



Betrug im Online- Zahlungsverkehr

X-Border 2016

d.gamma@crif.com



Betrug im Online-Zahlungsverkehr

- Wie gross ist das Problem Online-Betrug?
- Wie gehen Betrüger vor?
- Datenhandel im Internet
- Wie vor Betrug schützen?
- Fazit & Ausblick



Wie gross ist das Problem Online-Betrug?

2,4 Milliarden Euro

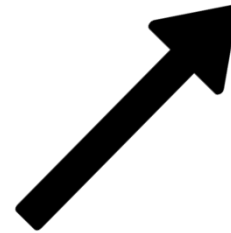
Schaden durch Betrug im Online-Handel

Quelle: Bundeskriminalamt, Daten für den deutschen Online-Handel 2014

Wie gross ist das Problem Online-Betrug?



4 von 5 Online-Händlern haben regelmässig mit Betrug zu kämpfen



Bei über 50% hat die Betrugszahl in den letzten fünf Jahren zugenommen



ca. 1.5% der Bestellungen im Durchschnitt sind Betrug

(Quelle 1&2: Betrug und Betrugsprävention im Online-Handel, Aktuelle Ergebnisse aus dem Projekt "E-Commerce-Leitfaden")
(Quelle 3: CyberSource Fraud Report, London Fraud Survey, EHI Online Payment Studie)

Die häufigsten Betrugsarten, mit denen Händler zu tun haben

Falsche Identitäten	Daten des Kundenkontos sind frei erfunden
Bonitätsbetrug	Kunde täuscht Solvenz vor
Identitätsdiebstahl	Daten des Kunden/des Kundenkontos sind gestohlen
Kreditkartenbetrug	Gestohlene Kreditkartendaten werden genutzt

Quelle: Umfrage im Rahmen des Online Fraud Forum 2015 von RiskIdent)

Wie gehen Betrüger vor?

Früher haben es Betrüger einfach mit falschen Daten versucht und waren relativ leicht zu erkennen.



Kundin

Martha Meier

24 Jahre alt

m.meier@trash-mail.com

Bonitätsauskunft: not found

Artikel: iPhone

Kauf auf Rechnung

Wie gehen Betrüger vor?

Früher haben es Betrüger einfach mit falschen Daten versucht und waren relativ leicht zu erkennen.



Kundin

Martha Meier

24 Jahre alt

m.meier@trash-mail.com

Bonitätsauskunft: not found

Artikel: iPhone

Kauf auf Rechnung

unseriöser E-Mail-Provider

Wie gehen Betrüger vor?

Früher haben es Betrüger einfach mit falschen Daten versucht und waren relativ leicht zu erkennen.



Kundin

Martha Meier

24 Jahre alt

m.meier@trash-mail.com

Bonitätsauskunft: not found

Artikel: iPhone

Kauf auf Rechnung

unseriöser E-Mail-Provider

keine Bonitätsauskunft möglich

Wie gehen Betrüger vor?

Früher haben es Betrüger einfach mit falschen Daten versucht und waren relativ leicht zu erkennen.



Kundin

Martha Meier

24 Jahre alt

m.meier@trash-mail.com

Bonitätsauskunft: not found

Artikel: iPhone

Kauf auf Rechnung

unseriöser E-Mail-Provider

keine Bonitätsauskunft möglich

Risikoartikel

Wie gehen Betrüger vor?

Früher haben es Betrüger einfach mit falschen Daten versucht und waren relativ leicht zu erkennen.



Kundin

Martha Meier

24 Jahre alt

m.meier@trash-mail.com

Bonitätsauskunft: not found

Artikel: iPhone

Kauf auf Rechnung

unseriöser E-Mail-Provider

keine Bonitätsauskunft möglich

Risikoartikel

keine sichere Zahlart

Wie gehen Betrüger vor?

Heute kommen Betrüger immer leichter an echte Identitäten heran.

Möglichkeiten:

- Telefonbücher
- Todesanzeigen
- Online-Gewinnspiele
- oder einfach Google ...

