
Swiss Banking
Swiss Anti-Fraud Summit
30. Juni 2026

# Das heutige Programm

## Teil 1

| | | |
|---|---|---|
| 13.00 | | **Eröffnung der Veranstaltung**<br>*August Benz, Swiss Banking · Cornelius Dorn, SIX* |
| 13.15 | KEYNOTE | **Inside the Fraudster's Playbook**<br>*Alex Wood, BBC Speaker* |
| 14.00 | KEYNOTE | **Die Wertschöpfungskette in der Betrugsbekämpfung**<br>*Stefan Giger & Elisa-Sophie Eikevaag, SIX* |
| 14.30 | PANEL | **Fraud: Einblicke und Erfahrungen führender Finanzinstitute**<br>*Max Piehl, UBS · Romano Ramanti, Zürcher Kantonalbank · Manuela Inauen, St.Galler Kantonalbank* |
| 15.10 | KEYNOTE | **Die Zukunft der Betrugsbekämpfung braucht Netzwerkeffekte**<br>*Elisa-Sophie Eikevaag, SIX* |
| 15.30 | | **Pause** |

# Heute auf der Bühne

## Teil 1

**Sarah A. Schütz**
Moderatorin

**August Benz**
Leiter International & Transformation, stv. CEO, *Swiss Banking*

BEGRÜSSUNG

**Stefan Giger**
Head Payment Fraud & Dispute Services, *SIX*

KEYNOTE

**Cornelius Dorn**
Head Strategy, Future Business & Terravis, *SIX*

BEGRÜSSUNG

**Manuela Inauen**
Leiterin Produktmanagement, *St. Galler Kantonalbank*

PANEL

**Alex Wood**
Keynote Speaker zu Fraud, Cybercrime und Social Engineering, *BBC*

KEYNOTE

**Max Piehl**
Fraud Initiative Lead, *UBS*

PANEL

**Elisa-Sophie Eikevaag**
Head Multi Rail Fraud Prevention, *SIX*

KEYNOTE

**Romano Ramanti**
Vizedirektor, Certified Ethical Hacker, *Zürcher Kantonalbank*

PANEL

# Das heutige Programm

## Teil 2

16.00 **KEYNOTE**
**Was die Daten nicht sehen – Der Faktor Mensch**
*Jill Wick, Jill Wick GmbH*

16.30 **KEYNOTE**
**Cybercrime gemeinsam statt alleine vorbeugen**
*Serdar Günal Rütsche, KaPo ZH/NEDIK*

17.00 **PANEL**
**Wie durchbrechen wir die Betrugskette – und wer muss wo handeln?**
*Richard Hess, Swiss Banking · Oskar Braszczynski, Meta · Katharina Höhn, TWINT · Susanne Grau, Hochschule Luzern*

17.30
**Zusammenfassung & Takeaways**

17.40
**Apéro & Networking**

# Heute auf der Bühne

## Teil 2

**Sarah A. Schütz**
Moderatorin

**Jill Wick**
Cyber Security Awareness Consultant & Wirtschaftspsychologin, *Jill Wick GmbH*

KEYNOTE

**Katharina Höhn**
Head Fraud Management, *TWINT*

PANEL

**Serdar Günal Rütsche**
Chef Cybercrime & Leiter NEDIK, *Kantonspolizei Zürich*

KEYNOTE

**Susanne Grau**
Leiterin Bereich Wirtschafts-kriminalistik, *Hochschule Luzern*

PANEL

**Richard Hess**
Leiter Digital Finance, *Swiss Banking*

PANEL

**Oskar Braszczynski**
Government & Social Impact Partner, *Meta*

PANEL

BEGRÜSSUNG

# Willkommen zum Swiss Anti-Fraud Summit 2026!

**August Benz**
Leiter International & Transformation,
stv. CEO, Swiss Banking

**Cornelius Dorn**
Head Strategy, Future Business
& Terravis, SIX

KEYNOTE

# Inside the Fraudster's Playbook: How External Fraud Really Succeeds – And How to Stop It

**Alex Wood** · Keynote Speaker on Fraud, Cybercrime and Social Engineering · BBC Presenter

# ALEX WOOD

CYBERCRIME, AI, SOCIAL ENGINEERING & COUNTER FRAUD SPEAKER

Alex is one of the most highly sought-after speakers in global finance. However, he was also responsible for some of the most high-profile and high-harm financial offences in modern criminal history.

Having served three lengthy stretches, Alex was finally released from prison in 2022 and has since turned his life around.

He now advises global financial institutions, banks, law firms, risk specialists,  Police forces and the UK Government and is a regular commentator on primetime TV (recent appearances including Good Morning Britain, This Morning and ITV News).  His written work has been featured in the Sunday Times, The Sun and the Daily Mail.

Alex is a resident member of the popular BBC Radio 4 show ‘Scam Secrets’ alongside Shari Vahl and Dr. Elisabeth Carter.

# SPEAKER QUALIFICATIONS

BBC NEWS

Home UK World Business Poli

## 'Fake duke' Alex Wood jailed for London hotels fraud

9 December 2015


The Duke of Marlborough (left) is more than 25 years older than Alexander Wood

Daily Mail MORE STORIES

## Cyber fraudster jailed for pretending to be the Duke of Marlborough is sent back to prison over a £2million scam

By Rebecca Camber Crime Correspondent For The Daily Mail
02:10 21 Jul 2018, updated 02:17 21 Jul 2018

Support us → The Guardian
News website of the year

News Opinion Sport Culture Lifestyle

UK news

## Fraudster who posed as aristocrat to stay in top London hotels is jailed

Ham&High Subscribe

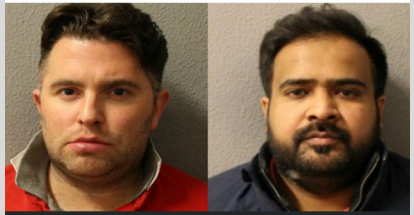
News Sport Things to do More

News > Crime Traffic & Travel Local Council


## Jailed: Conman who defrauded businesses of £2m

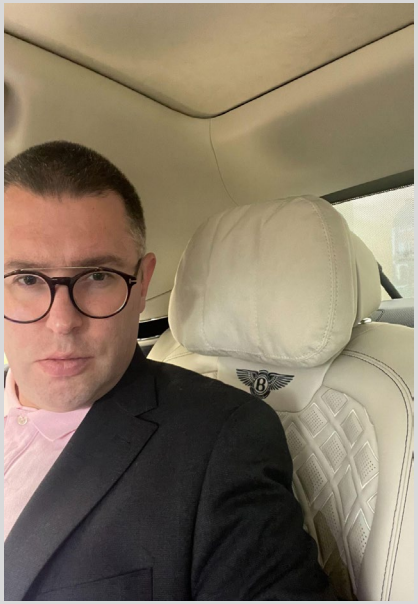
13th July 2018

CRIME



Alexander Wood and Muhammed Azhar. Picture: Metropolitan Police *(Image: Archant)*

# SPEAKER QUALIFICATIONS



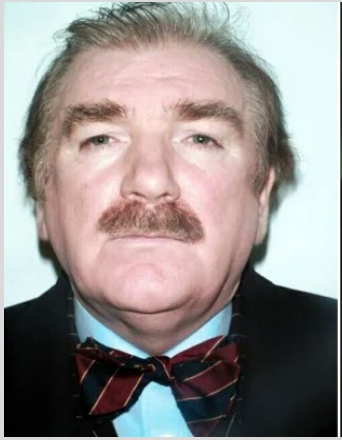
# SPEAKER QUALIFICATIONS

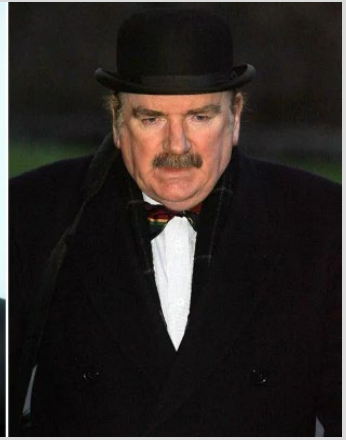
# SPEAKER QUALIFICATIONS


# SPEAKER QUALIFICATIONS

# SPEAKER QUALIFICATIONS

# PROFESSIONAL TRAINING
## SOUTHWARK CROWN COURT



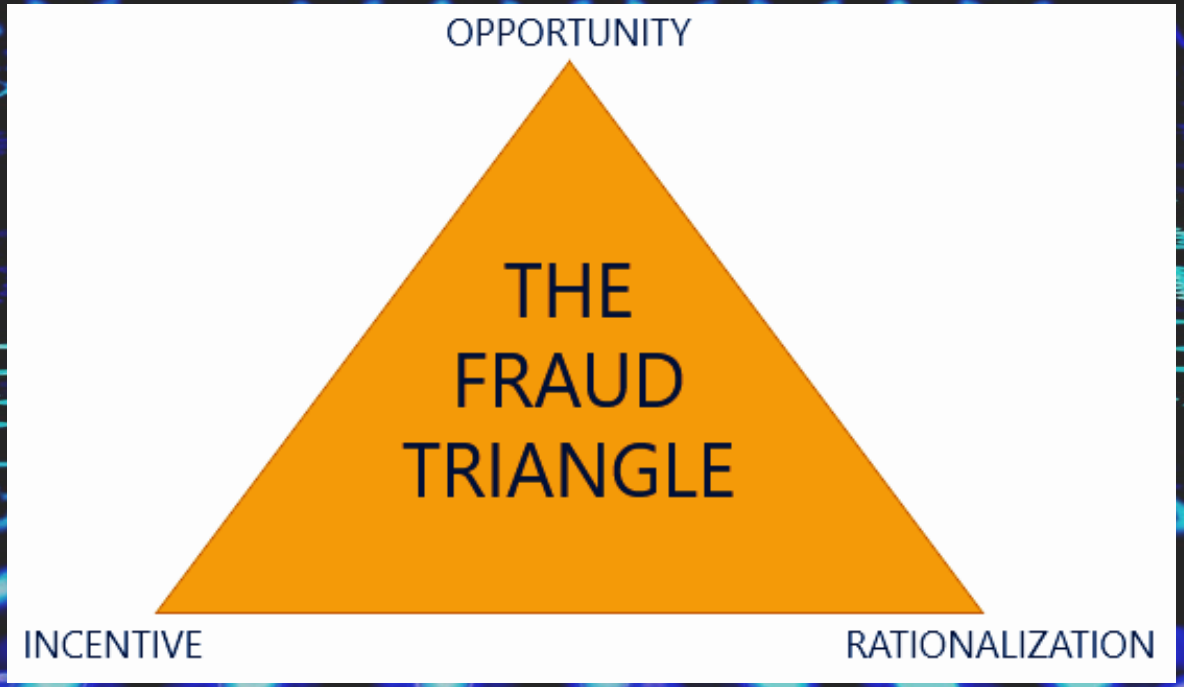


# HMP WANDSWORTH


# HMP WANDSWORTH

# HMP WANDSWORTH

# FRAUD MINDSET - TRADITIONAL



# OCN FRAUD MINDSET: PSYCHOPATHY SPECTRUM

| Interpersonal | Affective | Lifestyle | Antisocial |
|---|---|---|---|
| Superficial charm | Remorselessness | Impulsivity | Poor behavioural controls |
| Grandiosity | Callousness | Stimulation seeking | Delinquency |
| Lying | Failure to accept responsibility | Parasitic lifestyle | Criminal versatility |
| Cunning and manipulative | Promiscuous sexual behaviour | Lack of realistic goals | Early behavioural problems |

# ANATOMY OF A CYBER FRAUD

- Utilised social engineering techniques
- Target company
- Number spoofing
- Voice manipulation / mirroring

# ANATOMY OF A CYBER FRAUD

- Lay false trail (geolocation)
- “Suspend” gateway (suspicious emails / system lagging)
- Possibility of virus (seeds of doubt)

(Abandonment of historic techniques)

# ANATOMY OF A CYBER FRAUD

- Test session (inbound / outbound transactions “frozen”)
- Opportunity to opt-out (can visit branch with CPU / server unit).....a far more inconvenient alternative to opting-in
- Psychological pact to proceed

# ANATOMY OF A CYBER FRAUD

- Carefully log in **(do not divulge PINs / codes – further reinforcing banks' messaging)**
- 'Sync' with balances (last 4) - knowledge of values available to steal
- Acquire corresponding mules from the ML team (commercial / student)

# ANATOMY OF A CYBER FRAUD

- Inputting of data / generation of ‘random’ details / authorisation. Innocuous payment references. Are all fields filled (further social engineering)?
- Reverse / repeat
- **Counteracting the banks’ response (e.g. management of pop-ups / varying payment references…..“Fraud Check” / replacing tech after each job)**
- **Security PIN** (victim control)

# CASHING-OUT

- Manipulation / Embedding of Bank Tellers
- Creation of False Trust between Mule Accounts
- Traits of a Mule Account (Detection prior to a Fraud)

Application of the Criminal Mindset

# COLLABORATION (Police, Governments, Tech)

- Meta internally projected in 2025 that it would earn about 10% of its overall annual revenue – or $16 billion – from fraud
  (Reuters)

- Two-thirds (68%) of fraud originates on Meta platforms
  (Lloyds Banking Group)

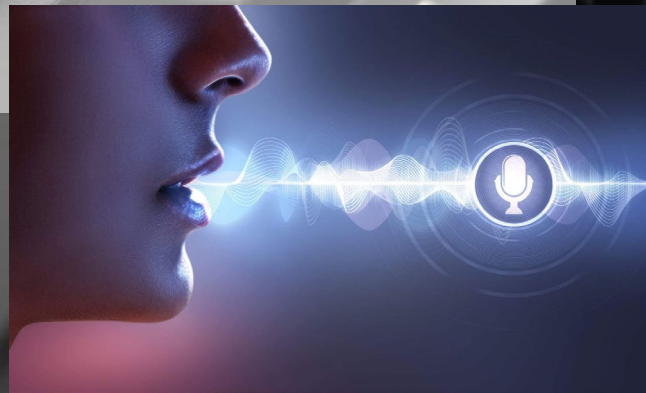
# GENERATIVE A.I.

