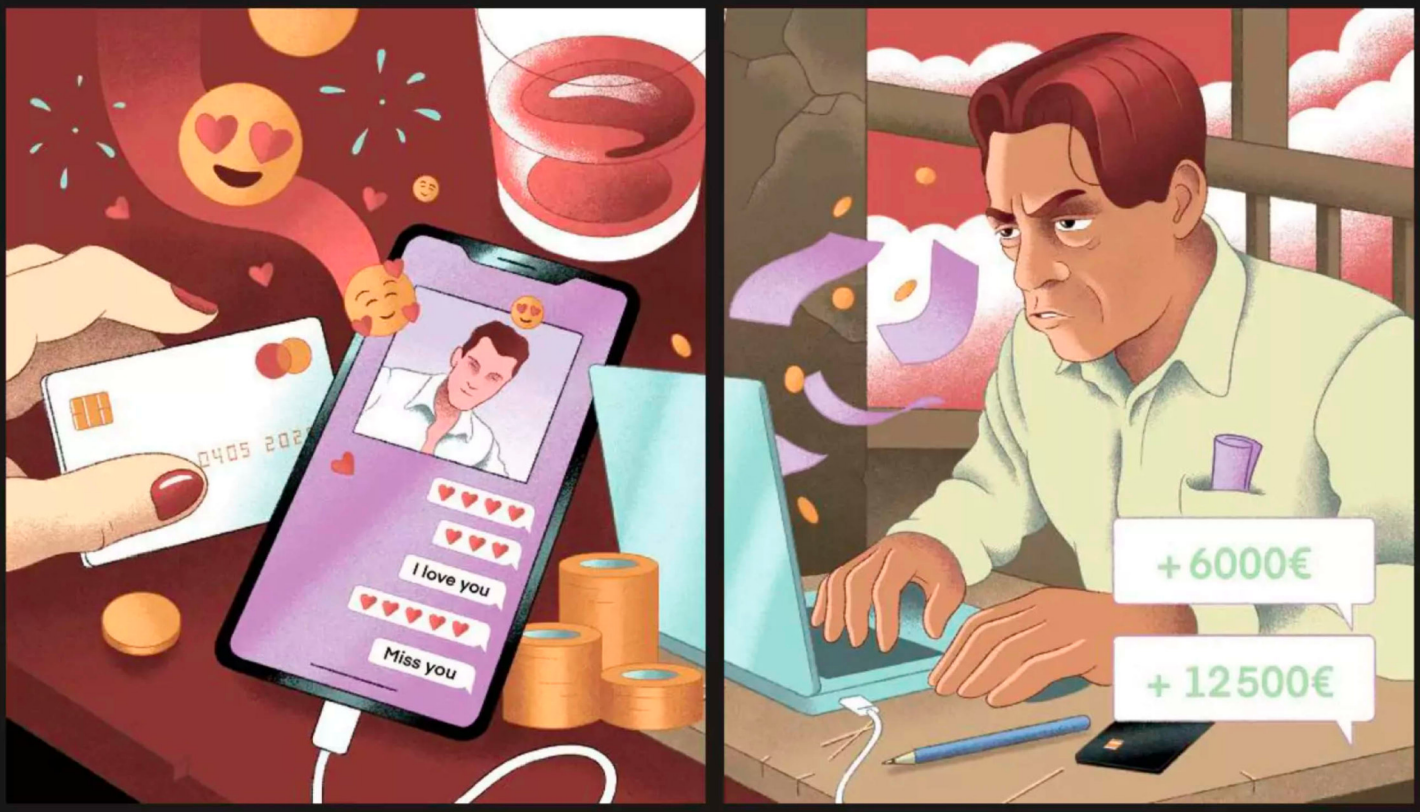
In den Fängen der Internetmafia

Leer geräumte Konten, gestohlene Identitäten, falsche Liebe. Mit perfiden Tricks scheffeln Onlinebetrüger Milliarden. Jeder kann zum Opfer werden. Die Ermittler sind oft hilflos. Aber es gibt Auswege

Text von Michael Kneissler, Jan-Philipp Hein, Lukas Koperek, Annica Kramer, Giuliano Ruben, Leon Werner, Lara Wernig, Janna Wolf und Christoph Elflein, Illustrationen von Lennart Menkhaus

Tatort Internet: Wer online unterwegs ist, läuft Gefahr, ausgespäht und Opfer weltweit agierender Betrügerbanden zu werden



Liebeslüge: Professionell geschulte Betrüger in nigerianischen Callcentern locken ihre Opfer mit falschen Versprechen

Die junge Frau heißt Mandy Lu. Hübsches Gesicht, glatte Haare, dunkle Augen. Eine zierliche Schönheit. „Sie wurden mir in der Freundesliste empfohlen“, schreibt sie über Facebook Messenger an Walter Matt, 58, aus Hessen. Matt heißt eigentlich anders, aber als nicht ganz unvermögender Selbstständiger möchte er seinen echten Namen nicht nennen. Die Sache ist ihm peinlich. „Würde es Sie stören, wenn wir uns ein wenig unterhalten?“, fragt Frau Lu höflich.