Wie gehen Betrüger vor?

**Und auch Ihre Zugangsdaten sind nicht sicher.
E-Mails und Passwörter werden immer wieder geklaut.**

Beispiele von Datenlecks bei grossen Onlinediensten:

- Softwareanbieter Adobe (152 Millionen Datensätze)
- Handelsplattform Ebay (145 Millionen Datensätze)
- Datingplattform Ashley Madison (32 Millionen Datensätze)
- Spielenetzwerk Sony Playstation Network (25 Millionen Kundenkonten)

Manchmal ist ein Klau gar nicht notwendig ...

Frage:

**Wie viele unterschiedliche Passwörter
nutzen Sie im Alltag?**

Manchmal ist ein Klau gar nicht notwendig ...

Frage:

**Wie viele unterschiedliche Passwörter
nutzen Sie im Alltag?**

... und wie sicher sind diese?

„Top 5“ bzw. „Worst 5“ der Passwörter

RANK	PASSWORD
1	123456
2	password
3	12345678
4	querty
5	12345

(Quelle: Worst Passwords of 2015 – Splashdata.com)

Datenhandel im Internet: Frage

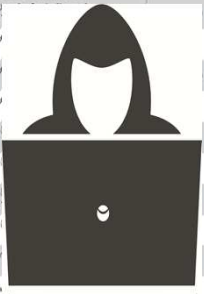
**Was kosten Ihre
Kreditkarteninformationen?**



Datenhandel im Internet

In Foren und auf Online-Marktplätzen bieten Hacker Ihre Daten zum Kauf an:

- Verifizierte Visa oder MasterCard (USA): 7\$
- Deutsche Visa oder MasterCard mit allen notwendigen Daten: 40\$
- Komplette US-Identität: 65\$
(Name, Adresse, Telefon-Nr., E-Mail-Adresse, Geburtsdatum, Sozialversicherungsnummer)
- Neue Identität in DE: 90\$
(inklusive Sozialversicherung, Führerschein, ...)



Price List for Hacker Goods and Services

Credit Cards	Price in 2013	Price in 2014	Recent Prices
Visa and MasterCard (U.S.)	\$4	\$4	\$7
Visa Classic and MasterCard (U.S.) with Track 1 and Track 2 Data	\$12	\$12	\$15
Visa Classic and MasterCard (IC New Zealand) with Track 1 and Track 2 Data		\$19 - \$20	\$25
Visa Classic and MasterCard 50 Track 1 and 2 Data		\$28	\$40
Visa Classic and MasterCard 50 Track 1 and Track 2 Data		\$19 - \$20	\$40
Visa Classic and MasterCard 50 Track 1 and Track 2 Data		\$28	\$50
Premium Visa and MasterCard Track 1 and Track 2 Data		\$23 (V); \$35 (MC)	\$30
Premium Visa and MasterCard with Track 1 and 2 Data		\$23 (V); \$35 (MC)	\$50 - \$60
Premium Visa and MasterCard New Zealand with Track 1 and Track 2 Data		\$23 (V); \$35 (MC)	\$35 for V and MC
Premium Visa and MasterCard with Track 1 and Track 2 Data		\$23 (V); \$35 (MC)	\$80 for V and MC
Premium American Express Card with Track 1 and Track 2 Data		\$23 (V); \$35 (MC)	\$30
Premium Discover Card (U.S.)		\$23 (V); \$35 (MC)	\$30
VBV (U.K., Australia, Canada, EU and Asia)	\$17 - \$20	\$28	\$25

Hacking Email and Social Media Accounts	Recent Prices
Popular U.S. Email Accounts (Gmail, Hotmail, Yahoo)	\$129
Popular Russian Email Accounts (Mail.ru, Yandex.ru, and Rambler.ru)	\$65 - \$103
Popular Ukrainian Email Accounts (Ukr.net)	\$129
Popular U.S. Social Media Accounts	\$129
Popular Russian Social Media Accounts (VK.ru and Ok.ru)	\$194
Corporate Email Accounts	\$500 per mailbox
IP address of Computer User	\$90

