um den Geldabholer zu identifizieren. – Keine Kamera hat den Geldabholer erfasst.
- ▶ Beim Geldübergabeort wurden die bei der Geldabholung erfassten Mobilgeräte welche sich dort eingeloggt hatten angeregt auszuwerten. – Keine Auswertung da Antrag abgewiesen wurde.



Fazit

- ▶ Ein Geschädigter mit einem Vermögensschaden in der Höhe von CHF 50'000.00.
- ▶ Keine Ermittlungsansätze zur telefonischen Täterschaft und dem Abholer.

Dr. med. Marc Risch, Facharzt für Psychiatrie & Psychotherapie

Multiperspektivische Betrachtung zu Täter-Opfer Dynamiken





Stiftung
TIEFSINN



**SeniorInnen – leichte Beute für Cyber-
und andere Betrügereien?**

Multiperspektivische Betrachtung zu Täter-Opfer Dynamiken





Stiftung
TIEFSINN

Agenda

Seins-, Wahrnehmungs-, Beziehungs- und Kommunikationskonzepte

Tätersicht – Opfersicht

Täter – Opferinteraktion

Empfehlungen





Stiftung
TIEFSINN

Seins-, Wahrnehmungs-, Kommunikations- und Beziehungskonzepte

Bio-Psycho-Soziales Modell

Maslov'sche Bedürfnispyramide

Sender-Empfänger Modell

Ebenen der Wahrnehmung

4-Ohren Modell

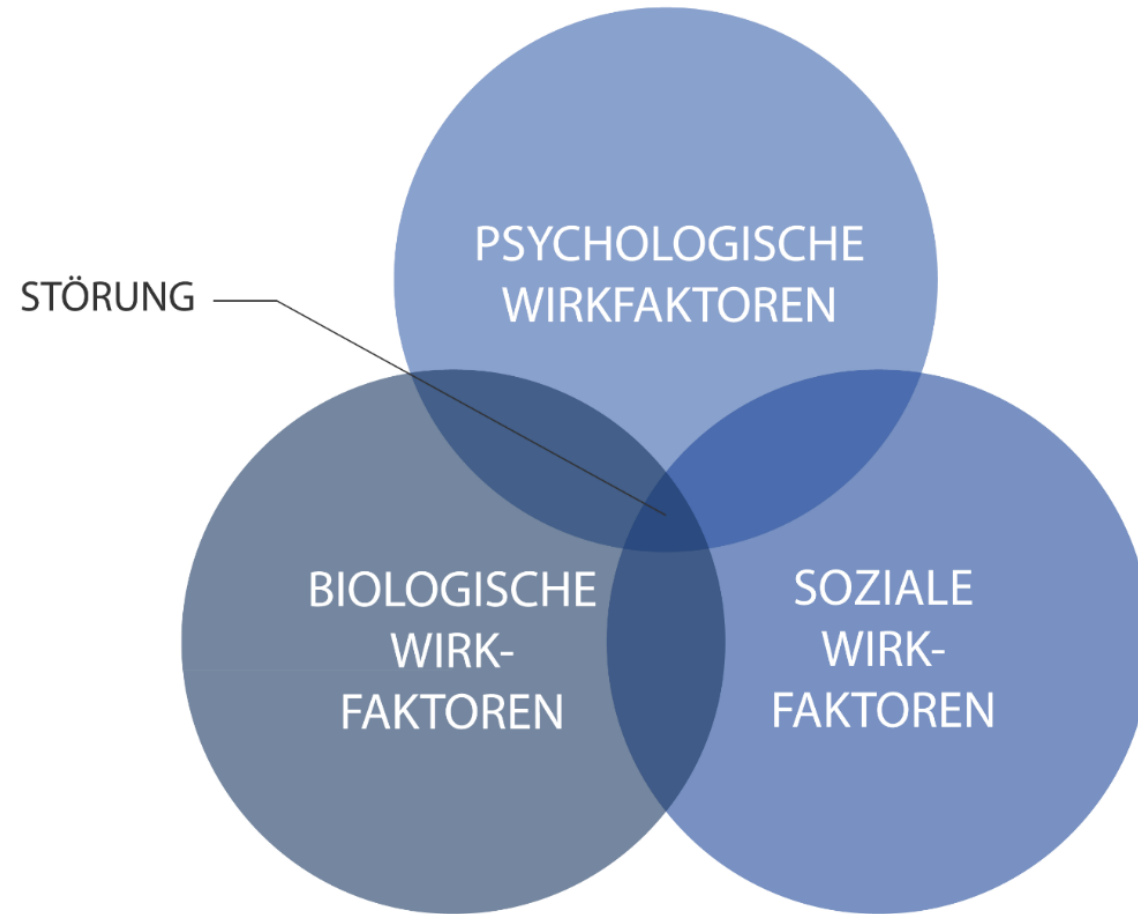
Ich-Ebenen und Transaktionen

Drama-Dreieck



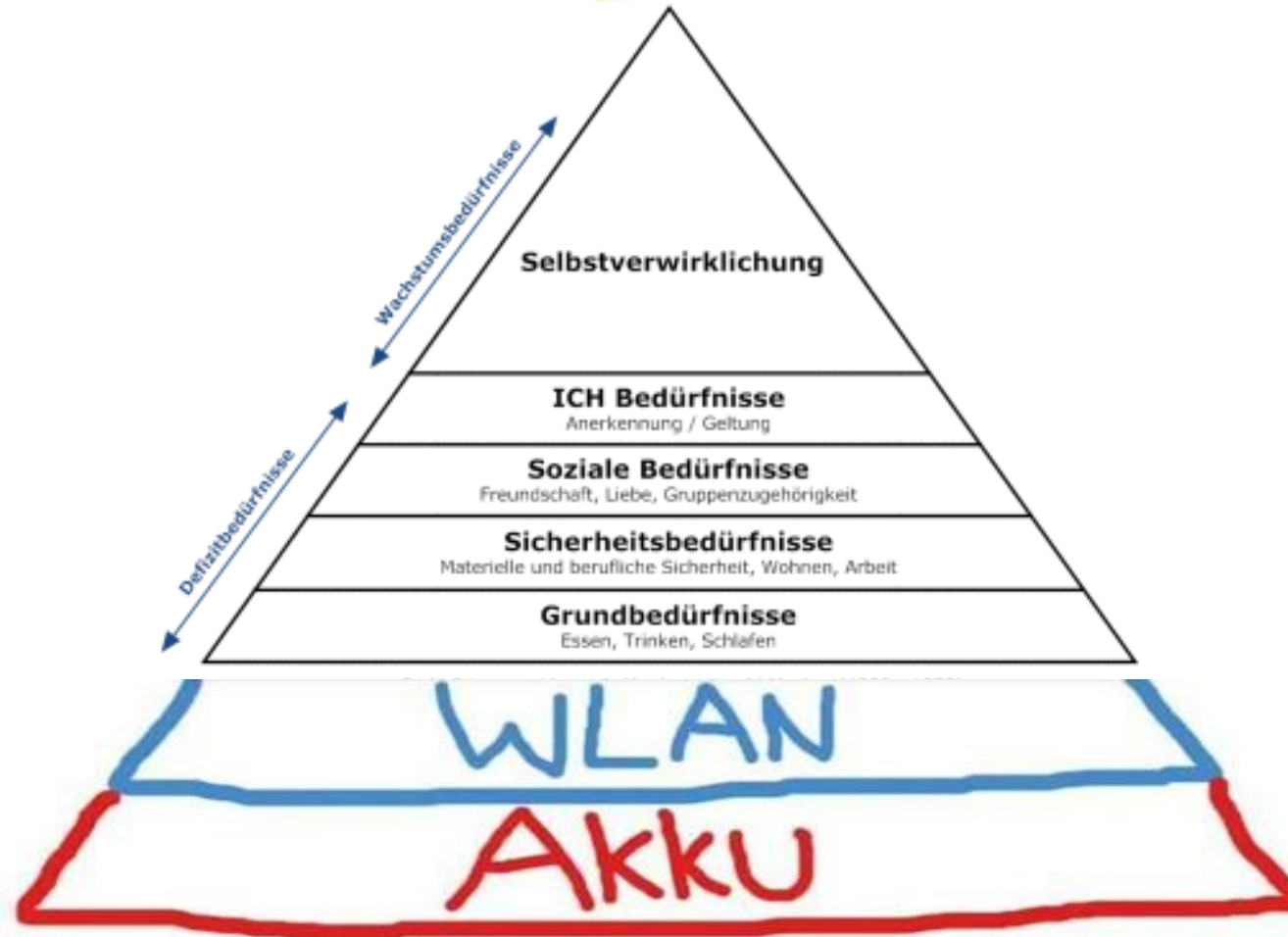


Stiftung
TIEFSINN





Stiftung
TIEFSINN

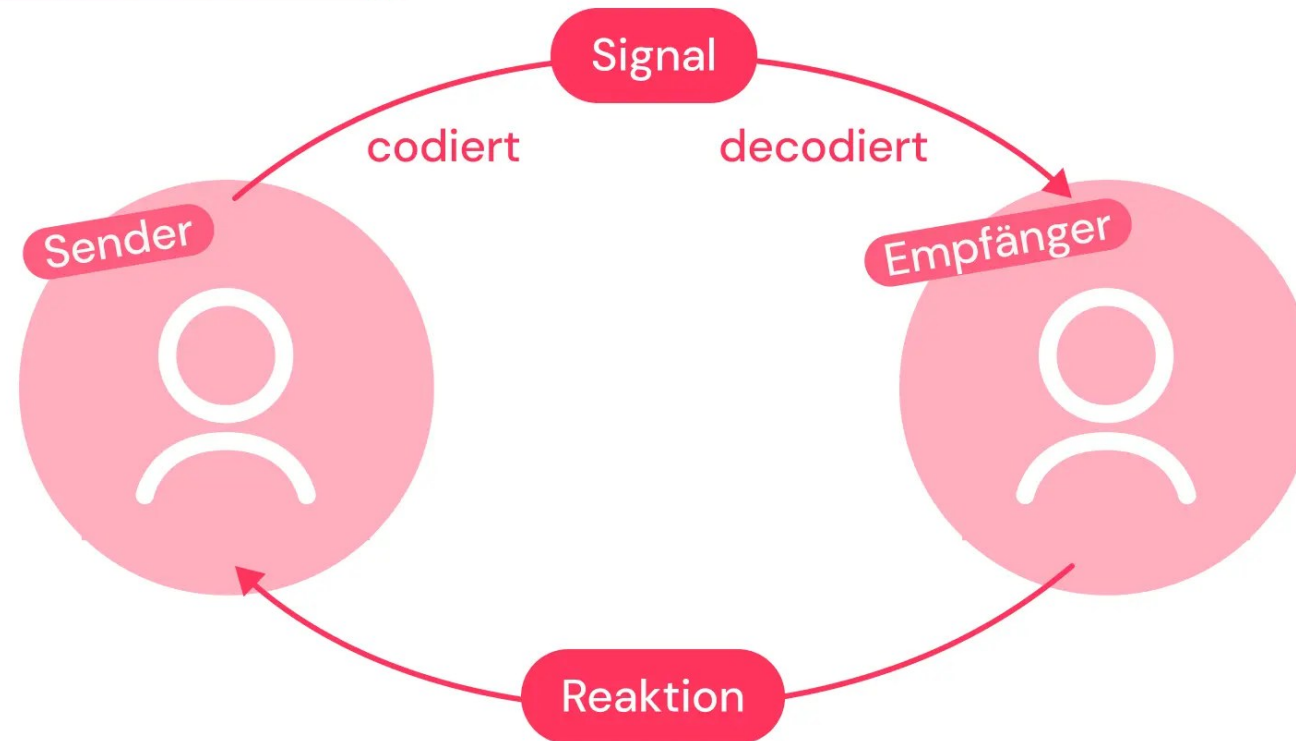