In ihrem Profil steht, dass sie Marketing-Managerin in London ist. Auf ihren Fotos zeigt sie ihr Gesicht

»Menschen haben sich nach einem solchen Betrug das Leben genommen«

Nino Goldbeck, Oberstaatsanwalt, Zentralstelle Cybercrime Bayern

selten. Dafür sieht man luxuriöse Hotels in Dubai, New York oder Hongkong, teure Handtaschen, opulente Menüs und einen edlen Sportwagen.

„Wie kannst du dir das denn alles leisten?“ Das fragt Matt. Denn natürlich ist der erfolgreiche Geschäftsmann misstrauisch. Mandy ziert sich ein wenig, das macht die Sache spannender, dann rückt sie damit raus: „Geldanlage. Ich habe einen Bekannten, der ist Krypto-Broker. Ein sehr guter. Wenn du willst, kann er dich auch beraten.“

Ziemlich sicher existiert dieser Broker nicht. Und Mandy Lu auch nicht. Dafür aber die über 100 000 Euro, die Matt verloren hat.

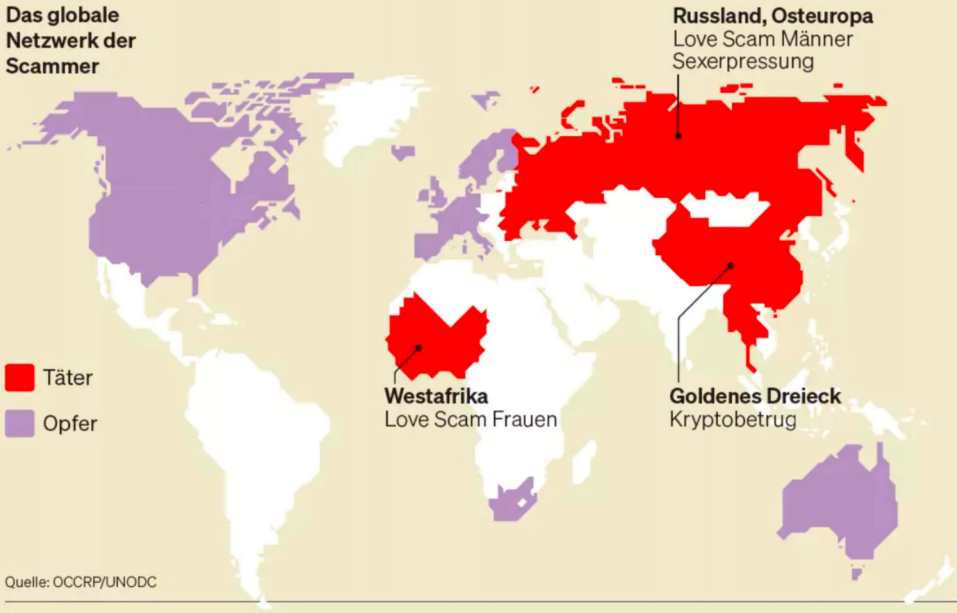
In den vergangenen Jahren entstand eine ganz neue Form der international organisierten Kriminalität. Je mehr das Surfen im Internet zum Dauerzustand wird; je mehr sich das Leben online abspielt – desto mehr eröffnen sich auch für Kriminelle ganz neue Betätigungsfelder. Risikoarm, global und lukrativ.

Skrupellose Verbrecher nutzen die Gier, aber auch die Sehnsüchte, die Gefühle und die Naivität ihrer Opfer aus, um Millionen zu scheffeln. Ach was. Milliarden! Sie gaukeln ehrliches Interesse und Freundschaft vor, manchmal sogar Liebe und Sex oder einfach nur die schnöde Aussicht auf Anlagegewinne. Sie verführen die ihnen Verfallenen zu irrsinnigen Zahlungen. Sie sind bisweilen so erfolgreich, dass sie Existenzen vernichten. Und Opfer, die sich aus dem Fenster in den Tod stürzen, nehmen sie mit einem Achselzucken in Kauf.