*“Generative AI” refers to deep-learning models that can generate high-quality text, images, and other content based on the data they were trained on.*

IBM Research

# DEEP FAKE VOICE CLONING

- 3-minute voice sample (OpenAI - 15 secs)
- 99% accurate clone



# DEEP FAKE VOICE CLONING

www.fakeyou.com

www.resemble.ai

www.elevenlabs.io

www.voice.ai

# FRAUD AUTOMATION

Combining Generative AI / Chat GPT / Deep Fake:

- APP-style fraud can be automated from start to finish
- Zero-touch fraud
- Opportunity for one bad actor to commit multiple frauds simultaneously

# FRAUD AUTOMATION

# DEEPFAKE (recent examples)


# LIVE DEEPFAKE

# and

# RESPONSIVE AI

# KEY TAKEAWAYS

- FRAUD MINDSET
- SPEED OF PIVOT
  (vs Implementation Delay)
- RESILIENCE
- ZERO TRUST PRINCIPLES

KEYNOTE

# Lücken schliessen: Die vollständige Wertschöpfungskette der Betrugsbekämpfung im Schweizer Zahlungsverkehr

**Elisa-Sophie Eikevaag**
Head Multi Rail Fraud Prevention, SIX

**Stefan Giger**
Head Payment Fraud & Dispute Services, SIX

BETRUGSBEKÄMPFUNG

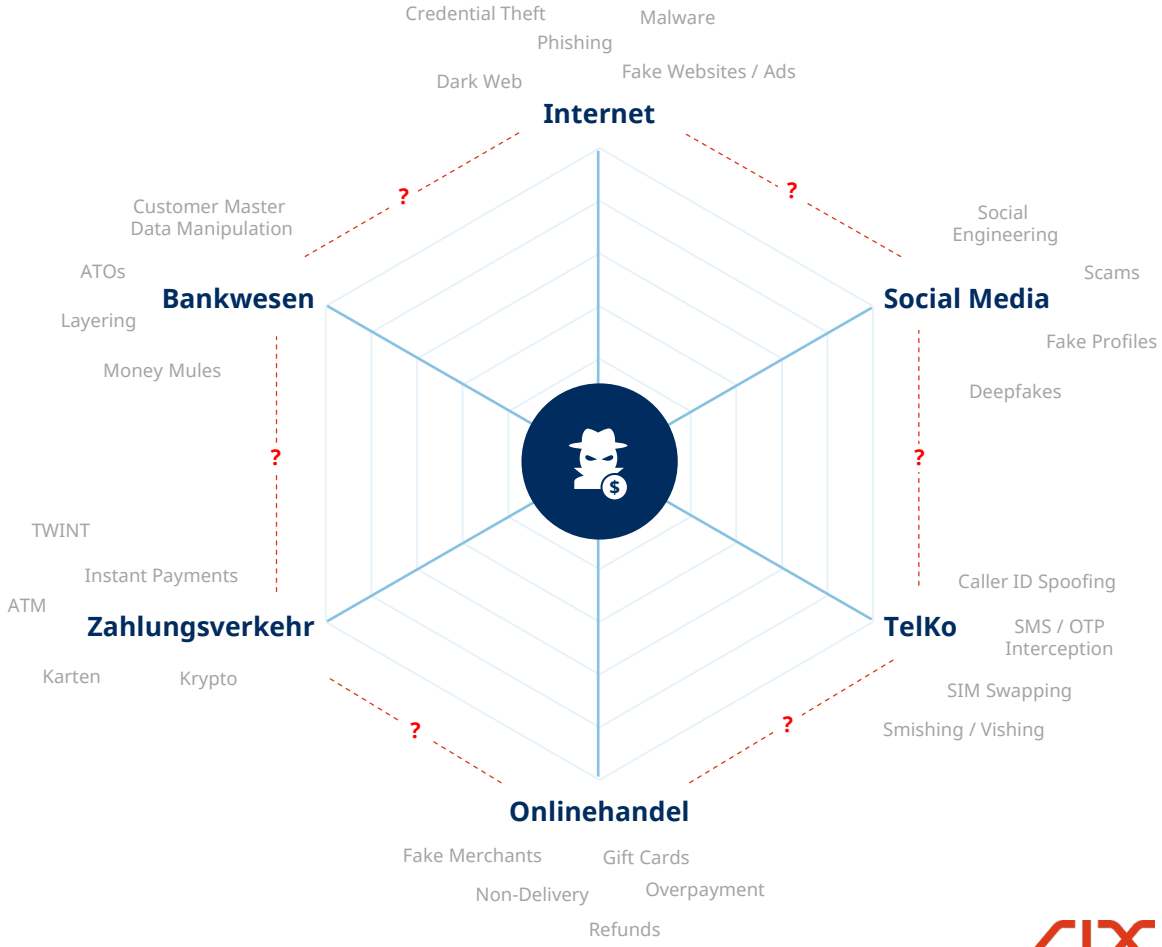
# ist vor allem ein Visibilitäts-problem

- **Der Betrüger**

  Sieht alle Bausteine – und verbindet sie frei zu einer durchgehenden Journey durch das gesamte Ökosystem.

- **? Die Abwehr**

  Sieht jeweils nur den eigenen Ausschnitt und meistens erst, wenn der Betrug bereits angekommen ist.



# 20 Jahre Lernen aus Betrugsfällen bei Debitkarten

*Vor dem Betrug* | *Während des Betrugs* | *Nach dem Betrug*

**01 Prevention**
Kunden über Fraud aufklären, Kontroll-systeme etablieren

**02 Detection**
Transaktion sowie kontextuelle Daten analysieren

**03 Decision**
Fraud Alerts einordnen, priorisieren und eskalieren

**04 Response**
Sperren von Trx und Konto, Abklärung mit dem Kunden

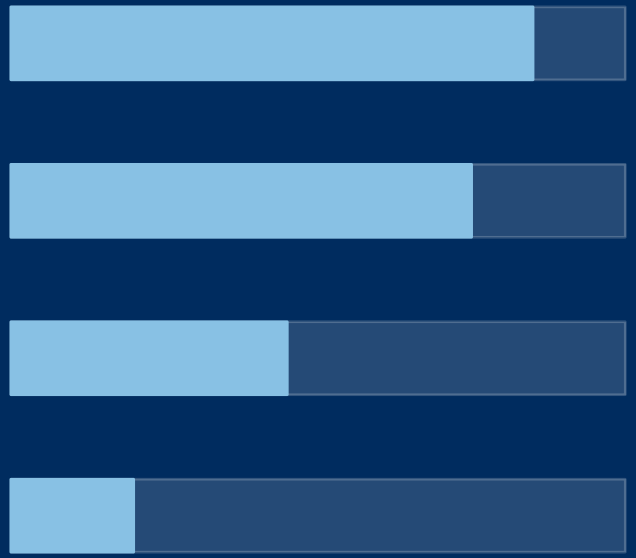
**05 Recovery**
Fall analysieren, Rückvergütung an Kunden prüfen

**06 Learning**
Anpassung von Kontrollsystemen, Fraud Reporting

Viele Finanzinstitute setzen primär auf Detection – aber die Lösung für erfolgreiche Betrugsbekämpfung ist kein einzelnes Tool, sondern das Zusammenspiel der gesamten Kette.

ERSTE LÜCKE

# Unterschiede in der Fraud-Maturität verschiedener Zahlungsnetzwerke



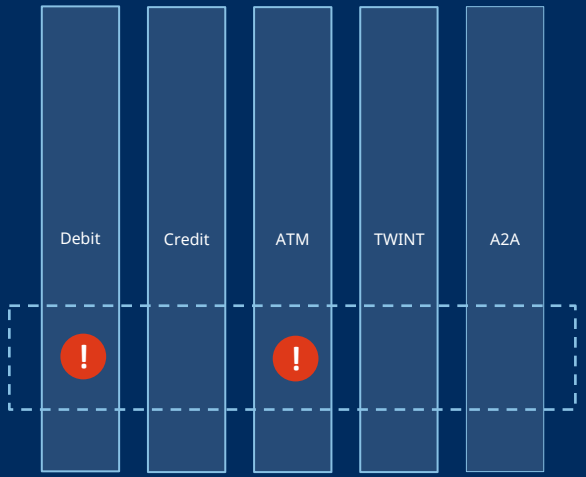
# Nicht alle Schweizer Zahlungsnetzwerke sind gleich weit

| MATURITÄT IN: | Karten | TWINT | Kontobasierter Zahlungsverkehr |
|---|---|---|---|
| **Fraud Intelligence** | Stark fortgeschritten | Mittel | Mittel |
| **Transaction Monitoring & Risk Scoring** | Stark fortgeschritten | Tief | Fortgeschritten |
| **Scheme Scores (Netzwerkdaten)** | Stark fortgeschritten | Mittel | Mittel |
| **Kunden- & Zahlungsauthentifizierung** | Stark fortgeschritten | Tief | Fortgeschritten |
| **Case Management & Kundensupport** | Stark fortgeschritten | Mittel | Mittel |
| **System für Dispute & Chargeback** | Stark fortgeschritten | Tief | Tief |

Diese Einschätzung basiert auf Marktbeobachtungen, Kundeninterviews und -umfragen sowie der operativen Erfahrung von SIX.