Stiftung
TIEFSINN

Sender-Empfänger-Modell





Stiftung
TIEFSINN

Wahrnehmung

visuell
auditiv
kinästhetisch
olfaktorisch
gustatorisch

Reaktion

bewusste oder automatische
- Empfindung
- Handlung

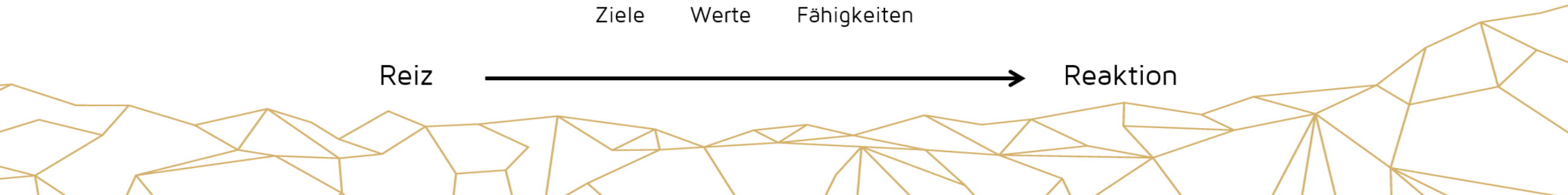
Interpretation

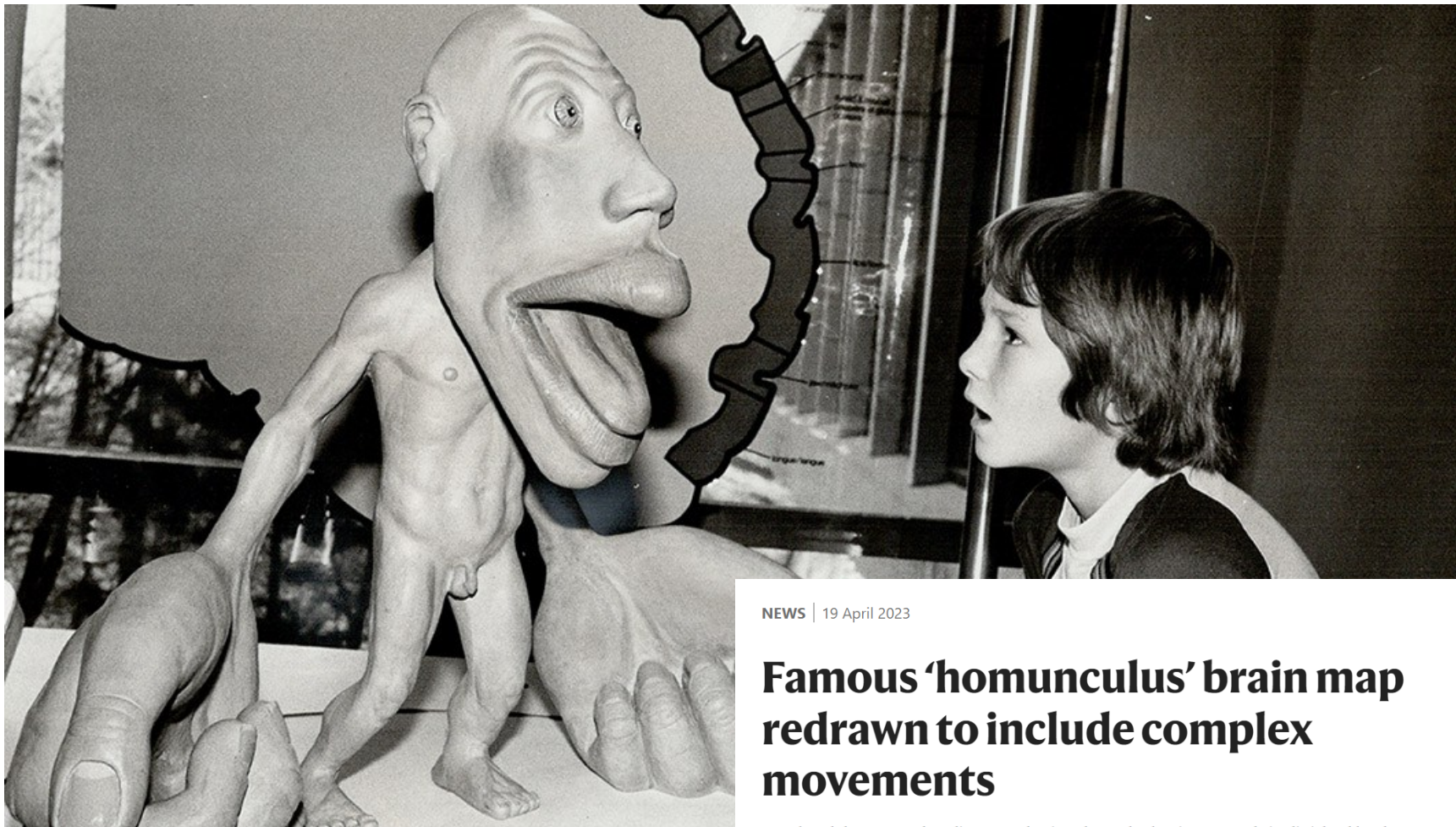
Ziele Werte Fähigkeiten

Reiz



Reaktion





NEWS | 19 April 2023

Famous 'homunculus' brain map redrawn to include complex movements

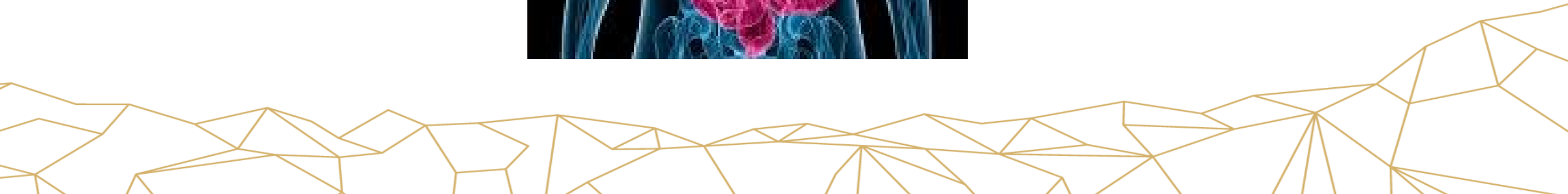
Textbook homunculus diagram depicts how the brain controls individual body parts – the revamp could improve treatments for brain injury.