(Quelle: Dell SecureWorks - Underground Hacker Markets, Annual Report – April 2016)

Datenhandel im Internet: Beispiel transfermarkt.de

The screenshot shows the profile of Christian Bickel, a 25-year-old left winger from Bad Langensalza, Germany. He is currently at SC Paderborn 07 in the 2. Bundesliga. His market value is listed as 400 Tsd. €. The page includes a detailed sidebar with his personal and career data, a position diagram, a market value development chart, and a list of relevant news items.

#16 Christian Bickel

SC Paderborn
2. Bundesliga
Ligahöhe: 2. Liga
Im Team seit: 20.08.2015
Vertrag bis: 30.06.2017

400 Tsd. €
Letzte Änderung: 11.02.2016

SPIELERDATEN

Geburtsdatum: 27.01.1991
Geburtsort: Bad Langensalza
Alter: 25
Größe: 1,78 m
Nationalität: Deutschland
Position: Mittelfeld - Linksaußen
Fuß: beidfüßig
Spielerberater: Karl M. Herzog Sportmanagement
Aktueller Verein: SC Paderborn 07
Im Team seit: 20.08.2015
Vertrag bis: 30.06.2017

Detailposition

Hauptposition: Linksaußen
Nebenposition: Rechtsaußen

Marktwertentwicklung

Aktueller Marktwert: 400 Tsd. €
Letzte Änderung: 11.02.2016
Höchster Marktwert: 500 Tsd. €
20.01.2014