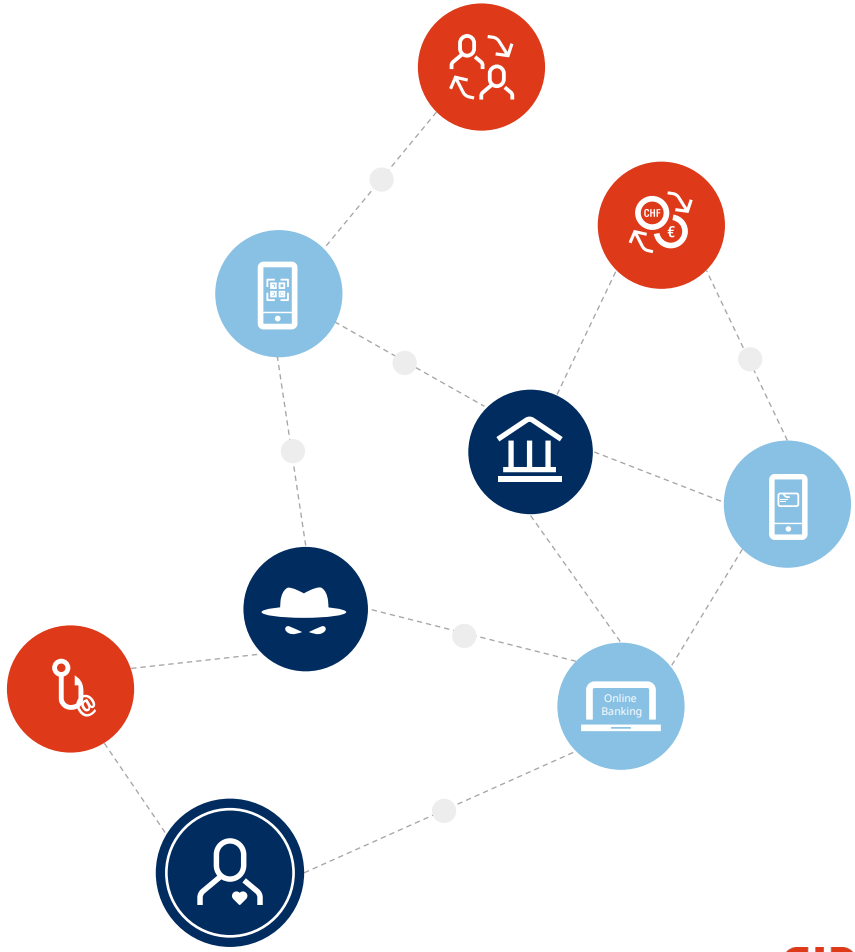
ZWEITE LÜCKE

# Isolierte, rail-spezifische Fraud-Systeme schaffen blinde Flecken

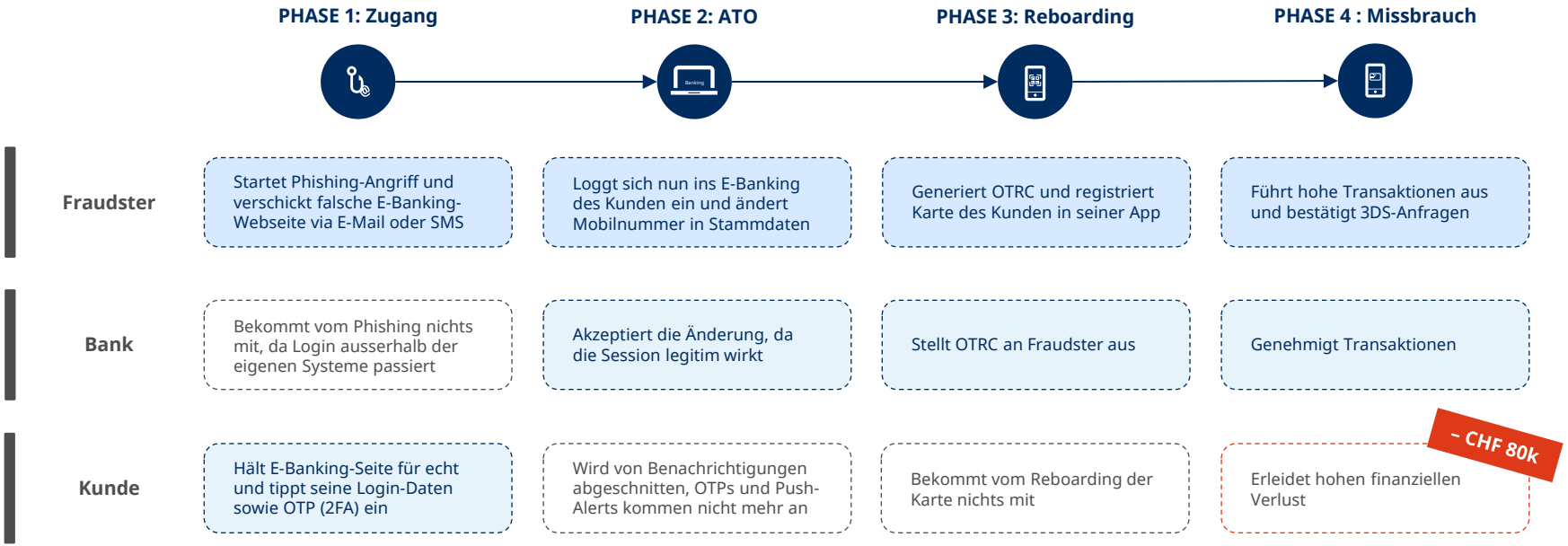


# Multi-Rail Fraud

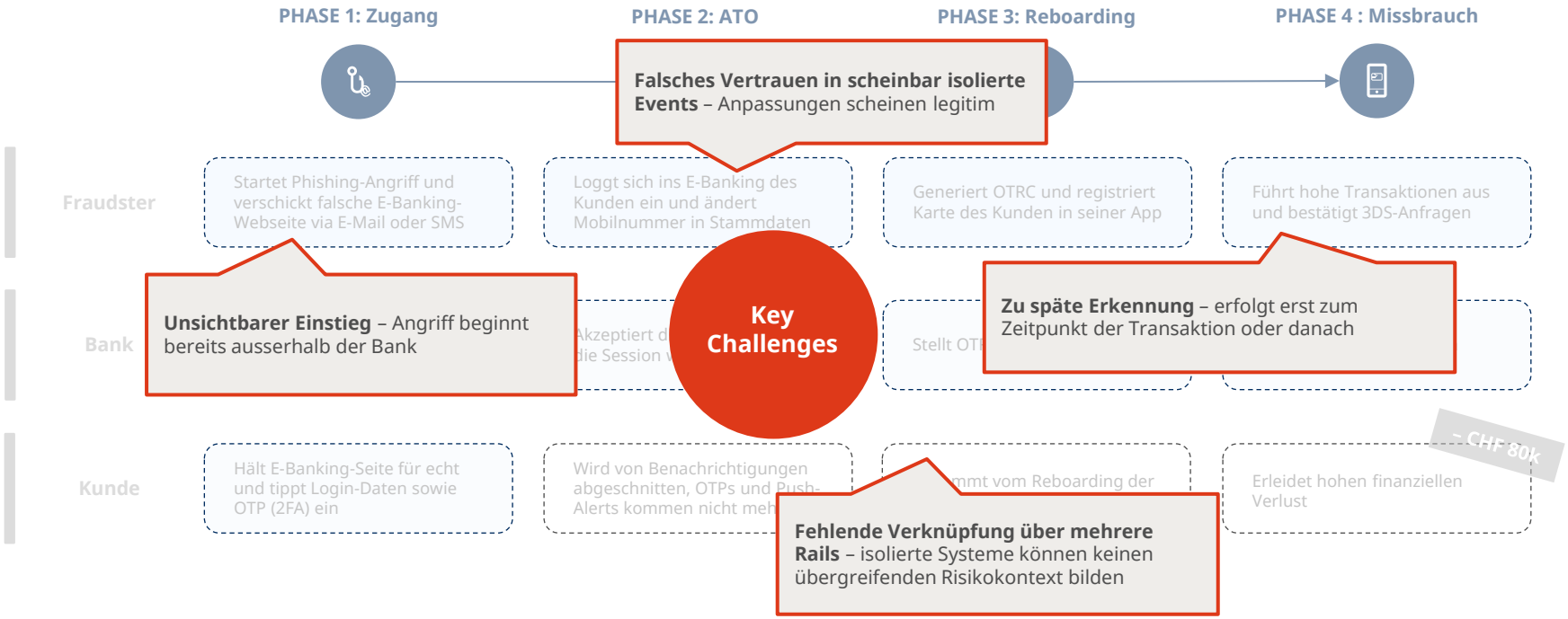
Wie verteidigt man sich, wenn Karte, TWINT oder E-Banking Teil desselben Angriffs sind?



# Wo konventionelle Kontrollmechanismen scheitern – ein aktueller Fall



# Wo konventionelle Kontrollmechanismen scheitern – zentrale Herausforderungen



# Von transaktions- zu kundenzentrierter Betrugsbekämpfung

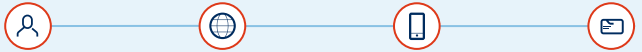
**BISHERIGER ANSATZ**

## Einzelne Transaktionsanalyse

- Einzelne Transaktionen werden überprüft
- Signale werden isoliert bewertet
- Entscheidung erfolgt punktuell

**NEUER ANSATZ**

## Kontinuierliche Analyse des Nutzerverhaltens



- Verhalten wird analysiert – nicht nur einzelne Events
- Signale werden entlang der gesamten Journey verknüpft
- Entscheidungen erfolgen kontinuierlich – vor, während und nach der Transaktion

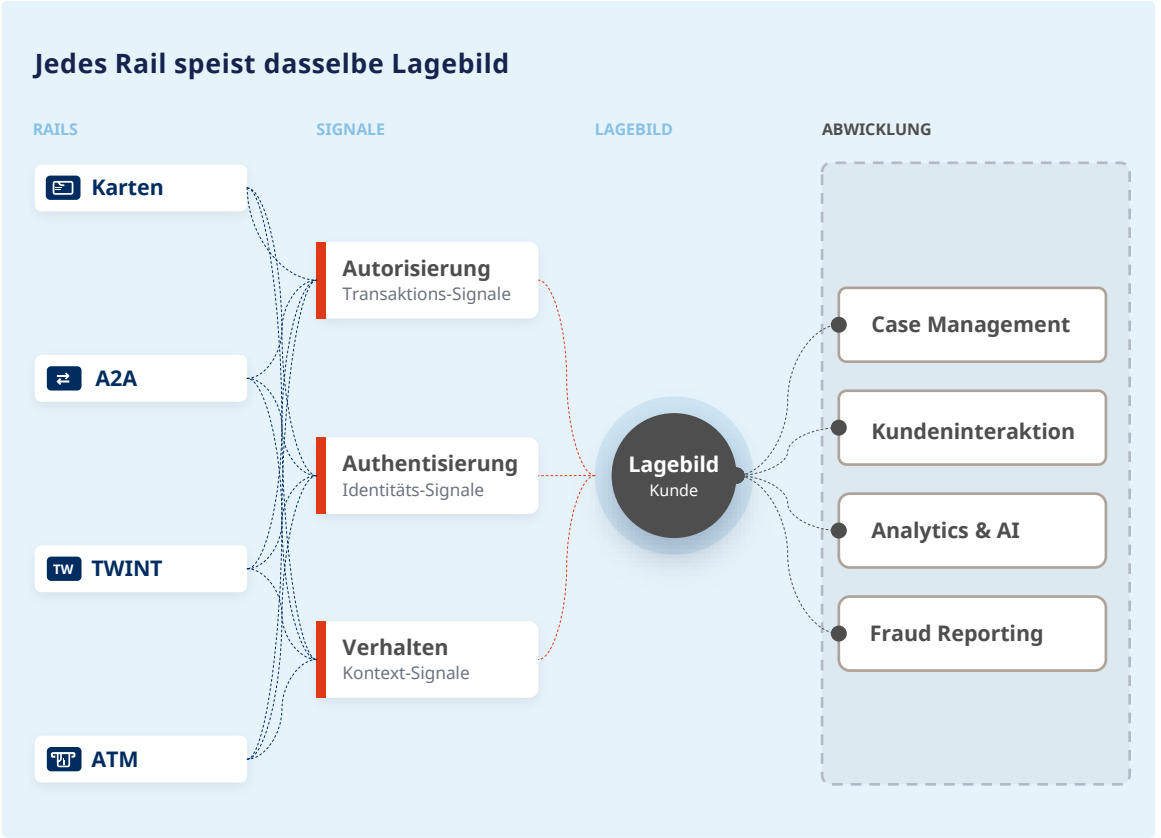
**Paradigmenwechsel**: Moderne Betrugsprävention fragt nicht mehr «*Soll ich diese Transaktion genehmigen?*» – sondern «*Vertraue ich dem Verhaltensmuster, das zu dieser Transaktion geführt hat?*»

Multi-Rail ist

# keine Technologie.

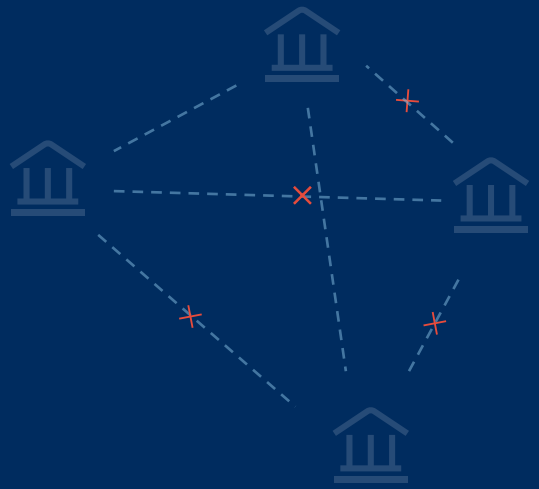
Es ist die Fähigkeit, Signale zu einem **gesamtheitlichen Lagebild** zusammenzuführen.

- Verbindet Signale aus Autorisierung, Authentifizierung und Verhalten zu einem übergreifenden Kundenbild
- Erkennt Betrugsmuster über alle Rails
- Bietet konsistente, zentralisierte Ressourcen und Kanäle für Case Management, Kundeninteraktion, Analytics & AI und Fraud Reporting



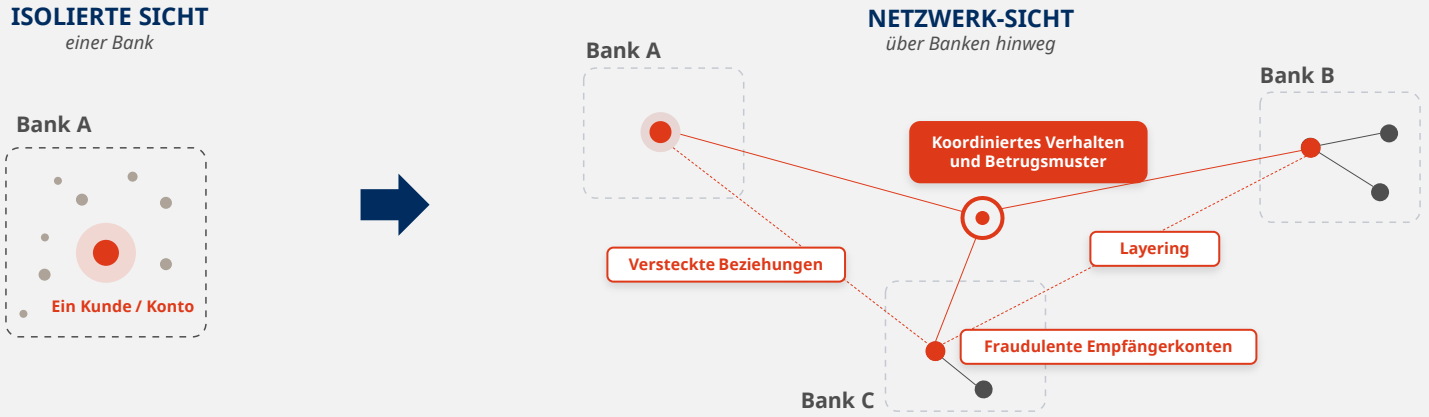
DRITTE LÜCKE

# Banken sehen nur ihre eigenen und keine netzwerk-weiten Daten



# Eine Bank sieht ihre Kunden, das Netzwerk sieht den Angriff

Netzwerkdaten decken auf, was allein unsichtbar bleibt – und bieten zusätzliche Risikosignale:




**Kartenwelt** — Etabliert

**Visa/Mastercard Scheme Scores**

**TWINT** — Im Aufbau

**TWINT Fraud Score**

**Swiss Interbank Clearing** — In Analyse

**Network-Level Risk Indicators NLRI**

# Schliessen der drei zentralen Lücken in der Betrugserkennung

LÜCKE 1

**Rail**

Unterschiedliche Maturität der Rails

WENN GESCHLOSSEN

**Einheitliche Risikoerkennung über alle Zahlungskanäle hinweg**

LÜCKE 2

**Multi-Rail**

Rails sehen nur ihren Ausschnitt

WENN GESCHLOSSEN

**Sichtbarkeit von kanalübergreifenden Betrugsmustern**

LÜCKE 3

**Netzwerk**

Banken sehen nur ihre eigenen Daten

WENN GESCHLOSSEN

**Systemischer Blick auf Betrugsmuster und -netzwerke**

# Betrug wird nicht verschwinden.

Entscheidend wird sein, ob und wie wir **gemeinsam** dagegen vorgehen.

PANEL

# Fraud im Schweizer Zahlungsverkehr – Einblicke und Erfahrungen führender Finanzinstitute

**Manuela Inauen**
Leiterin Produktmanagement, SGKB

**Max Piehl**
Fraud Initiative Lead, UBS

**Romano Ramanti**
Vizedirektor, Certified Ethical Hacker, ZKB

KEYNOTE

# Gemeinsam stärker: Die Zukunft der Betrugsbekämpfung braucht Netzwerkeffekte

**Elisa-Sophie Eikevaag** · Head Multi Rail Fraud Prevention · SIX

# Immer mehr und neue Betrugsmaschen in der Schweiz

Blick

Festnahmen in Steinhausen ZG

## Zuger Polizei warnt vor «Lost Traveller»-Betrugsmasche

**Zwei Iren sind in Steinhausen ZG wegen des Verdachts auf Betrug verhaftet worden. Sie sollen mit der «Lost Traveller Scam»-Masche junge Menschen getäuscht und Bargeld erbeutet haben.**

SRF

Zahlreiche Hausdurchsuchungen

## Zehn Verhaftungen nach internationalem Betrug in der Schweiz

- Verschiedene Schweizer Polizeikorps haben in mehreren Kantonen zehn Männer festgenommen.
- Den Beschuldigten werden «Romance Scam» und schwere Geldwäscherei vorgeworfen.
- Unter der Leitung der Staatsanwaltschaft des Kantons Zürich wurden in den frühen Morgenstunden zeitgleich zahlreiche Hausdurchsuchungen durchgeführt.

TA

## Über 200'000 Franken: Schweizerin verliert ganzes Erbe ihres Vaters an Fake-Tinder-Date

Mehr als eine halbe Milliarde Franken haben professionell agierende Betrüger Schweizerinnen und Schweizern seit 2022 abgenommen. Die Behörden sind meist machtlos.

watson

## Wasserglas-Trick: So dreist gehen Betrüger in der Schweiz vor

**Sie geben sich am Telefon als falscher Polizist, im Internet als Märchenprinz oder vor der Haustür als durstige Mitmenschen aus – Trickbetrüger. Ihre Maschen sind fies. Jährlich fallen zahlreiche Schweizer und Schweizerinnen den Betrügern zum Opfer – auch im Kanton Zürich. Das sind die neuesten Tricks.**

20 Minuten

«CALLBACK-SCAM»

## Neue Betrugsmasche – rufe bei diesen Nachrichten nicht zurück

Dem Bundesamt für Cybersicherheit wurden in der vergangenen Woche vermehrt Fälle einer neuen Betrugsmasche gemeldet. Dabei wird das Opfer zu einem Rückruf verleitet.

watson

## Jeder siebte Schweizer hat bei Cyberbetrug Geld verloren – darunter viele Junge

Beobachter

## 170'000 Franken weg – wegen «wertvollen» Büchern?

Ein Ehepaar aus der Nordwestschweiz wird über Jahre systematisch betrogen: Vertreter verkaufen ihnen «wertvolle» Faksimiles als Geldanlage.