nature 2023





Stiftung
TIEFSINN



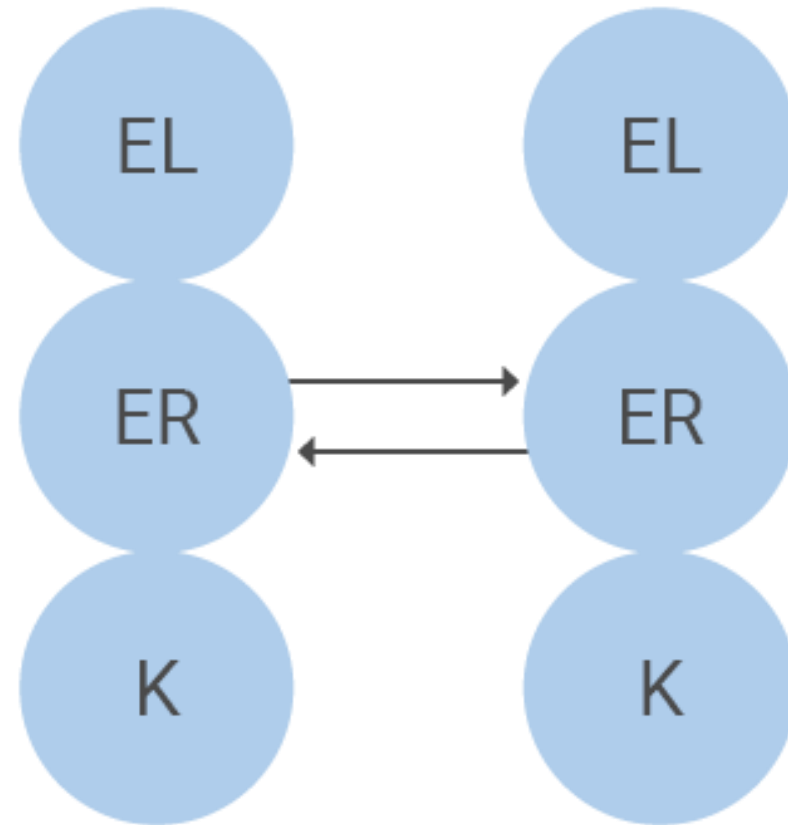
Das 4 Ohren-Modell

Nach Friedemann Schulz von Thun





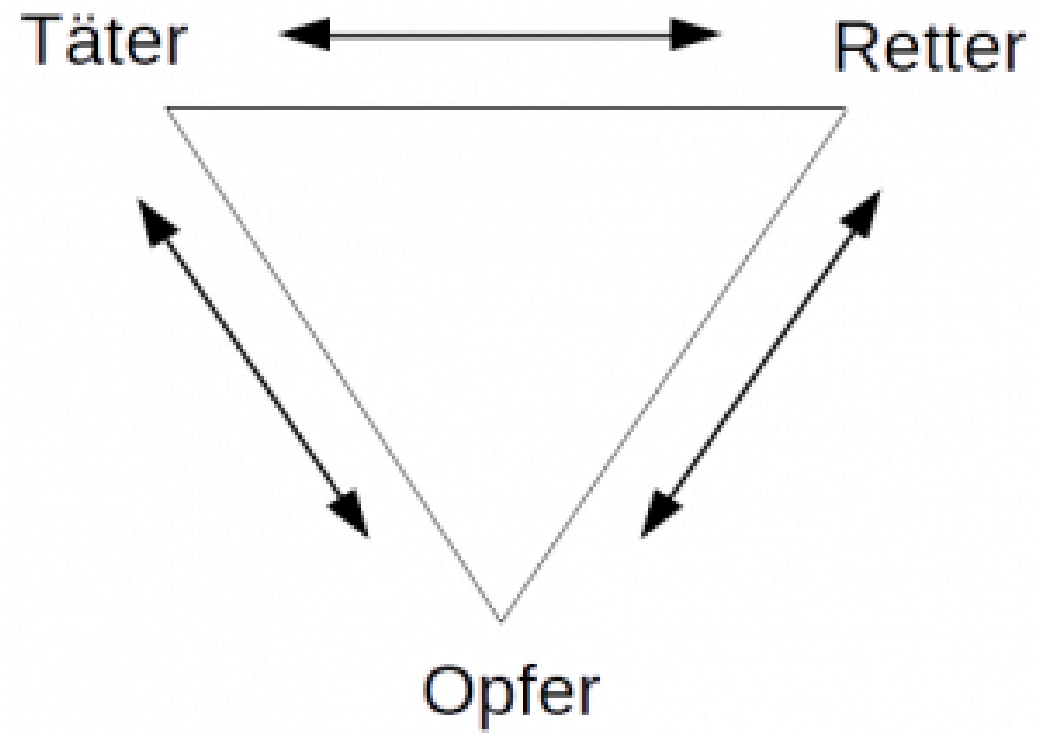
Stiftung
TIEFSINN



Ich-Ebenen-Modell & Transaktionen



Stiftung
TIEFSINN





Stiftung
TIEFSINN

Tätersicht - Opfersicht







Stiftung
TIEFSINN

Emotionaler „Terror“

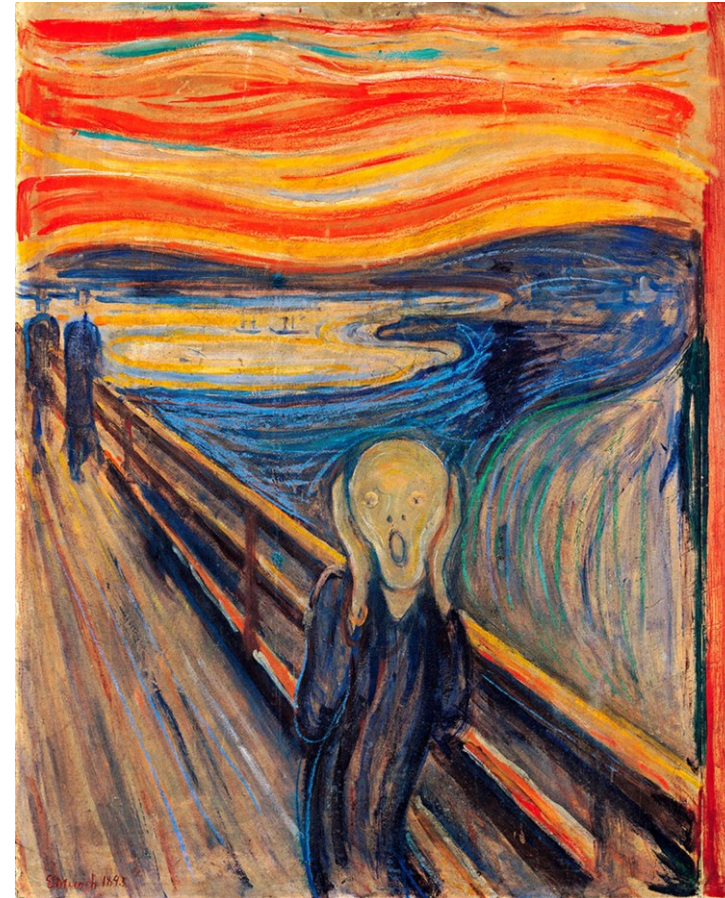
Katastrophisieren

Kognitive Verzerrung

Kognitive Dissonanz

Überforderung

„information overload“ ...