DIE AKTUELLEN TRIKOTS

ZUM TRIKOTSHOP

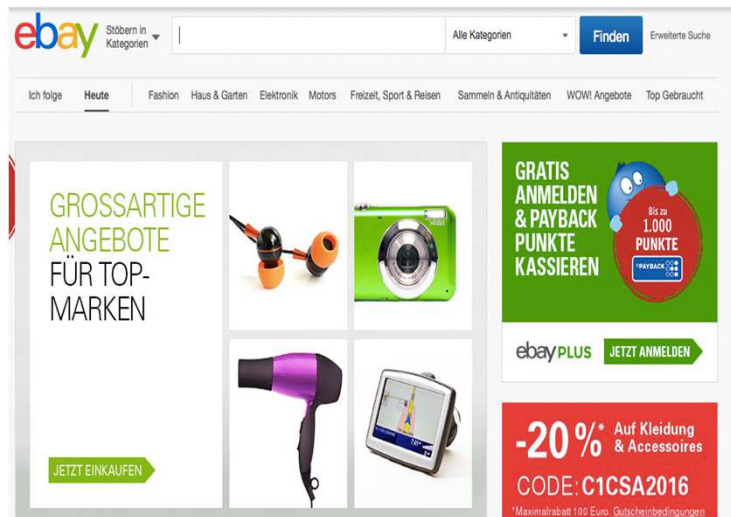
RELEVANTE NEWS

20.08.2015 18:58
Bestätigt: SC Paderborn verpflichtet Rostocker Bickel

13.05.2015 20:47
Hansa Rostock holt den Landespokal

- Vorname, Name
- Geburtsdatum
- Wohnort
- Gute Bonität

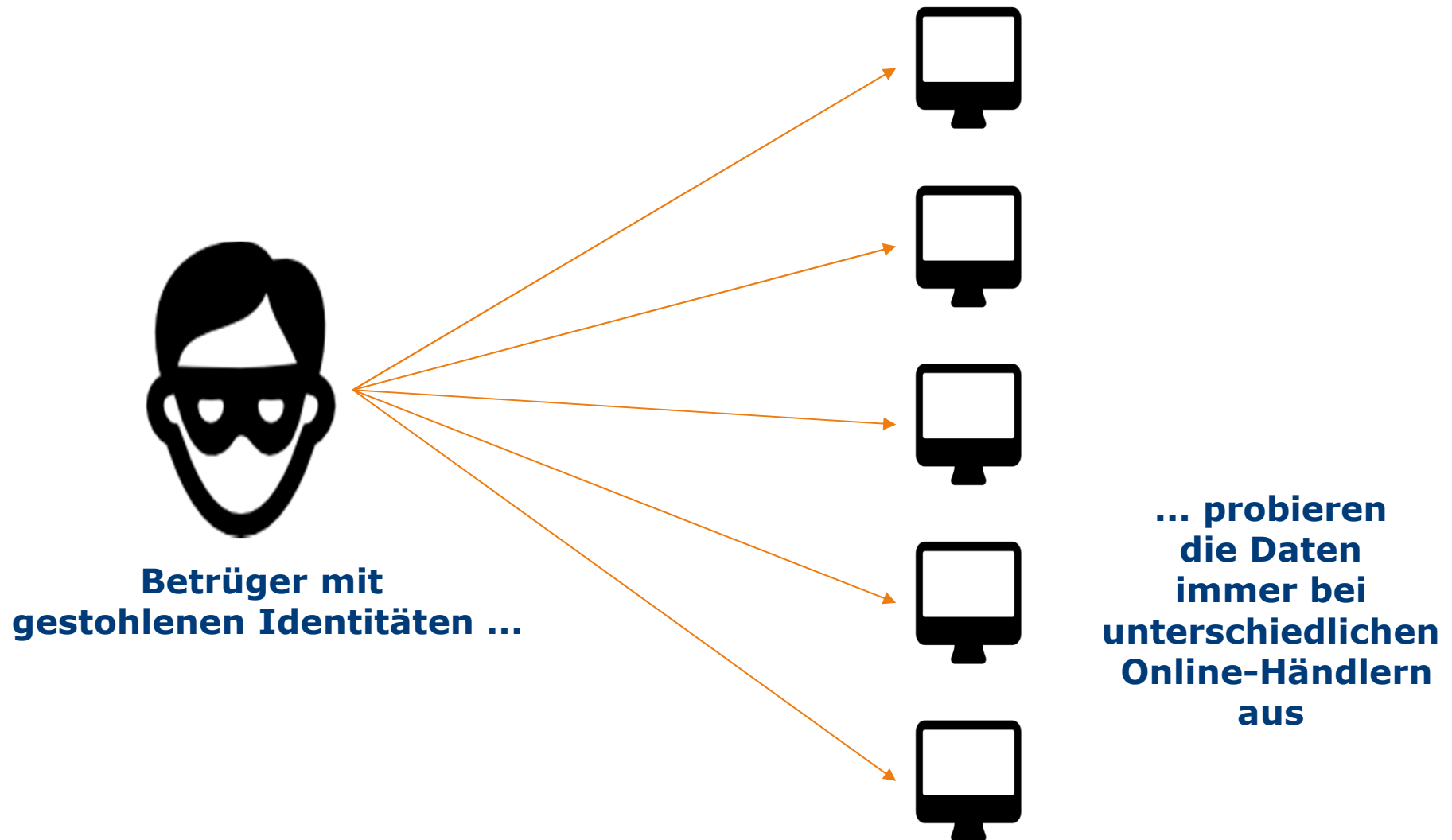
Datenhandel im Internet: Beispiel Marktplätze



- Vorname, Name
- E-Mail
- Adresse
- Kontoinformationen oder PayPal E-Mail



Wie nutzen Betrüger die gestohlenen Daten?



Wie können Online-Händler sich vor Betrug schützen?

Problem:

- Manuelle Betrugserkennung meist gut, aber zeitaufwendig
- Überprüfung **aller** Transaktionen bei mittleren und grossen Online-Händlern nur mit sehr hohem Aufwand

Wie können Online-Händler sich vor Betrug schützen?