Blick

Falscher Bankanruf, echte Gefahr

## Raiffeisen warnt vor dreistem Geld-weg-Betrug

**Ein Aargauer erhielt einen Anruf von angeblichen Raiffeisen-Mitarbeitern. Betrüger versuchten, an die Bankdaten zu kommen, indem sie eine falsche Abbuchung vortäuschten – Raiffeisen warnt.**

# Das internationale Ausmass von Fraud in Zahlen

**€ 6,2 Mrd.**

Verluste durch Zahlungsbetrug in der EU und GB im Jahr 2024

**+17 % YoY**

Wachstum alleine in der EU
+16 % bei Banktransfers
+29 % bei Kartenzahlungen

**7 von 10**

betrügerische Banktransfers basieren auf Manipulation des Kontoinhabers

**59 %**

der APP-Fraud-Schäden mussten britische Banken ihren Kunden zurückerstatten

*Quellen: EBA 2025 Report on Payment Fraud, UK Annual Fraud Report 2025*

# Weltweit entstehen zentrale Lösungen und strengere Regulierung, um Betrug systematisch zu bekämpfen

## Zentrale Marktlösungen

Gemeinsame Plattformen und zentrale Services bündeln Daten aller Teilnehmer und schaffen mehr Transparenz über Betrugsrisiken innerhalb des gesamten Netzwerks.

**Verbesserte Risikobewertung**

durch netzwerkweite Erkenntnisse und Risikosignale

**Datenaustausch in Form von**

Empfängerprüfung, Validierungslisten bis hin zu voll-umfänglichem Echtzeit-IBAN- und Transaktions-Risk-Scoring

**Internationale Beispiele**

- Mastercard **VocaLink**
- Iberpay **Payguard**
- EBA Clearing **FPAD**

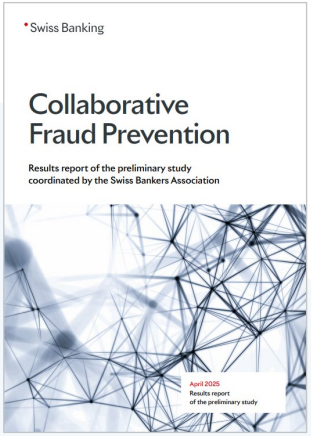
## Regulatorisch getriebene Lösungen

Regulierungsbehörden verschärfen die Betrugsbekämpfung durch verbindliche Präventionsmassnahmen für Zahlungs-dienstleister und neue gesetzliche Anforderungen.

- EU UK AU **Confirmation/Verification of Payee**
- UK PT **Neue Entschädigungs-Regelungen**
- SG **Kontrolle über Bankkonten**

# Swiss Banking: «It Takes a Network to Beat a Network»

2025: Vorstudie **Collaborative Fraud Prevention** der SBVg




### Mission / Zielsetzung

Das abstrakte Interesse verschiedener Stakeholder an kollaborativer Betrugsprävention in eine engagierte **«Koalition der Willigen»** mit einem konkreten, priorisierten und abgestimmten Aktionsplan überführen.

**Teilnehmer:** diverse Schweizer Banken, SIX

**Gemeinsame Sensibilisierungs-kampagnen**

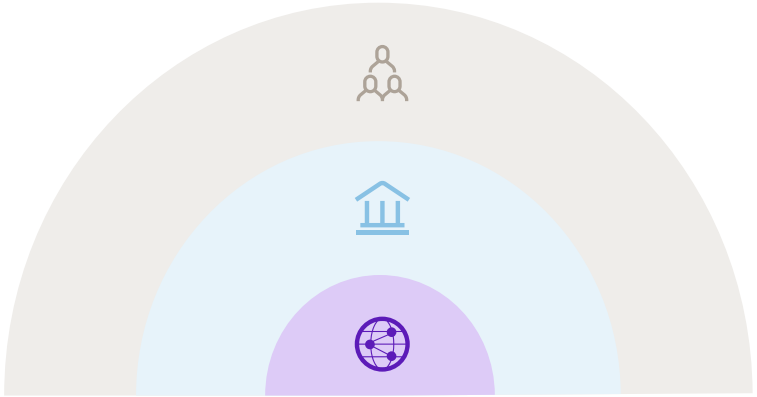
**Produkt- und branchenübergreifender Austausch**

**«Network-Level Risk Indicators» Service (NLRI)**

Laufende Machbarkeits-studie von SIC

*Quelle: Results report of the preliminary study - Collaborative Fraud Prevention.pdf, Swiss Banking, 2025*

# Vorteile eines NLRI-Services für den Schweizer Zahlungsverkehr



Endkunden
Finanzinstitute
Zahlungsverkehr

>

## Vorteile für Endkunden

- Stärkung der Resilienz des Zahlungssystems, insbesondere bei Echtzeitzahlungen
- Erhöhung der Sicherheit durch frühzeitige (Echtzeit-)Erkennung verdächtiger Zahlungen

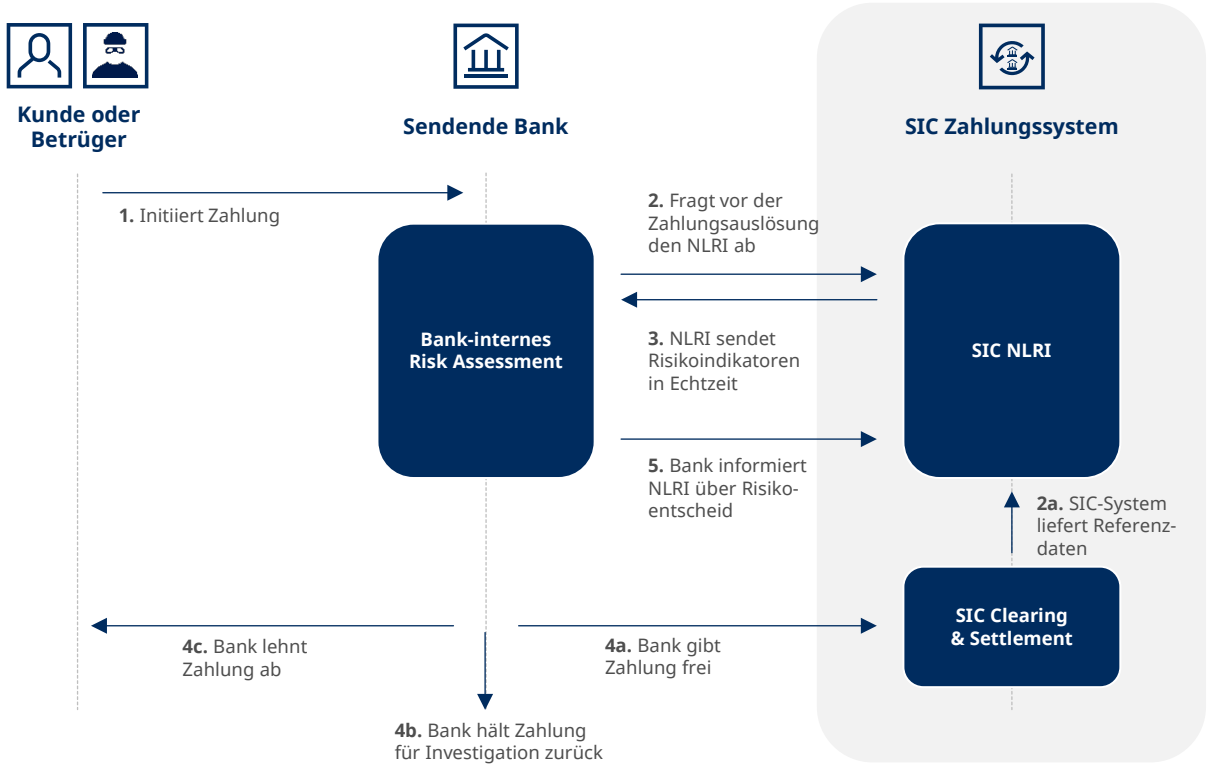
## Vorteile für Finanzinstitute

- Steigerung von Effizienz und Effektivität durch Nutzung netzwerkweiter Daten
- Aufrechterhaltung der Reputation durch Reduktion von Betrugsverlusten

## Vorteile für den Zahlungsverkehr

- Förderung von Innovation, Zusammenarbeit und Informationsaustausch
- Verfolgung eines proaktiven, markt-getriebenen Ansatzes (statt Regulation)

# Wie der NLRI-Service funktioniert – Ein Überblick




**Beschreibung**

Der **NLRI-Service** liefert eine **Echtzeitbewertung von Betrugsrisiken** für Zahlungen im SIC-System und integriert sich nahtlos in den Zahlungs-prozess.

Banken übermitteln dabei Transaktionsdaten an den Service und erhalten in Echtzeit verschiedene Risikoindikatoren zurück. Diese Netzwerksignale ergänzen die internen Risiko-bewertungen der Banken und unterstützen die Entscheidung, Zahlungen zu verarbeiten, zurückzustellen oder abzulehnen.

Die Ergebnisse der finalen Risikobewertung werden an den NLRI zurückgemeldet, um die Servicequalität kontinuierlich zu verbessern.

# Der NLRI fokussiert initial auf Risikosignale für kontobasierte Transaktionen in der Schweiz

| DIMENSION | ✓ **Was der NLRI ist** (initialer Fokus) | ✗ **Was der NLRI nicht ist** |
|---|---|---|
| **Geographischer Scope** | Schweiz | Grenzüberschreitend |
| **Zahlungen in Scope** | Kontobasierte Zahlungen (RTGS und IP) | Kartenzahlungen, TWINT |
| **Input-Daten** | Transaktionsdaten, Fraud Risk Reporting | Kundendaten (z. B. IP-Adresse, Nutzungsdaten) |
| **Fraud Risk Reporting** | Empfangendes Konto ist nicht bei der anfragenden Bank | Sender- und Empfängerkonto bei derselben Bank |
| **Output** | Risikoindikatoren (z. B. Score 0–100) | IBAN Whitelist oder Blacklist |

# Risikoindikatoren nutzen regelbasierte Logik sowie Machine-Learning-Datenmodelle

### 01 Regelbasierte Indikatoren

- Fünf Indikatoren initial priorisiert – z. B. das **Alter einer IBAN**
- Kontinuierliche Weiterentwicklung ist vorgesehen

+

### 02 Machine-Learning-Indikator

- Statistische Wahrscheinlichkeit von **Anomalien** (potenzieller Betrug)
- Basierend auf beobachteten Daten

ERGEBNIS

**NLRI-Risikoindikatoren**

Netzwerkbasierte Signale aus Kontobeziehungen & -verhalten, kombinieren regelbasierte Logik mit statistischen ML-Mustern.

## MEHRWERT FÜR BANKEN

### 1 Mehr Transparenz

Klare Sicht auf Kontobeziehungen und Transaktionsverhalten im Netzwerk.

### 2 Frühe Erkennung

Banken erkennen betrügerische Zahlungen frühzeitig anhand der NLRI-Ergebnisse.

### 3 Kontinuierliche Verbesserung

Feedback zum Betrugsrisiko verbessert die Genauigkeit des NLRI kontinuierlich.

# Indikativer Zeitplan 2026 bis 2028

## 2026
**KONZEPT & RAHMEN**

- Ausarbeitung des detaillierten Servicekonzepts
- Klärung der rechtlichen Rahmenparameter
- Definition der Governance

## 2027
**UMSETZUNG & INTEGRATION**

- Technische Umsetzung des NLRI
- Fachliche und technische Integrationsanalyse
- Schaffung der vertraglichen Grundlagen

## 2028
**GO-LIVE**

- Entwicklung und Training der Fraud-Modelle
- Kalibrierung der Indikatoren
- Go-live NLRI

# NLRI

## Vom Netzwerkgedanken zum gemeinsamen Handeln

Schaffen Sie in Ihrer Bank das Bewusstsein für den Wert dieser Initiative und gewinnen Sie frühzeitig die Unterstützung entscheidender Stakeholder.

KEYNOTE

# Was die Daten nicht sehen – Der menschliche Faktor hinter dem Betrug

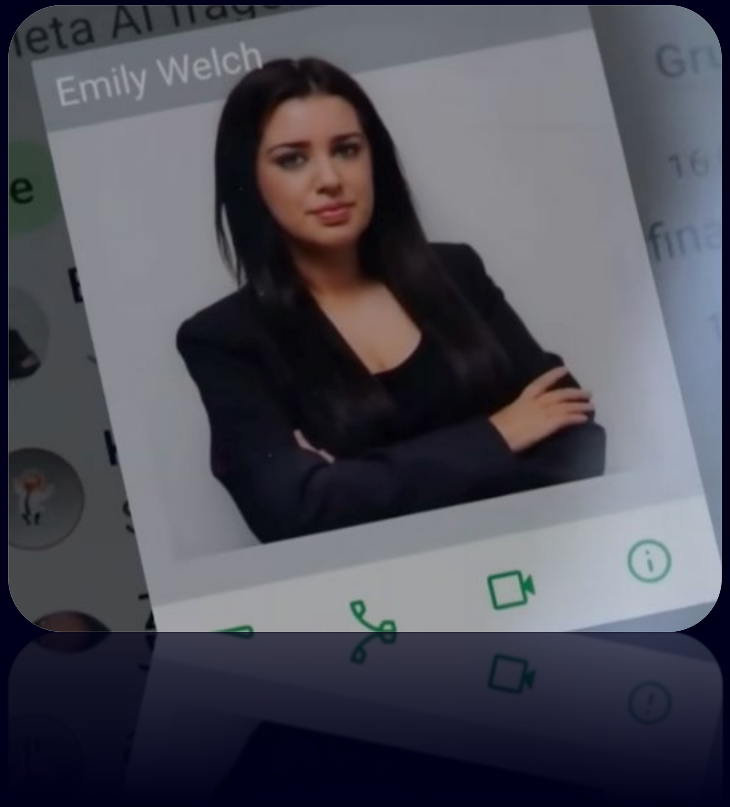
**Jill Wick** · Wirtschaftspsychologin & Cyber Security Awareness Consultant · Jill Wick GmbH