Stiftung
TIEFSINN



information overload
durch TEMPO & DRAMA





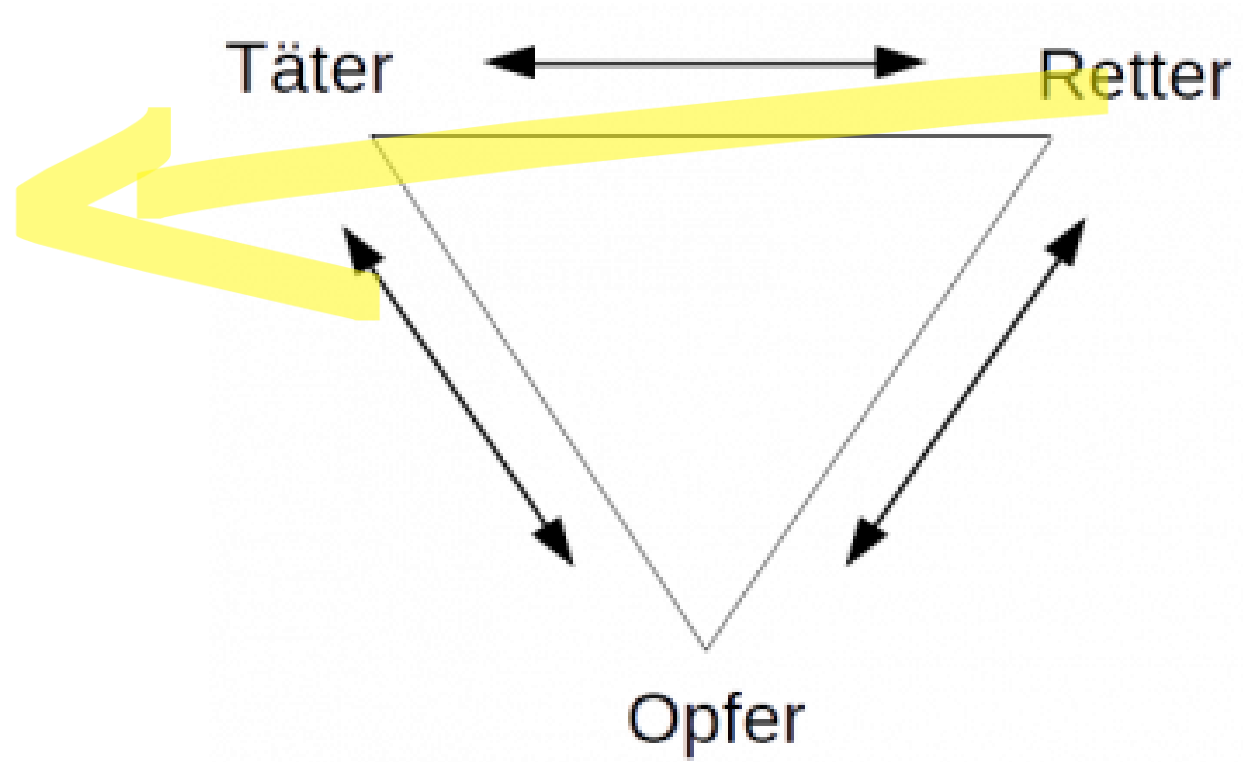
Stiftung
TIEFSINN



Low-Hanging Fruits ernten!
Mit wenig Aufwand schnelle Resultate
mit großer Wirkung erreichen



Stiftung
TIEFSINN





Stiftung
TIEFSINN

Typisches OPFER?