Bereits oft im Einsatz sind folgende Lösungen:

- Identifikations- und Bonitätsprüfung
- Blacklist (eigene oder z.B. VSV)
- Fraud-Filter

Diese Massnahmen reichen aber heute aufgrund der Zunahme von «Identitätsdiebstahl» und «Account-Takeover» nicht mehr aus.

Wie können Online-Händler sich vor Betrug schützen?

Lösung:

Verbinden von

- Mensch
- Daten (Erfahrung)
- Domänenwissen (Betrugsmuster)
- Technologie



Präventiv durch Lernfähige Transaktionsanalyse-Tools

Machine Learning in der Betrugsprävention

- Machine Learning ermöglicht skalierbare Betrugsprävention
- Selbstlernende Systeme können
 - Muster erkennen
 - Wahrscheinlichkeiten in Echtzeit berechnen
- Anders als beim starren Scoring, kann beim Machine Learning ein einzelnes Attribut ausschlaggebend sein



Beispiel Transaktionsanalyse: **Account-Takeover?**

Kundin

Hedwig Müller

74 Jahre alt



Transaktionsinformationen:

- Langjährige Bestandskundin
- Bislang hauptsächlich Kleidung bestellt
- Lieferadresse nicht Rechnungsadresse
- Artikel: Lego Star Wars (Wert: 350 CHF)

Bewertungs-Verfahren:

Alter +10	Abw. Lieferadresse -10
Bestandskundin +10	Risikoartikel -10
Bonität +10	Kauf auf Rechnung -10

Bewertung: 0

Beispiel Transaktionsanalyse: **Account-Takeover?**

Kundin

Hedwig Müller

74 Jahre alt



Blick in die Bestellhistorie:

... | 2.1.15 Kleidung | **10.2.15 Spielzeug**
| 15.6.15 Kleidung | 18.9.15 Kleidung |
11.2.16 Spielzeug | ...

Frau Müller hat vor einem Jahr schon einmal Spielzeug gekauft. Eventuell Geburtstag eines Enkels?

Die Maschine erkennt Muster, unabhängig von der Erklärung.

Einzelnes Attribut kann den Ausschlag geben

Nächster Schritt: Daten anreichern, Daten vergleichen

Heutige Systeme sind auch in der Lage, aus einzelnen Informationen neue Erkenntnisse zu ziehen. **Beispiele:**

- Aus Adressangaben > Genaue Orte
- Aus Browserinformationen > Angaben zum Gerät
- Aus E-Mail-Adressen > Genereller Aufbau der E-Mail
- Korrelation zwischen Namen und Alter

Diese Daten können dann direkt verglichen werden

Aus Adressangaben Ortsinformationen (Geo-Daten) extrahieren

Adresse 1:

Hochallee 74

20149 Hamburg

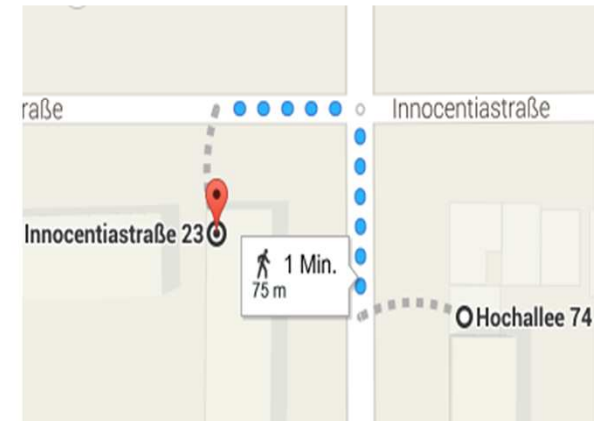
Entfernung
75 Meter



Adresse 2:

Innoccientiastraße 23

20144 Hamburg



Adresse 1:

Signastrasse 14

8008 Zürich

Entfernung
52 Meter



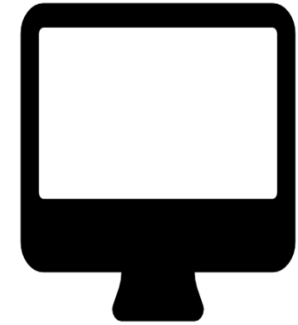
Adresse 2:

Forchstrasse 52

8032 Zürich



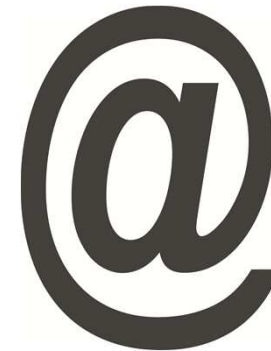
Aus Browserdaten eine Geräteart identifizieren



- Auflösung 1280x909 (spezifisch)
- Windows XP (alt)
- Firefox 31.0 (alt)
- ...
- **... Virtuelle Maschine !**

Mustererkennung bei E-Mails

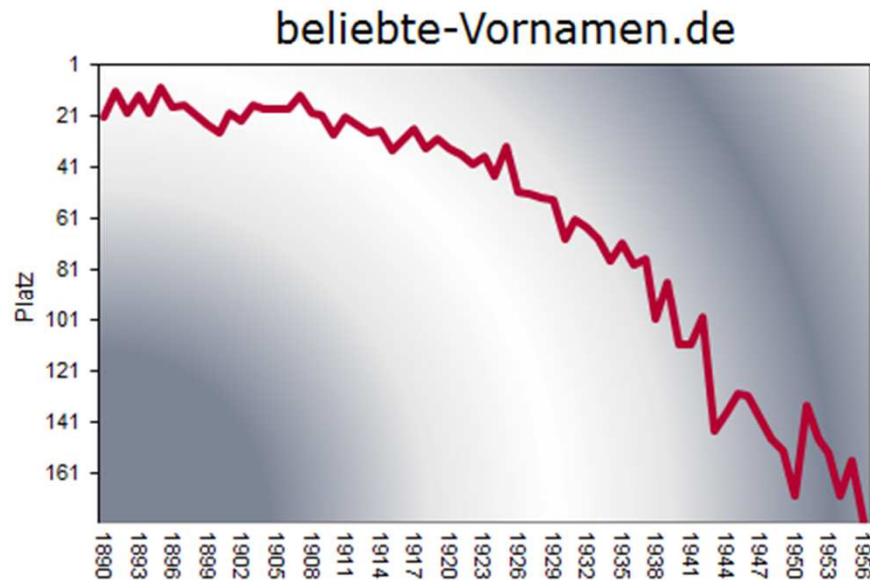
- schmid-0812@gmx.de
- mueller-0814@gmx.at
- meier-0815@gmx.ch
- schulze-0912@gmx.it



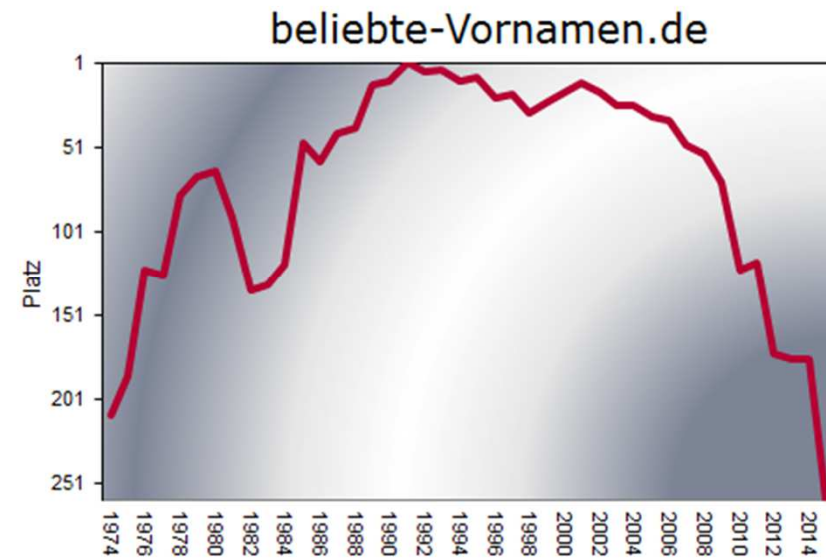
Häufige Namen, Uhrzeit etc.