# Jill Wick

- Betrugsanalyse
- Wirtschaftspsychologin
- Security Awareness Consultant

# Max

# Lernt Emily kennen

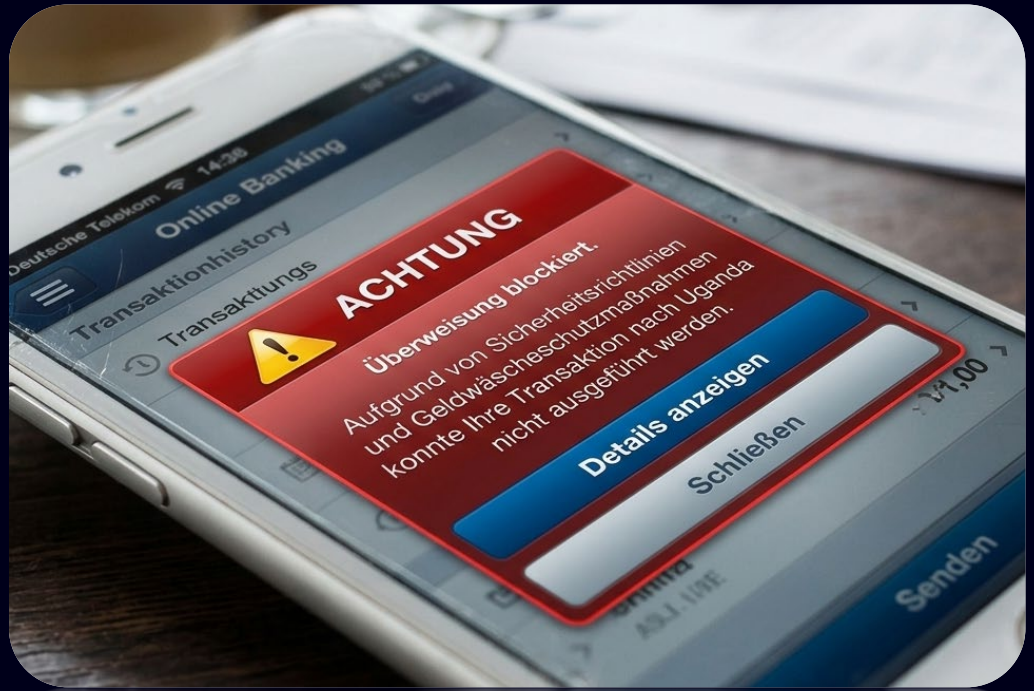


# Sie ist “Brokerin”

**Max prüft nach…**

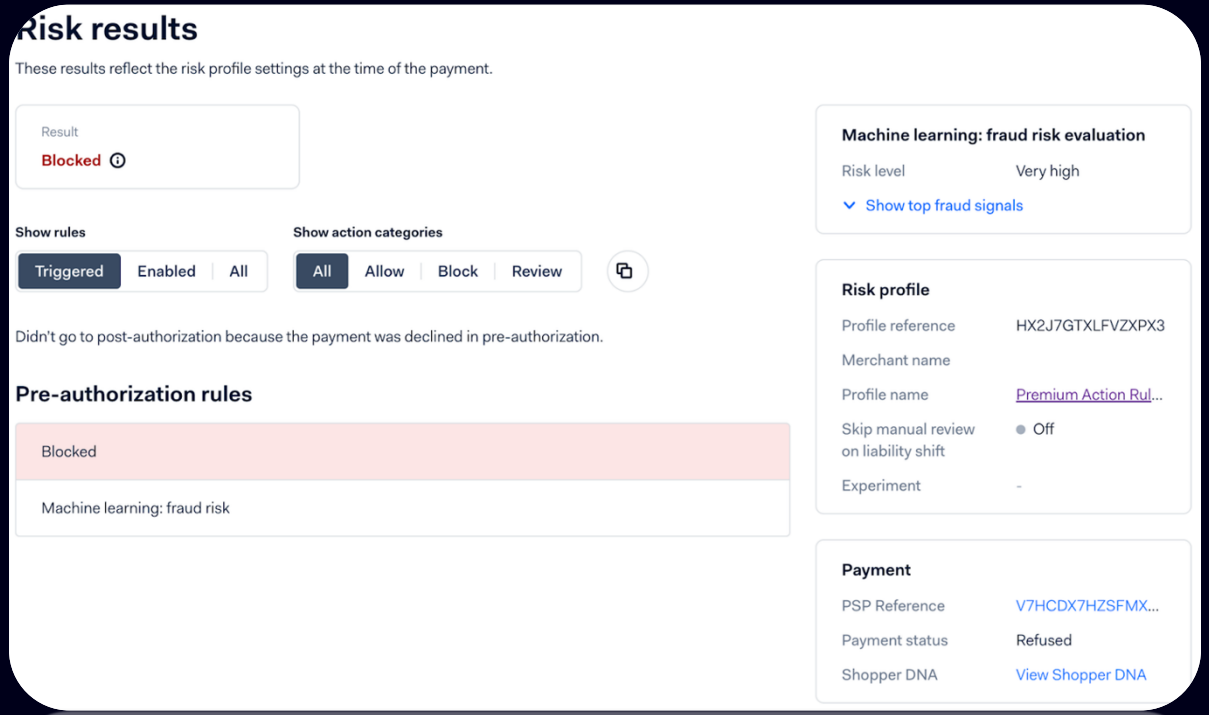
- **Fragt nach ihrer ID**
- **Facetimed mit ihr**

# Er überweist Geld

# Bank blockiert...

Sehr geehrte(r) Kunde/ Kundin, eine verdächtige Transaktion wurde blockiert. Bei Zweifel kontaktieren Sie bitte die Notrufzentrale: +4113950657901



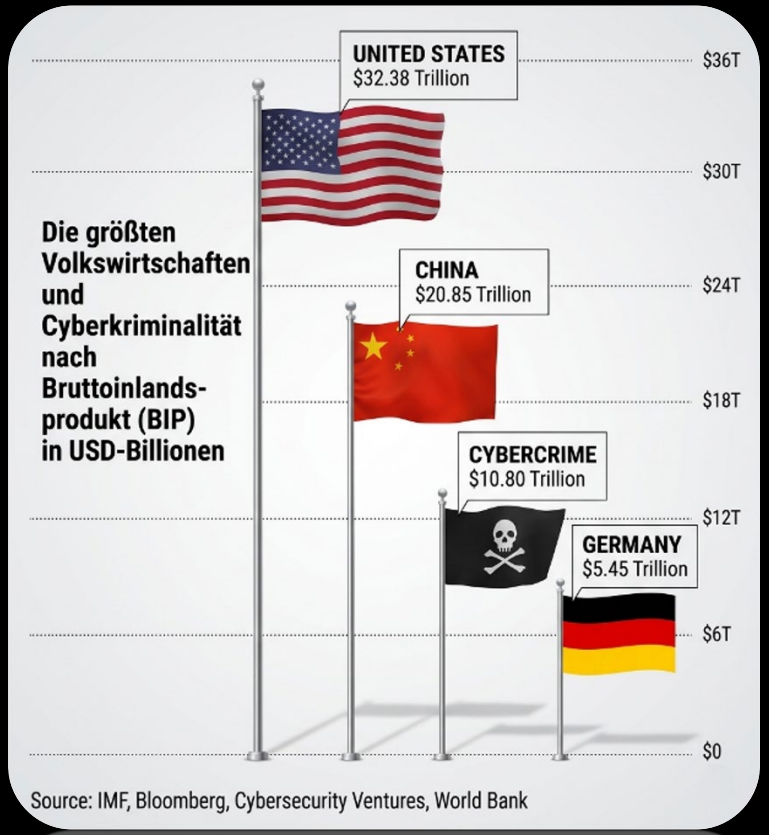
# Max übersteuert...

| | |
|---|---|
| westernU.<br>04. Feb. | -4,329.00 |
| westernU.<br>04. Feb. | -4,492.00 |
| westernU.<br>04. Feb. | -4,493.00 |
| westernU.<br>04. Feb. | -4,494.00 |
| westernU.<br>04. Feb. | -4,496.00 |
| westernU.<br>04. Feb. | -4,497.00 |
| westernU.<br>04. Feb. | -4,498.00 |
| westernU.<br>04. Feb. | -4,499.00 |

# Cybersicherheit ist ein immer wichtigeres Thema…

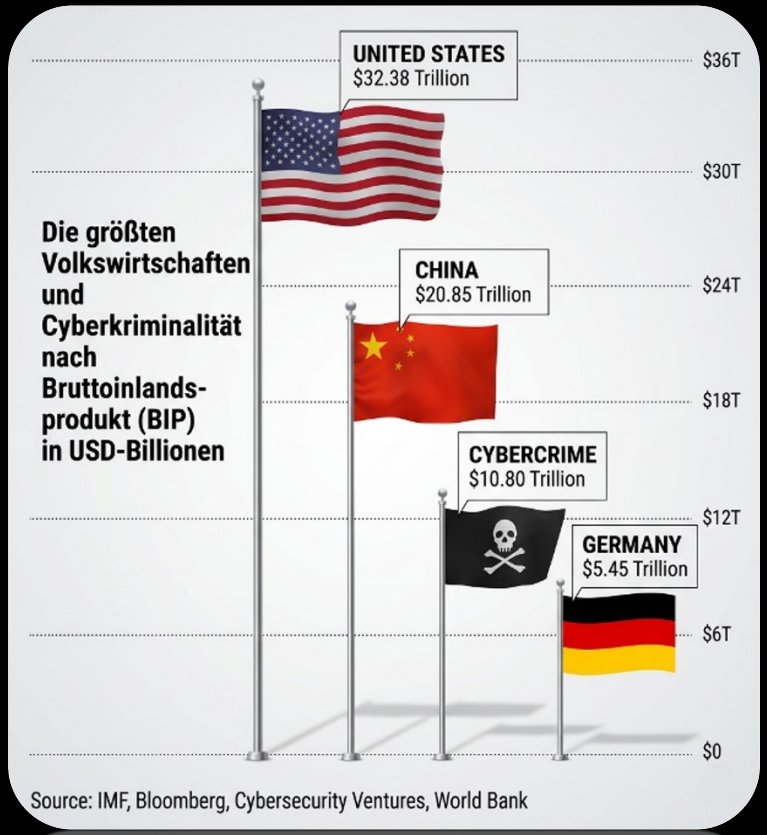
# Cybercrime ist die drittgrösste „Wirtschaft" der Welt.

*Quellen: IMF, Bloomberg, Cybersecurity Ventures*



# Sie lebt davon, dass Opfer schweigen.

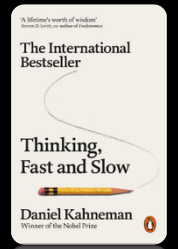
*Quellen: IMF, Bloomberg, Cybersecurity Ventures*



Cybersicherheit ist ein immer wichtigeres Thema…

**… und die Psychologie spielt dabei eine grosse Rolle!**

# Wir haben ein begrenztes Arbeitsgedächtnis:



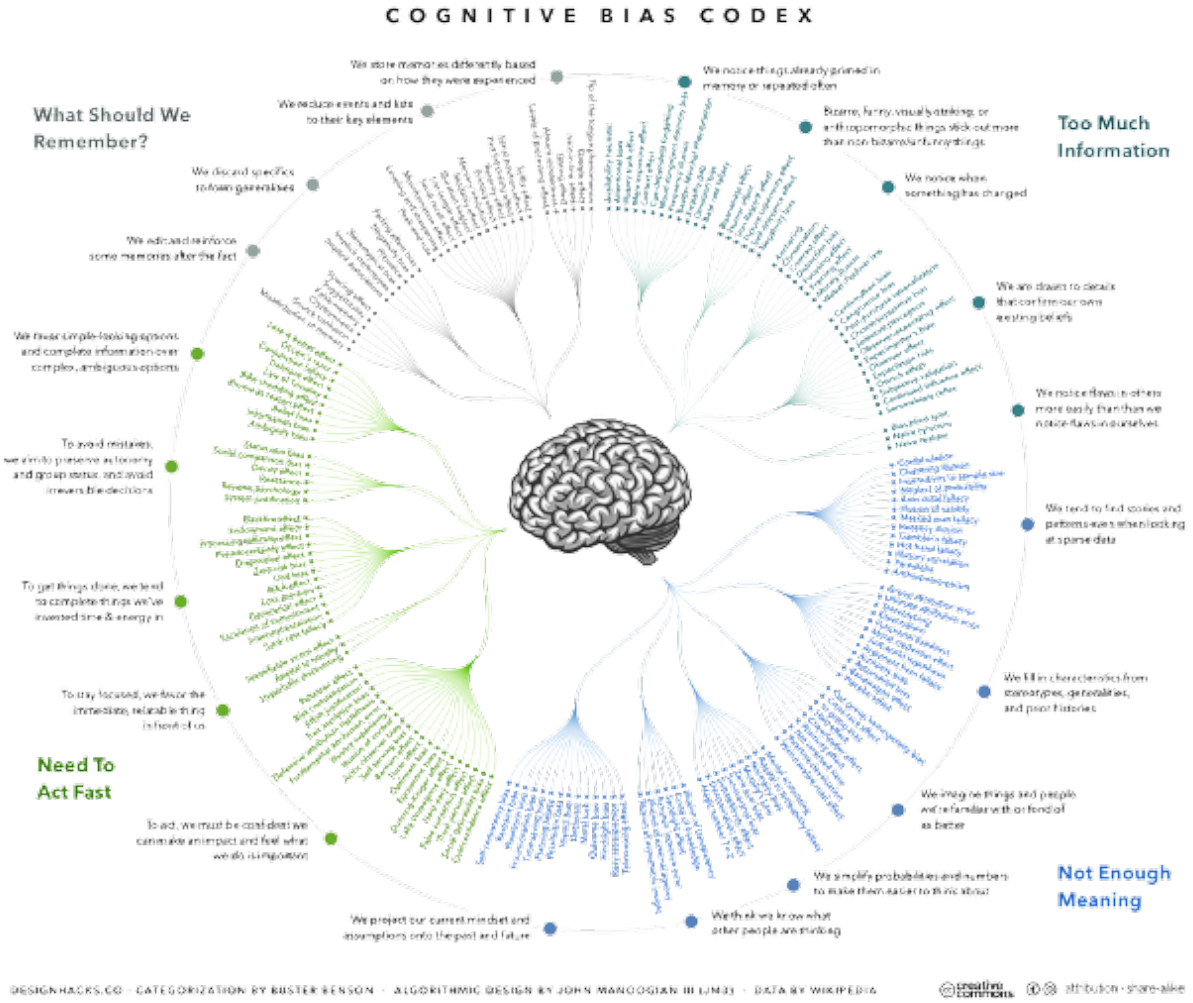

## 🐇 System 1

Schnell · intuitiv · automatisch

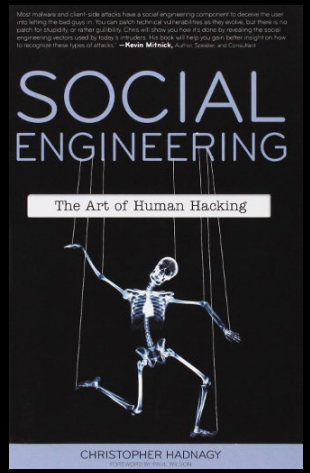
## 🐢 System 2

Langsam · rational · durchdacht

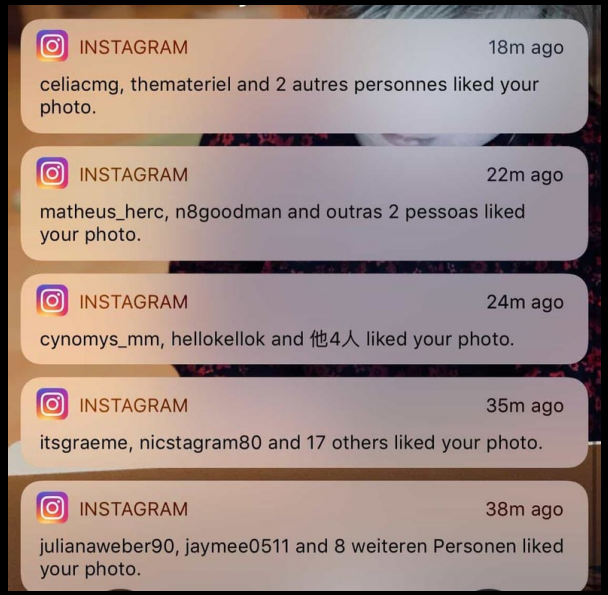
# Heuristisches Denken ist meistens hilfreich. Aber ist anfällig für Biases.