Stiftung
TIEFSINN





Stiftung
TIEFSINN



verrückte Welt
neue Kommunikationsmittel
„Chancen“ für Kriminelle



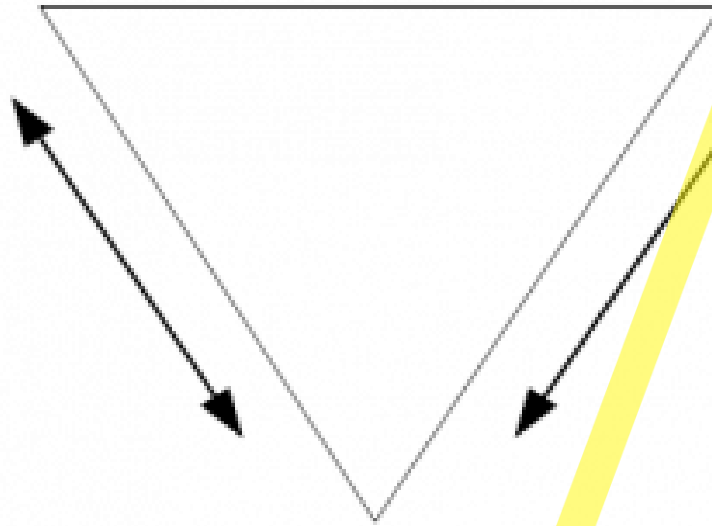


Stiftung
TIEFSINN

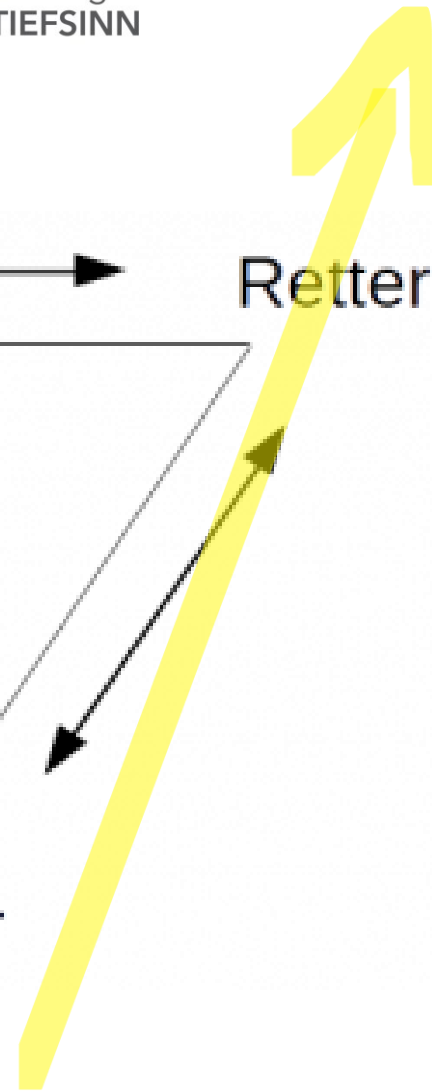
Täter



Retter



Opfer

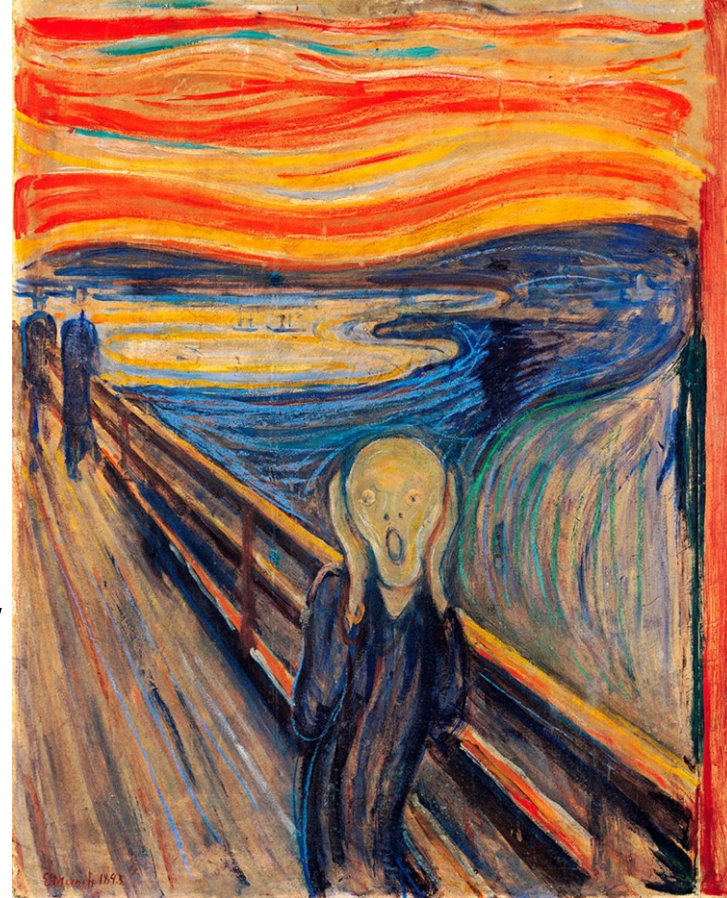




Stiftung
TIEFSINN

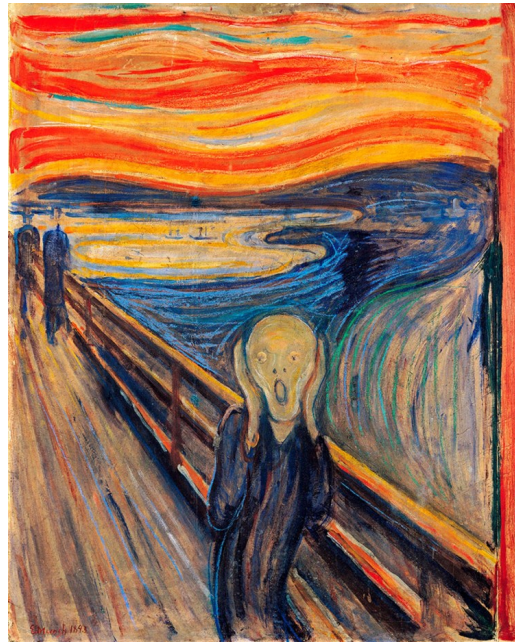
Täter-Opferinteraktion

*„Momentum der
emotionalen Verwirrung“*



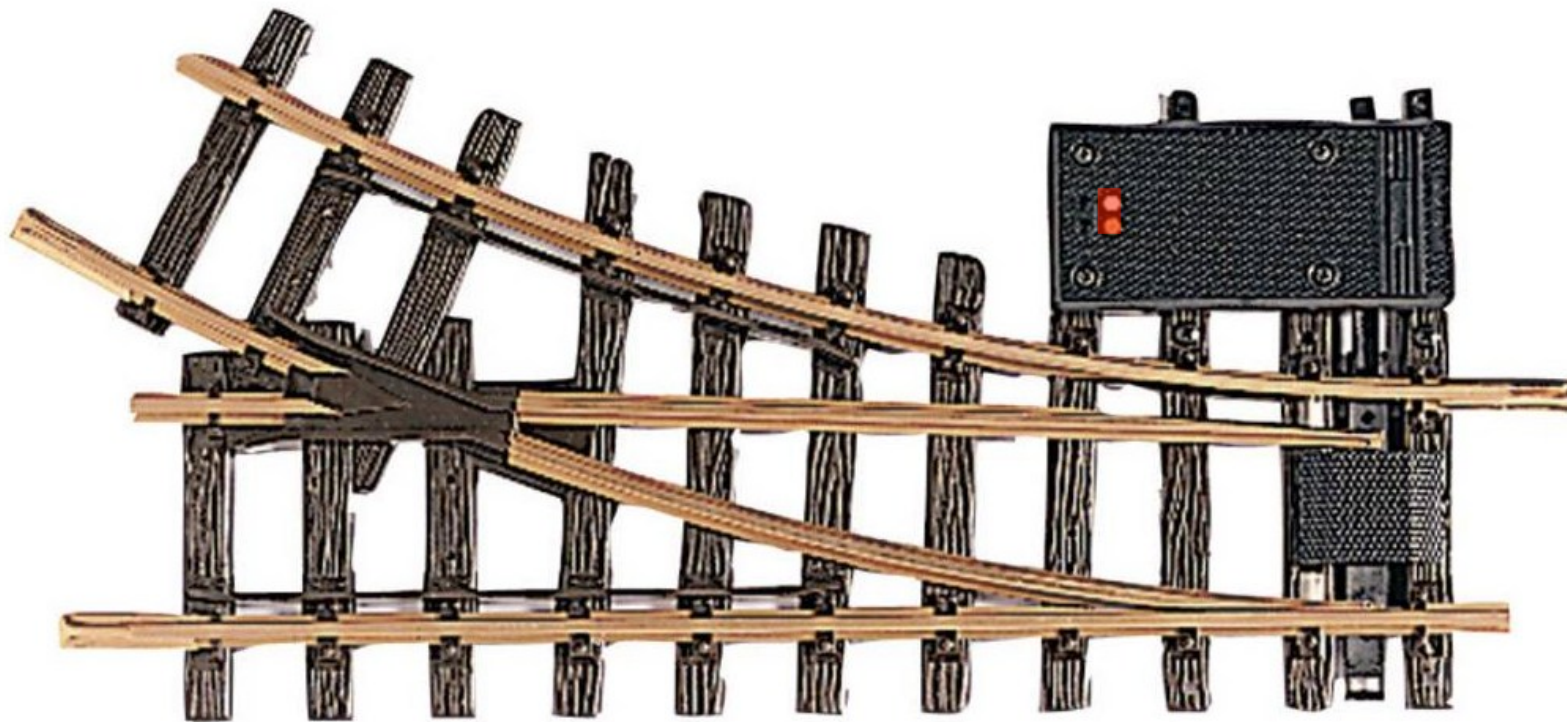


Stiftung
TIEFSINN





Stiftung
TIEFSINN





Stiftung
TIEFSINN

Bei „non response“

*„Täter-Opfer-Umkehr
suggestiert“*

Don't.

Shoot.

The.

Messenger.



Stiftung
TIEFSINN

Empfehlungen





Stiftung
TIEFSINN

Shoot.

The.

Messenger.





Stiftung
TIEFSINN



CALLBACK



Stiftung
TIEFSINN





Stiftung
TIEFSINN

DAS BAUCHGEFÜHL
IST EIN VERDAMMT
KLUGER KOPF.





Stiftung
TIEFSINN

KESTER SCHLENZ

ICH KOMM DA NICHT MEHR MIT

SPIEGEL
Bestseller-
Autor



Wie Informationsflut und
digitale Überforderung uns in
den Wahnsinn treiben –
wenn wir es zulassen!

mosaik

Martin Möbes, Group Information Security