Korrelation zwischen Namen und Alter

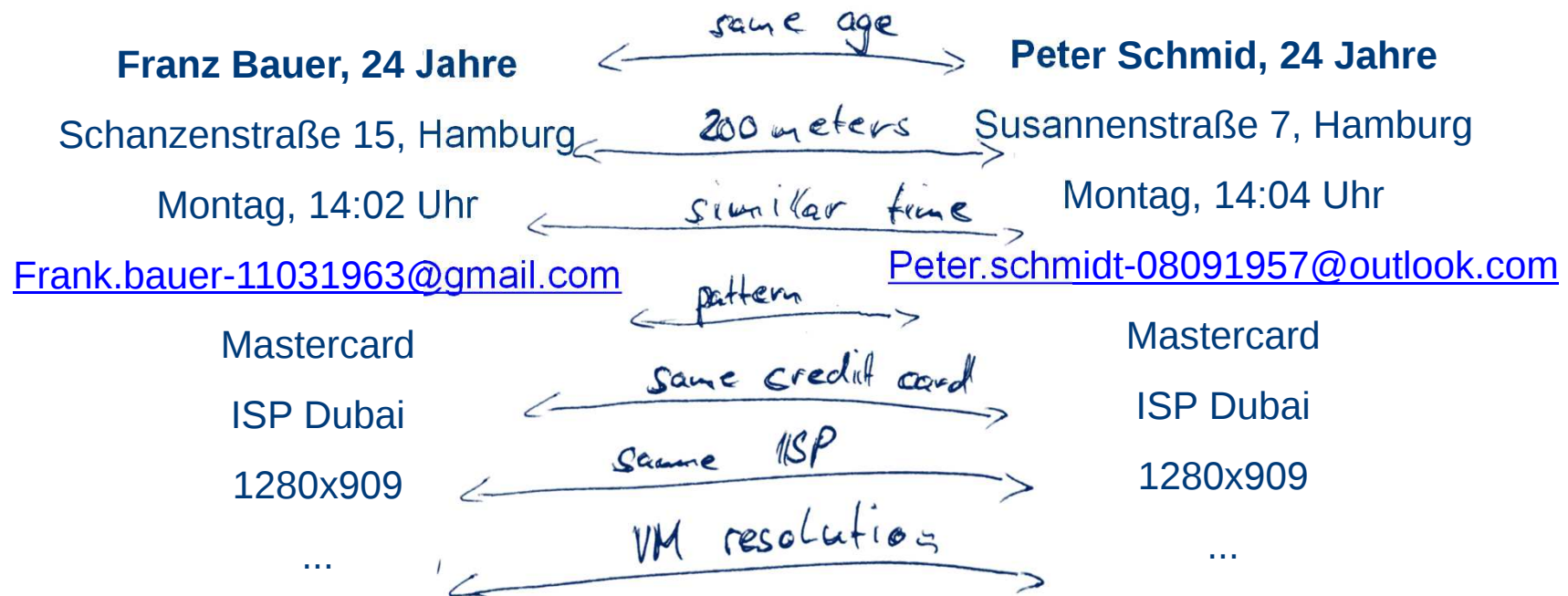
Hedwig, die jünger ist als 50:
weniger wahrscheinlich



Kevin, der älter ist als 50:
weniger wahrscheinlich



Unauffällige Angaben stehen in Verbindung



Fazit & Ausblick

- **Es war schon schwieriger sich eine Identität für den Zahlungsverkehr zu beschaffen**
- **Betrugsversuche und Betrugserfolge nehmen zu**
- **Es gibt Lösungen sich besser gegen Betrug zu schützen**
- **Händler müssen Entscheiden ob Sie proaktiv oder reaktiv handeln**



Vielen Dank

d.gamma@crif.com