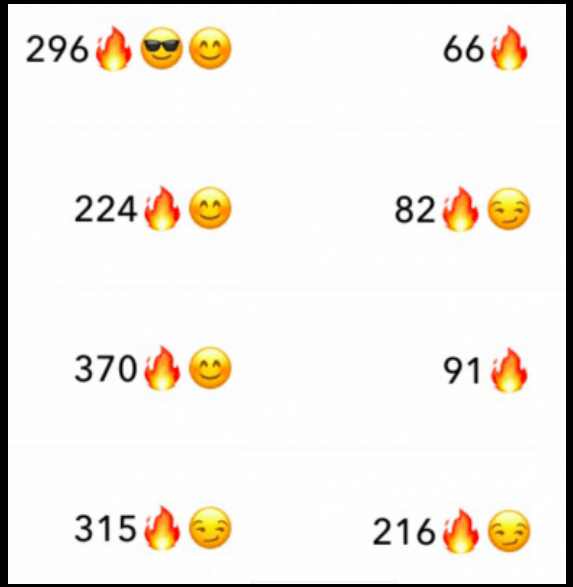

COGNITIVE BIAS CODEX
What Should We Remember?
We store memories differently based on how they were experienced
We reduce events and lists to their key elements
We discard specifics to form generalizes
We edit and reinforce some memories after the fact
We favor simple-looking options and complete information over complex, ambiguous options
To avoid mistakes, we aim to preserve autonomy and group status, and avoid irreversible decisions
To get things done, we tend to complete things we've invested time & energy in
To stay focused, we favor the immediate, relatable thing in front of us
Need To Act Fast
To act, we must be confident we can make an impact and feel what we do is important
We project our current mindset and assumptions onto the past and future
We think we know what other people are thinking
We simplify probabilities and numbers to make them easier to think about
We imagine things and people we're familiar with or fond of as better
We fill in characteristics from stereotypes, generalities, and past histories
We tend to find stories and patterns even when looking at sparse data
We notice flaws in others more easily than we notice flaws in ourselves
We are drawn to details that confirm our own existing beliefs
We notice when something has changed
Bizarre, funny, visually striking, or anthropomorphic things stick out more than non-bizarre/unfunny things
We notice things already primed in memory or repeated often
Too Much Information
Not Enough Meaning
DESIGNHACKS.CO · CATEGORIZATION BY BUSTER BENSON · ALGORITHMIC DESIGN BY JOHN MANOOGIAN III (JM3) · DATA BY WIKIPEDIA
creative commons attribution · share-alike

**„Social Engineering bezeichnet jede Handlung, die eine Person dazu bewegt, eine Massnahme zu ergreifen, die möglicherweise in ihrem besten Interesse liegt, *oder auch nicht.*"**

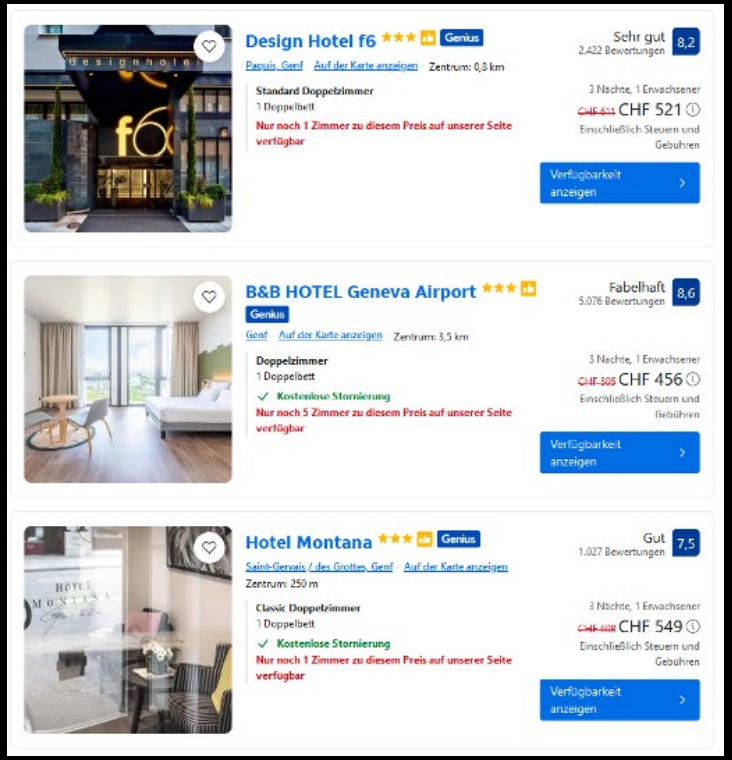


# Die Welt ist voll von Social Engineering:

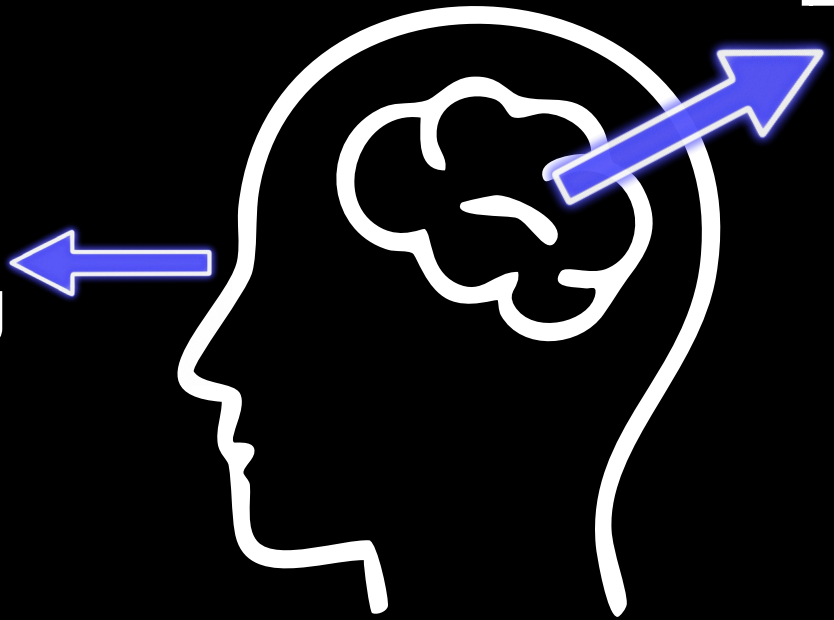



# Die Welt ist voll von Social Engineering:



# Social Engineering nutzt Psychologie

Emotionales Hijacking

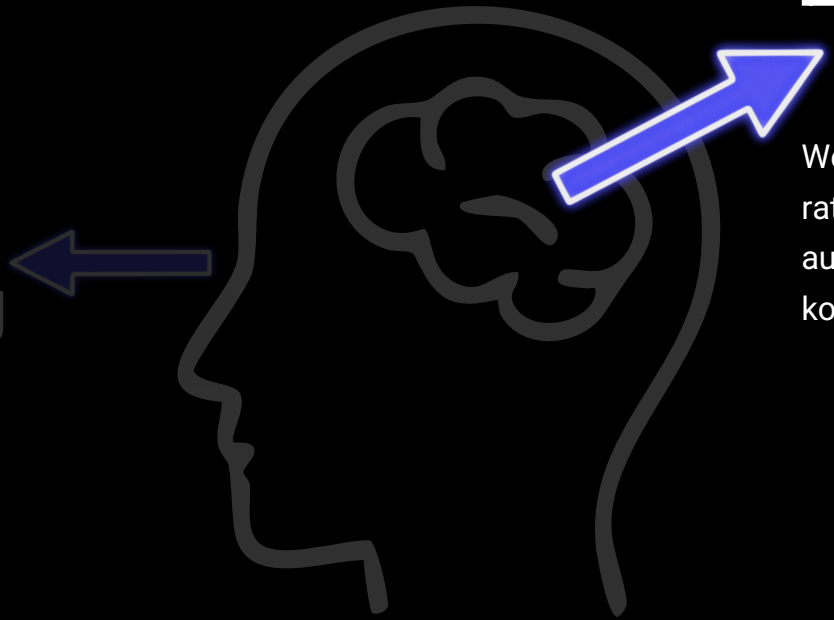


Sinne, Wahrnehmung

# Emotionales Hijacking

Wenn starke Emotionen das rationale Denken vorübergehend ausser Kraft setzen, Stress, kognitive Überlastung...