Einblick in **Investmentbetrug** und Tipps zum Schutz



Agenda & Ziel

Ziel: Aufklärung über häufige Betrugsmaschen und Schutzmassnahmen

- Was ist Investmentbetrug
- Typische Betrugsmaschen
- Wie die Betrüger vorgehen
- Warnzeichen erkennen
- So schützen Sie sich
- Was tun im Verdachtsfall

Was ist Investmentbetrug?

Definition:

Falsche oder betrügerische Angebote für Geldanlagen, die hohe Renditen versprechen

Ziel der Betrüger:

Geld und/oder persönliche Daten erbeuten

Beispiele:

Falsche Aktien, Kryptowährungen, Immobilienprojekte

Gefälschte Online-Trading-Plattformen (z. B. 'Bitcoin Code', 'FX-Leader')

Social-Media-Werbung mit Prominenten (z. B. gefälschte Thomas-Gottschalk-Anzeigen)

E-Mail-Betrug mit "**passivem Einkommen**"

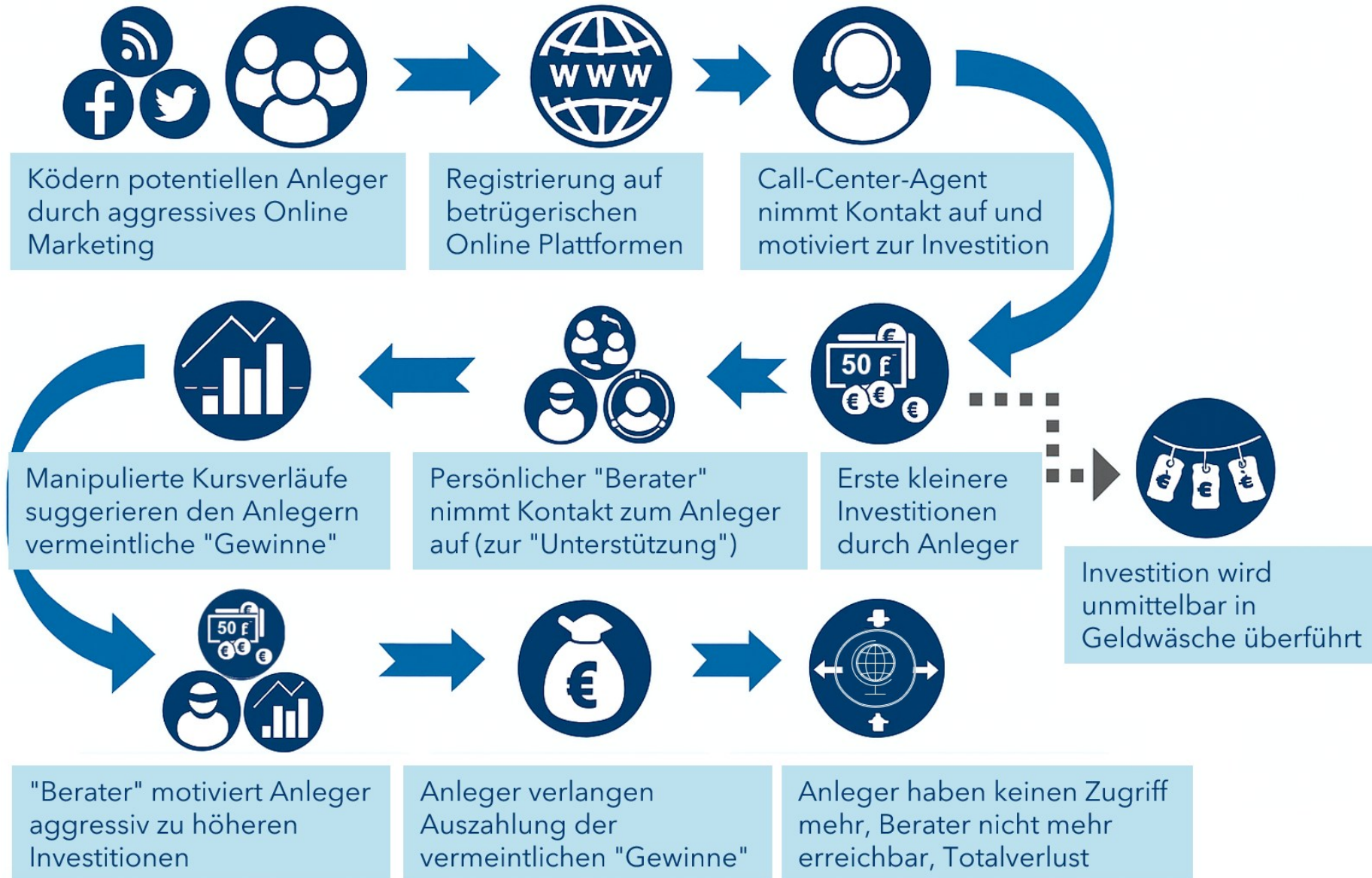


Typische Betrugsmaschen

- Telefonbetrug:
„Geheime Investition“ mit hoher Rendite
- E-Mail/Internet:
Gefälschte Webseiten oder Angebote
- Social Media:
Kontaktaufnahme durch vermeintliche Experten
- Dringlichkeit:
„Nur heute verfügbar!“ – Druck erzeugen