Sinne, Wahrnehmung



# Auch die Betrüger kennen und verwenden Social Engineering

**Stress / Druck**

**Angst**

**Autorität**

**Sympathie**

*Quelle: Robert Cialdini, Persuasionsforschung*

# Auch die Betrüger kennen und verwenden Social Engineering

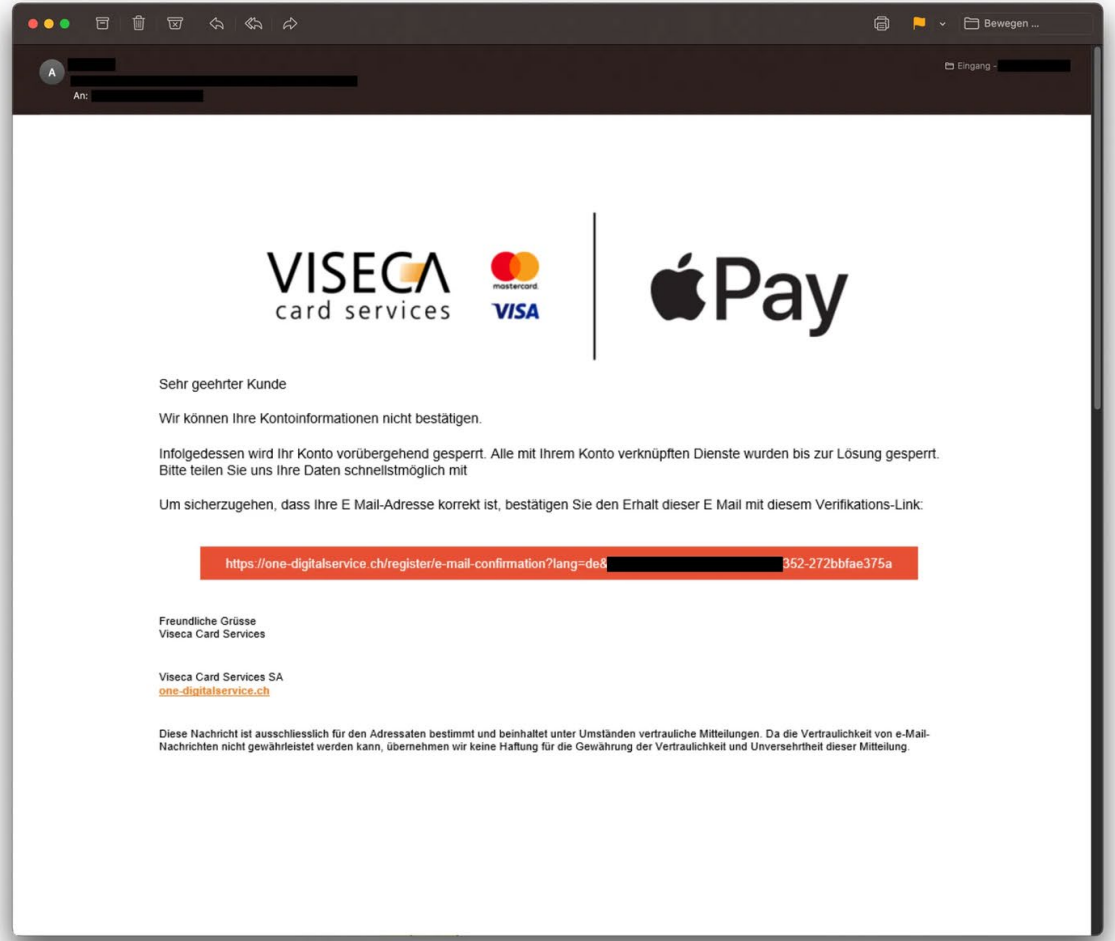
**Stress / Druck**

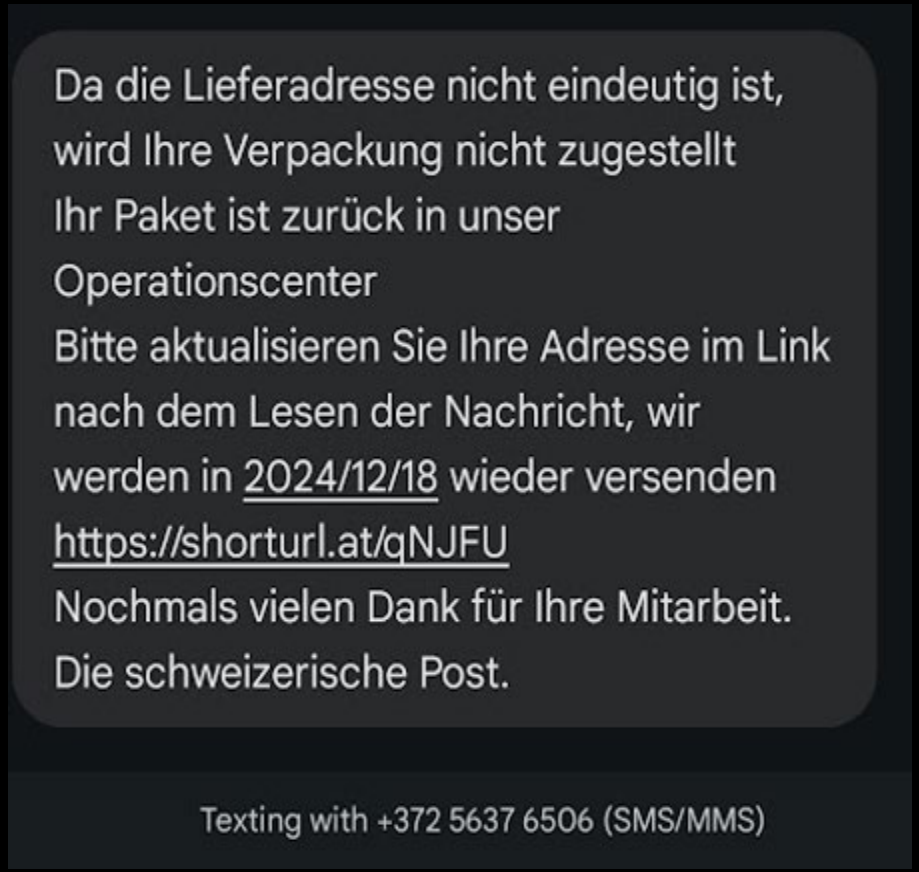
**Angst**

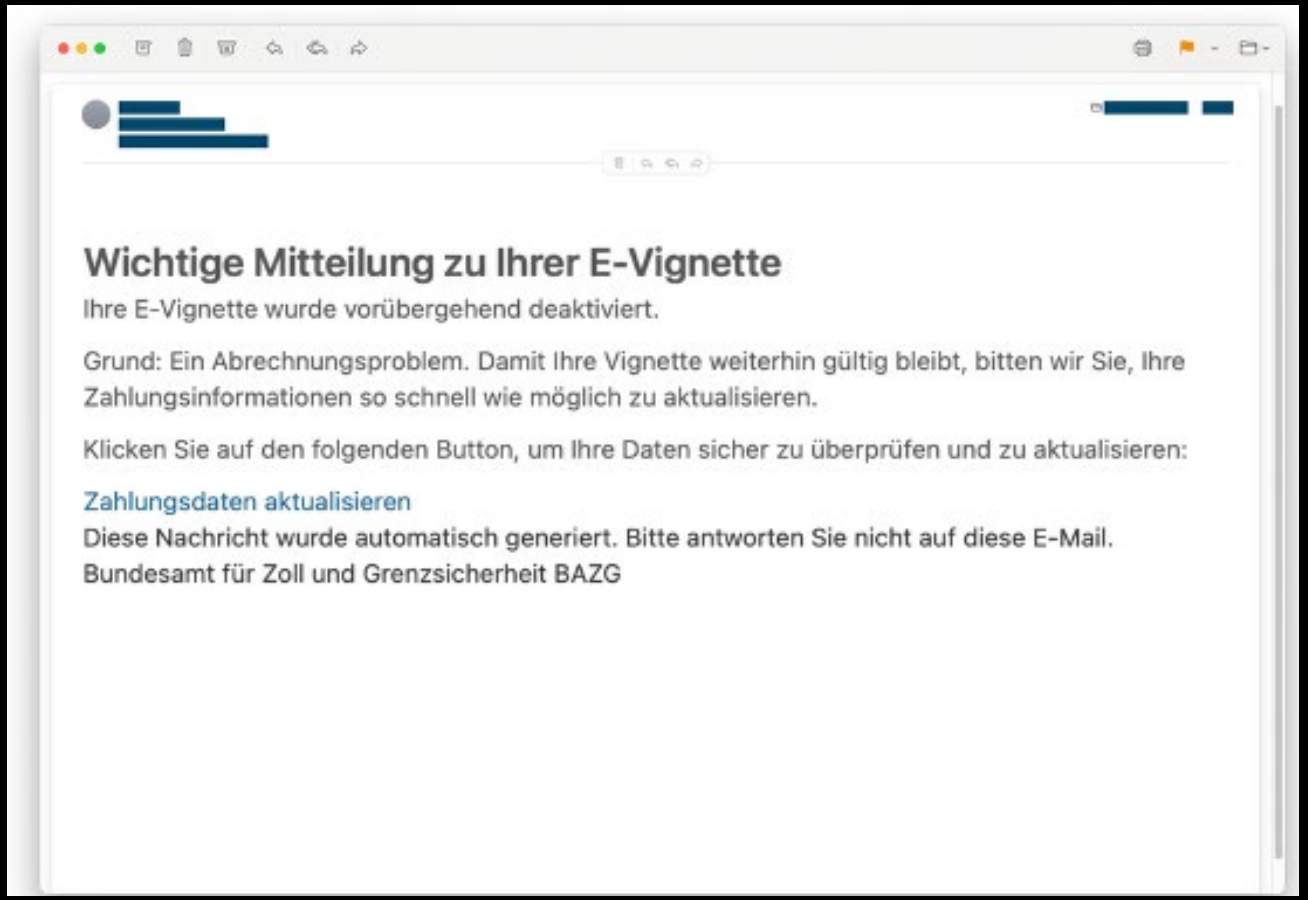
Autorität

Sympathie

*Quelle: Robert Cialdini, Persuasionsforschung*


Bewegen ...
A
An:
Eingang -
VISECA
card services
mastercard
VISA
Pay
Sehr geehrter Kunde
Wir können Ihre Kontoinformationen nicht bestätigen.
Infolgedessen wird Ihr Konto vorübergehend gesperrt. Alle mit Ihrem Konto verknüpften Dienste wurden bis zur Lösung gesperrt.
Bitte teilen Sie uns Ihre Daten schnellstmöglich mit
Um sicherzugehen, dass Ihre E Mail-Adresse korrekt ist, bestätigen Sie den Erhalt dieser E Mail mit diesem Verifikations-Link:
https://one-digitalservice.ch/register/e-mail-confirmation?lang=de&
352-272bbfae375a
Freundliche Grüsse
Viseca Card Services
Viseca Card Services SA
one-digitalservice.ch
Diese Nachricht ist ausschliesslich für den Adressaten bestimmt und beinhaltet unter Umständen vertrauliche Mitteilungen. Da die Vertraulichkeit von e-Mail-Nachrichten nicht gewährleistet werden kann, übernehmen wir keine Haftung für die Gewährung der Vertraulichkeit und Unversehrtheit dieser Mitteilung.


Da die Lieferadresse nicht eindeutig ist, wird Ihre Verpackung nicht zugestellt
Ihr Paket ist zurück in unser Operationscenter
Bitte aktualisieren Sie Ihre Adresse im Link nach dem Lesen der Nachricht, wir werden in 2024/12/18 wieder versenden
https://shorturl.at/qNJFU
Nochmals vielen Dank für Ihre Mitarbeit.
Die schweizerische Post.
Texting with +372 5637 6506 (SMS/MMS)



## Wichtige Mitteilung zu Ihrer E-Vignette

Ihre E-Vignette wurde vorübergehend deaktiviert.

Grund: Ein Abrechnungsproblem. Damit Ihre Vignette weiterhin gültig bleibt, bitten wir Sie, Ihre Zahlungsinformationen so schnell wie möglich zu aktualisieren.

Klicken Sie auf den folgenden Button, um Ihre Daten sicher zu überprüfen und zu aktualisieren:

Zahlungsdaten aktualisieren

Diese Nachricht wurde automatisch generiert. Bitte antworten Sie nicht auf diese E-Mail.
Bundesamt für Zoll und Grenzsicherheit BAZG

# Auch die Betrüger kennen un
# Social Engineerin

Stress

Angst

**Autorität**

Sympathie

*Quelle: Robert Cialdini, Persuasionsforschung*



World / Asia

## Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magramo, CNN
Published 2:31 AM EST, Sun February 4, 2024

boonchai wedmakawand/Moment RF/Getty Images

Authorities are increasingly concerned at the damaging potential posed by artificial intelligence technology.

**(CNN) —** A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call, according to Hong Kong police.

# Auch die Betrüger kennen und verwenden Social Engineering

Stress

Angst

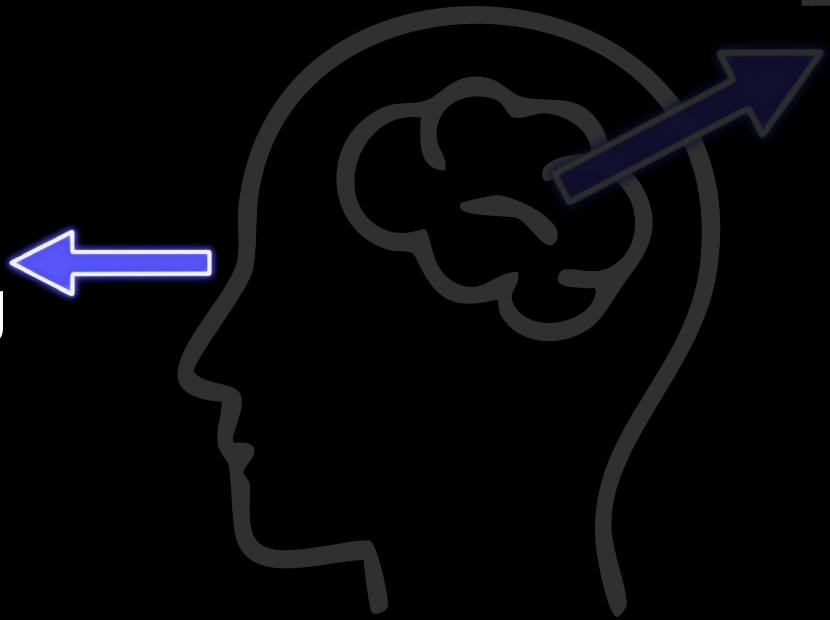
Autorität

**Sympathie**

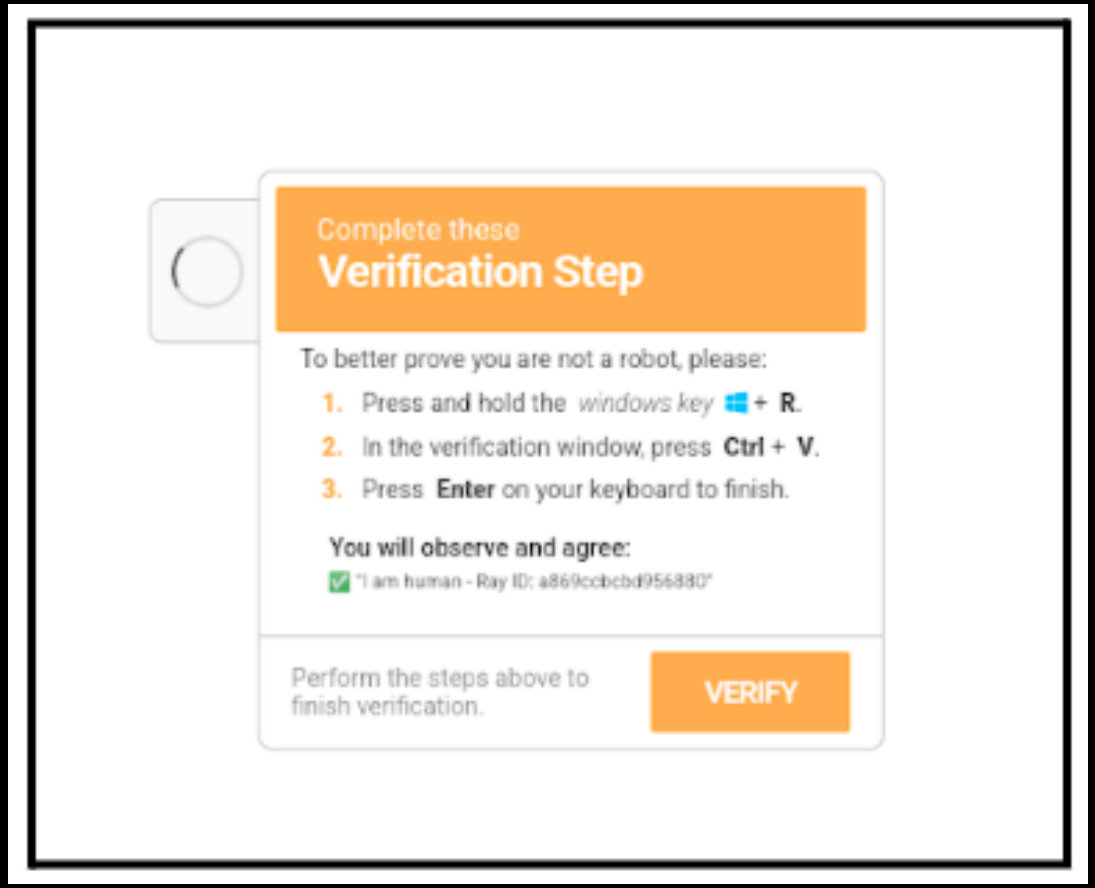

*Quelle: Robert Cialdini, Persuasionsforschung*

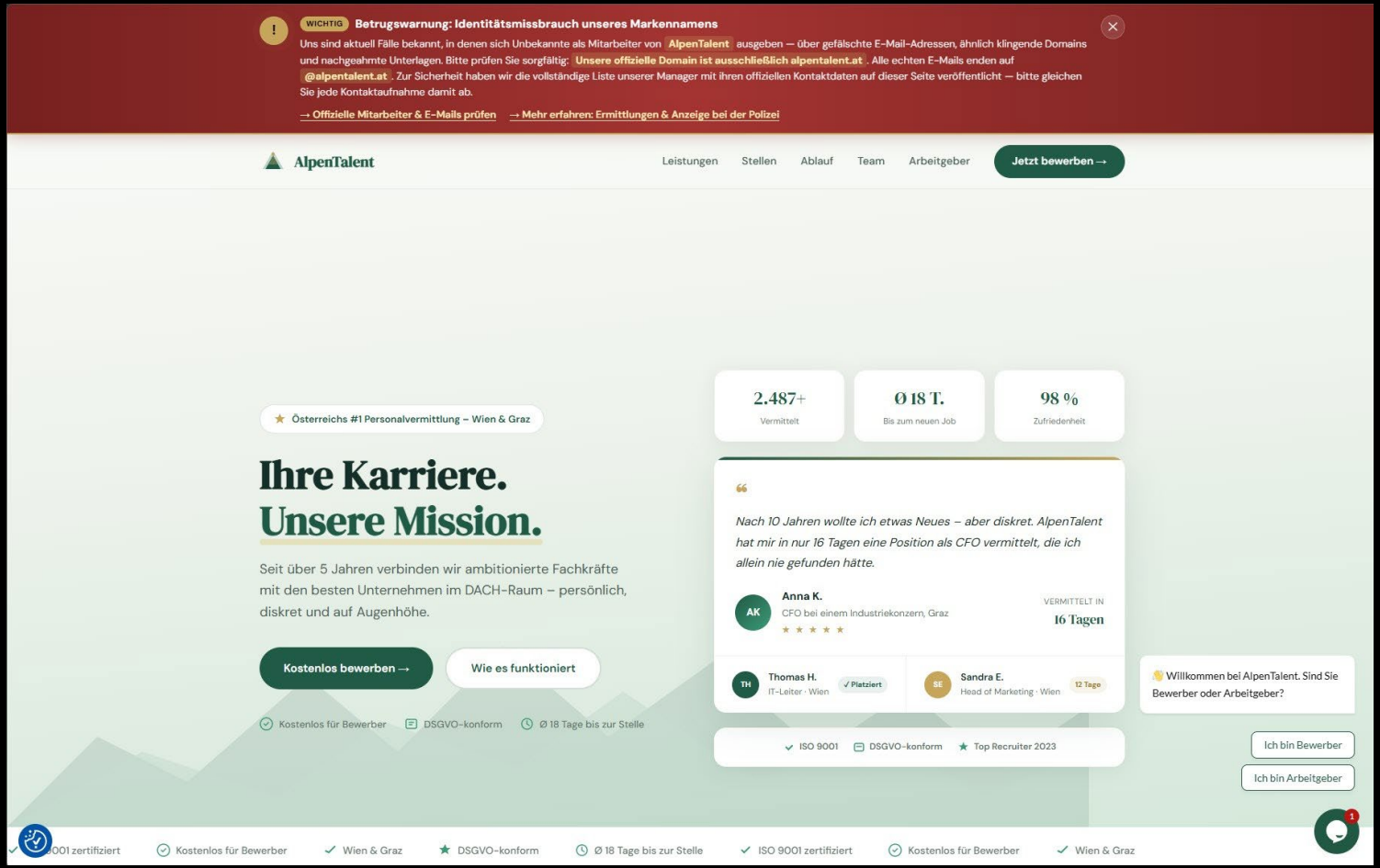
Emotionales Hijacking

Sinne, Wahrnehmung



**Zählen:**
**Wie viel Pässe geben sich die Spielerinnen in den weissen Shirts?**


Complete these
Verification Step
To better prove you are not a robot, please:
1. Press and hold the windows key + R.
2. In the verification window, press Ctrl + V.
3. Press Enter on your keyboard to finish.
You will observe and agree:
"I am human - Ray ID: a869cobcbd956880"
Perform the steps above to finish verification.
VERIFY


WICHTIG
Betrugswarnung: Identitätsmissbrauch unseres Markennamens
Uns sind aktuell Fälle bekannt, in denen sich Unbekannte als Mitarbeiter von AlpenTalent ausgeben — über gefälschte E-Mail-Adressen, ähnlich klingende Domains und nachgeahmte Unterlagen. Bitte prüfen Sie sorgfältig: Unsere offizielle Domain ist ausschließlich alpentalent.at. Alle echten E-Mails enden auf @alpentalent.at. Zur Sicherheit haben wir die vollständige Liste unserer Manager mit ihren offiziellen Kontaktdaten auf dieser Seite veröffentlicht — bitte gleichen Sie jede Kontaktaufnahme damit ab.
→ Offizielle Mitarbeiter & E-Mails prüfen
→ Mehr erfahren: Ermittlungen & Anzeige bei der Polizei
AlpenTalent
Leistungen
Stellen
Ablauf
Team
Arbeitgeber
Jetzt bewerben →
Österreichs #1 Personalvermittlung – Wien & Graz
Ihre Karriere.
Unsere Mission.
Seit über 5 Jahren verbinden wir ambitionierte Fachkräfte mit den besten Unternehmen im DACH-Raum – persönlich, diskret und auf Augenhöhe.
Kostenlos bewerben →
Wie es funktioniert
Kostenlos für Bewerber
DSGVO-konform
Ø 18 Tage bis zur Stelle
2.487+
Vermittelt
Ø 18 T.
Bis zum neuen Job
98 %
Zufriedenheit
Nach 10 Jahren wollte ich etwas Neues – aber diskret. AlpenTalent hat mir in nur 16 Tagen eine Position als CFO vermittelt, die ich allein nie gefunden hätte.
AK
Anna K.
CFO bei einem Industriekonzern, Graz
VERMITTELT IN
16 Tagen
TH
Thomas H.
IT-Leiter · Wien
✓ Platziert
SE
Sandra E.
Head of Marketing · Wien
12 Tage
ISO 9001
DSGVO-konform
Top Recruiter 2023
Willkommen bei AlpenTalent. Sind Sie Bewerber oder Arbeitgeber?
Ich bin Bewerber
Ich bin Arbeitgeber
ISO 9001 zertifiziert
Kostenlos für Bewerber
Wien & Graz
DSGVO-konform
Ø 18 Tage bis zur Stelle
ISO 9001 zertifiziert
Kostenlos für Bewerber
Wien & Graz

AlpenTalent

Leistungen Stellen Ablauf Team Arbeitgeber **Jetzt bewerben →**

UNSER TEAM

# Lernen Sie uns kennen

Erfahrene HR-Profis, die Ihre Branche aus dem Effeff kennen. Wir verbinden ambitionierte Fachkräfte mit den besten Unternehmen im DACH-Raum.

## Unser Management

### Julia Neumann

Senior Partner & Co-Gründerin

15 Jahre HR-Expertise in Finance & Executive Search. Ehem. Head of Talent bei einer der führenden Wirtschaftsprüfungsgesellschaften.

julia.neumann@alpentalent.at

### Elisabeth Böhm

Managing Partner

Spezialist für IT, Tech & Digitalisierung. 12 Jahre Erfahrung in der Vermittlung von Software-Profis und digitalen Führungskräften.

elisabeth.boehm@alpentalent.at

### Sophia Zöllner

Senior Recruiterin

Expertin für Marketing, Sales & HR. Vermittelt seit 9 Jahren erfolgreich Kandidaten in Branchen von FMCG bis FinTech.

sophia.zoellner@alpentalent.at

👋 Willkommen bei AlpenTalent. Sind Sie Bewerber oder Arbeitgeber?

Ich bin Bewerber

Ich bin Arbeitgeber

1

SteinerSearch
— BOUTIQUE PERSONALBERATUNG

Leistungen Mandate Ablauf Team Unternehmen +43 316 487 011 BEWERBEN →

# Unsere Geschäftsführung

Drei Persönlichkeiten, die SteinerSearch täglich mit Anspruch und Herzblut leiten.

## Julia Steiner

GESCHÄFTSFÜHRERIN

15 Jahre HR-Expertise in Executive Search & Strategie. Übernimmt seit 2024 die Gesamtverantwortung für SteinerSearch und gestaltet die nächste Wachstumsphase der Boutique.

julia.steiner@steinersearch.at

## Katharina Jäger

SENIOR PARTNERIN

Spezialistin für Finance & Executive Search. 12 Jahre Erfahrung in der Vermittlung von Top-Führungskräften — ehemalige Head of Talent bei einer der führenden Wirtschaftsprüfungsgesellschaften.

katharina.jaeger@steinersearch.at

## Hannah Kölbl

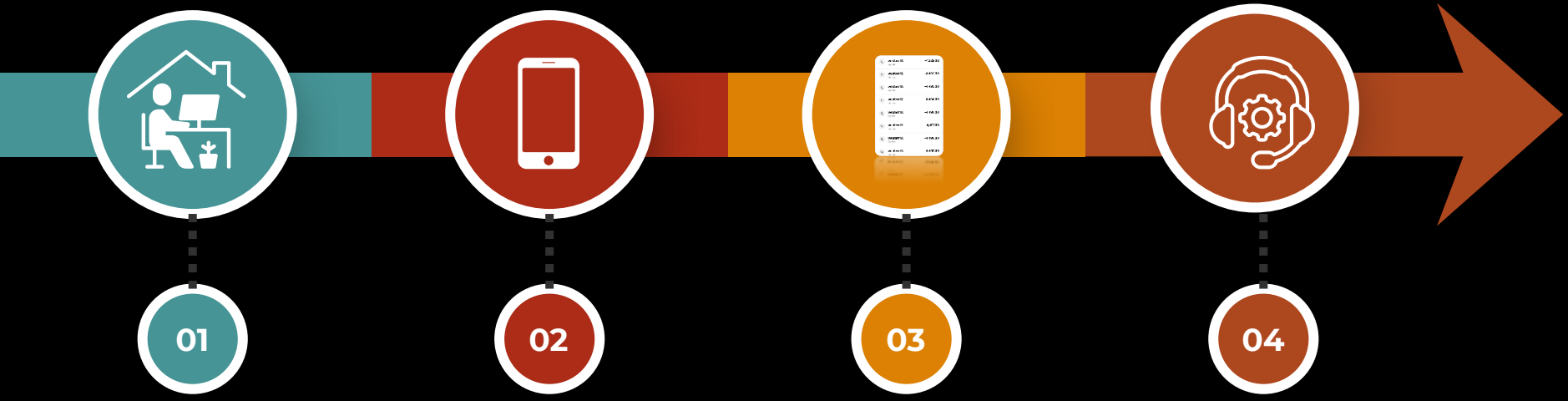
MANAGING PARTNERIN

Expertin für IT, Tech & Digitalisierung. Über ein Jahrzehnt Erfahrung in der Vermittlung von Software-Profis und digitalen Führungskräften — mit ausgeprägtem Gespür für Kultur-Fit.

hannah.koelbl@steinersearch.at

Guten Tag 👋 Wie k

# Max




**Vertrauen aufgebaut**

**Max fragt nach ID**

**Überweisung nach Afrika**

**Haftung wird abgelehnt**

## ID nicht recht geprüft:

- Confirmation Bias
- Autorität

# Emotional Hijacking

- Gefühle, Attraktivität
- Sympathie
- Isolation
- Allenfalls Vorwarnung Bank-Ablehnung

# Weg vom “doofen” Kunden.
# Hin zu: Human Centred Fraud Prevention

1

### Transparenz  & Austausch

Kooperation, Daten teilen,
Spuren sichtbar machen

2

### Liability Shift?

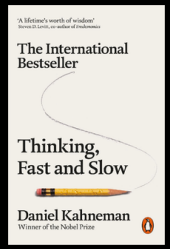
Faktor Mensch einberechnen

3

### Psychologie einbauen

App, Kundendienst, Benachrichtigungen: Psychologie-Check machen

# Bei Betrug sollten wir unsere rationalen 20 % „aufwecken”:




~~🐇 System 1~~

~~Schnell · intuitiv · automatisch~~

## 🐢 System 2

Langsam · rational · durchdacht

# Danke!

**Jill Wick**

KEYNOTE

# Cybercrime vorbeugen – Gemeinsam statt allein

**Serdar Günal Rütsche** · Chef Cybercrime & Leiter NEDIK · Kantonspolizei Zürich

**Hinweis**

# Diese Vortragsfolien stehen nicht für den Nachversand zur Verfügung.

Der Referent stellt die Folien seiner Keynote bewusst nicht zum Download bereit.
Wir danken Ihnen für Ihr Verständnis.


CYBER CRIME POLICE.CH
Hier immer informiert bleiben
SERDAR GÜNAL RÜTSCHE

PANEL

# Wie durchbrechen wir die Betrugskette – und wer muss wo handeln?

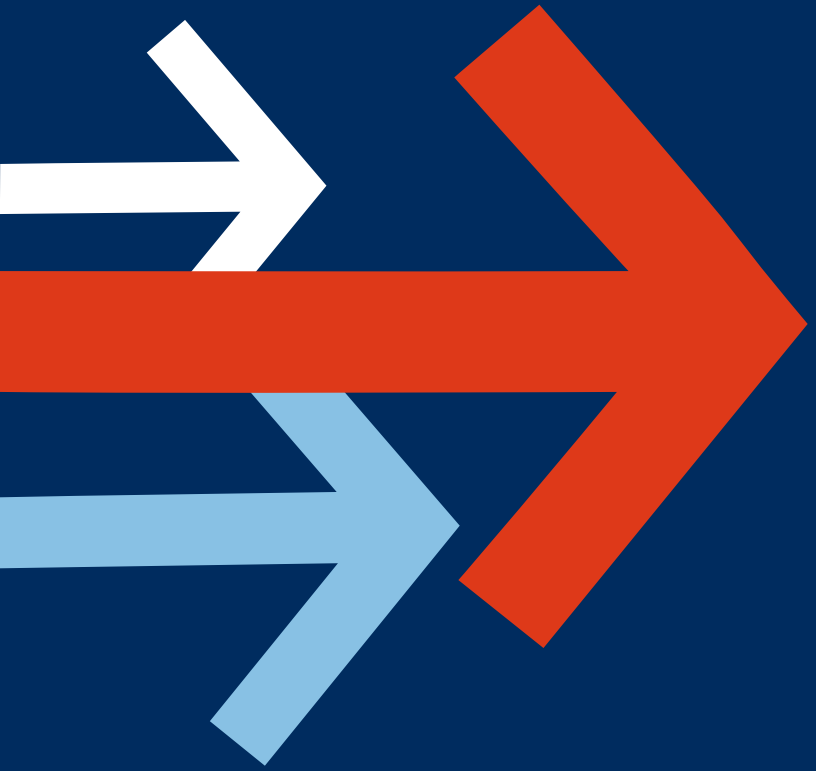
**Oskar Braszczynski**
Government & Social Impact Partner, Meta

**Katharina Höhn**
Head Fraud Management, TWINT

**Susanne Grau**
Leiterin Bereich Wirtschafts-kriminalistik, HSLU

**Richard Hess**
Leiter Digital Finance, Swiss Banking

# Eindrücke vom Cross-Industry Roundtable am Vormittag

# Key Takeaways

Swiss Anti-Fraud Summit 2026

FEEDBACK-UMFRAGE

→ Feedback teilen

# Vielen Dank! Wie war es für Sie?

Helfen Sie uns, den Swiss Anti-Fraud Summit weiterzuentwickeln. Teilen Sie Ihr Feedback zu den heutigen Keynotes, Referierenden und dem Gesamterlebnis – die Antworten sind anonym.

**Bewerten Sie Ihre Erfahrung.**