Wie die Betrüger vorgehen



Warnzeichen erkennen

- Versprechen von „garantierten“ Gewinnen bzw. hohe Renditen bei minimalem Risiko
- Undurchsichtige Kontakt- und Anbieterinformationen
- Zeitdruck oder Drängen zum schnellen Handeln
- Ungewöhnliche Zahlungsmethoden per Kryptowährung oder Auslandsüberweisung
- Rezensionen können helfen, aber auch gefälscht sein → somit Vorsicht
- Keine Zulassung bei Finanzmarktregulierung: FMA, FINMA, BaFin...



So schützen Sie sich

- Niemals unter Druck entscheiden
- Anbieter genau prüfen, nur bei lizenzierten Finanzinstituten investieren (z. B. FMA, FINMA ...)
- Keine persönlichen Daten am Telefon oder per E-Mail, WhatsApp preisgeben (z.B. Zugangsdaten e-Banking, Passwörter etc.)
- Kein (Fern-) Zugriff auf Gerät (und e-Banking gewähren)
- Bei "garantiertem Gewinn" immer skeptisch sein
- Mit Familie, Bankberater oder Polizei sprechen



Was tun im Verdachtsfall?

- Kontakt sofort abbrechen
- Keine Zahlungen leisten
- Polizei informieren
- Dokumentation sichern (E-Mails, Telefonnummern, Screenshots)

Nützliche Anlaufstellen

- Polizei / Cybercrime-Hotline
→ Betrugsverdacht Anzeige erstellen
- Finanzmarktaufsicht (FMA, FINMA ...)

Wissenswertes kompakt: Glossar & FAQ

Glossar - wichtige
Begriffe einfach erklärt.

Begriff
PIN
Passwort
TAN
CW

FAQ - Häufige Fragen zu
digitalen Zahlungen und
Sicherheit.

Warum gibt es so viele Begriffe für «Geheimwörter»?
Jeder Begriff bezeichnet eine andere Art von Sicherheits-
merkmal: PIN, Passwort/Kennwort, TAN, CW.
Diese Vielfalt dient der Sicherheit, denn verschiedene
Systeme brauchen unterschiedliche Schutzmechani-

Zusammenfassung

- Investmentbetrug ist raffiniert, aber erkennbar
- Betrüger treten oft sehr professionell auf
- Anzeichen erkennen, wie etwa Zeitdruck und Unterstützung bei Zahlungen
- Ruhe bewahren, Angebote sorgfältig prüfen, beraten lassen
- "gesunder Menschenverstand" - "es gibt nichts geschenkt"





Partnerschaft bedeutet, die Ziele unserer Kundinnen und Kunden zu **gemeinsamen Zielen** zu machen. Für den **langfristigen Erfolg**.



Danke

**Danke für Ihre Aufmerksamkeit und
herzlich willkommen beim Apéro!
Offeriert von der VP Bank AG**

Disclaimer

Obwohl bei der Ausarbeitung dieser Dokumentation grösstmögliche Sorgfalt angewandt wurde, können wir keine Gewähr für die Vollständigkeit, Aktualität oder Richtigkeit der darin enthaltenen Informationen übernehmen. Die Angaben in dieser Dokumentation dienen lediglich Informationszwecken und sind weder als Angebot, Aufforderung zur Offertstellung noch als öffentliche Werbung aufzufassen, welche zu Transaktionen mit bestimmten Finanzinstrumenten oder zur Inanspruchnahme von Dienstleistungen auffordern.

Diese Dokumentation stellt insbesondere keine Anlageberatung dar und trägt spezifischen oder zukünftigen Anlagezielen, finanziellen oder steuerlichen Umständen oder sonstigen besonderen Bedürfnissen einer Anlegerin oder eines Anlegers keine Rechnung. Ebenso können je nach Staatsangehörigkeit oder Wohnsitz einer Anlegerin oder eines Anlegers gesetzliche Beschränkungen hinsichtlich Transaktionen mit Finanzinstrumenten oder der Inanspruchnahme von Dienstleistungen bestehen. Bevor eine Anlegerin oder ein Anleger einen Anlageentscheid fällt bzw. Dienstleistungen in Anspruch nimmt, sollte sie oder er sich daher durch die eigene Kundenberaterin oder den eigenen Kundenberater beraten lassen.

Der Wert sowie die Erträge von Finanzinstrumenten können sowohl steigen als auch sinken. Es ist möglich, dass eine Anlegerin oder ein Anleger den ursprünglich investierten Betrag nicht mehr zurückerhält. Die bisherige Performance ist kein verlässlicher Indikator für zukünftige Resultate. Jedes Finanzinstrument kann mit den nachfolgenden, nicht abschliessend aufgezählten Risiken behaftet sein: Emittenten- (Bonitätsrisiko), Markt-, Kredit-, Liquiditätsrisiko, Zins- und Währungsrisiko sowie wirtschaftliches und politisches Risiko. Näheres zu diesen Risiken kann der Broschüre «Risiken im Effektenhandel» des Liechtensteinischen Bankenverbandes, welche unter www.bankenverband.li verfügbar ist, entnommen werden.

Die Haftung für sämtliche Schäden respektive Verluste, welche auf der Grundlage der in dieser Dokumentation enthaltenen Informationen geltend gemacht werden, ist ausgeschlossen. Diese Dokumentation ist urheberrechtlich geschützt und ihre Verwendung ausser zum privaten Gebrauch bedarf unserer vorgängigen Zustimmung.

© VP Bank AG
Aeulestrasse 6 · 9490 Vaduz · Liechtenstein · T +423 235 66 55
info@vpbank.com · www.vpbank.com · MwSt.-Nr. 51.263 · Reg.-Nr. FL-0001.007.080-0