Zu besonders bösartigen Verbrechen kommen Betrügereien, die beinah alltäglich sind: Fake Shops, Identitätsdiebstahl oder die moderne Form des Enkeltricks, bei dem arglosen Eltern und Großeltern

Gelockt, geliebt, gelinkt

Internationale Liebesschwindler zocken weltweit eine Billion Euro ab



Geldflüsse weltweit ▶ Europa, Australien, Nordamerika ▶ **1 Billion Euro pro Jahr** ▶ Bitcoins, Krypto, Geldwäscher, Hawala ▶ Nigeria: Black Axe; Russland: Mafia; China: Triaden

Das Locken der Liebesbetrüger

Phase 1 „Loader" durchforsten das Internet nach Opfern. Beliebt sind wohlhabende Singles über 45. Gesucht wird auf allen Plattformen: Instagram, Facebook, TikTok, WhatsApp, Tinder, Hinge.

Phase 2 „Storyteller" übernehmen. Sie denken sich passende (Fake-)Personen und ihre Geschichte für die Opfer aus.

Phase 3 „Moderatoren" starten erst vorsichtig: „How are you?" Dann schnell: „I love you." Sie kundschaften aus, was zu holen ist: Geld, Schmuck, Auto?

Phase 4 Die Täter locken ihr Opfer mit dem, was sie haben wollen: Geld, Aufmerksamkeit, Sex, Liebe.

Phase 5 Beim „Proof of Concept" werden Zweifler mit gefälschten Bankauszügen, Pässen oder Nacktfotos überzeugt.

Phase 6 Die „Terminatoren" quetschen die Opfer aus. Es werden Gewinne versprochen, Probleme wie Unfälle oder gesperrte Konten erfunden. Das ergaunerte Geld schleusen die „Agenten" über Finanzdienstleister wie Western Union nach Nigeria, Laos oder Georgien.

das Geld aus der Tasche gezogen wird: „Hallo Mutti, das ist meine neue Nummer…", heißt es dann auf WhatsApp. Oder Rentnern wird vorgegaukelt, sie müssten schnell ihre Wertsachen vor möglichen Einbrechern in Sicherheit bringen.

Zu den seelischen Verheerungen, die die breit gefächerte Betrugsindustrie hinterlässt, kommt der ökonomische Schaden. Über neun Billionen Euro sollen das weltweit sein – allein beim Love Scamming eine Billion nach Schätzungen der Global Anti-Scam Alliance (GASA). Den Schaden für die deutsche Wirtschaft beziffern Experten auf 179 Milliarden Euro. Durchschnittlich wird jeder Deutsche jährlich beim Einkaufen im Internet um 600 Euro geprellt. 61 Prozent der Verbraucher geben an, in den vergangenen zwölf Monaten Onlinebetrügern auf den Leim gegangen zu sein. Das ist allerdings nur die Spitze des Eisbergs. Die meisten Fälle werden niemals angezeigt. Die Opfer schämen sich.

Das globale Netz der Verbrecher

Bis vor Kurzem steckten vor allem russische und westafrikanische Mafia-Organisationen wie die brutale Bruderschaft Black Axe aus Nigeria hinter den Scams (englisch für Betrug). Aber jetzt mischen auch asiatische Gangster-Syndikate mit. Sie haben im Grenzgebiet von Thailand, Laos und Myanmar große Bürokomplexe hochgezogen, sogenannte Scam-Fabriken, in denen Tausende von Mitarbeitern nichts anderes machen, als weltweit ihre Opfer auszunehmen.

Westliche Geheimdienste und Polizeiorganisationen gehen davon aus, dass die mächtigen chinesischen Triaden im Hintergrund die Fäden ziehen. „Es breitet sich aus wie ein Krebsgeschwür", sagt Benedikt Hofmann von der UN-Behörde zur Drogen- und Kriminalitätsbekämpfung (UNODC). Die Gewinne sind gigantisch: mindestens 35 Milliarden Euro jährlich.

275
Millionen Euro kassierten allein zwei gerade aufgeflogene Mafiagruppen aus Georgien und Israel

32 954
Opfer in 33 Ländern fielen auf die Anlagebetrüger mit 500 Mitarbeitern herein

3,9
Millionen Euro war der höchste Betrag, den ein Investor verlor

Aber Walter Matt in Hessen ahnt nicht, dass er ins Fadenkreuz asiatischer Gangster geraten ist, als „Mandy Lu" ihm ein paar Charts schickt, die zeigen, wie sich ihr Kryptovermögen Monat für Monat verdoppelt hat. Bitcoins, Solana, Shiba – die meisten Namen kennt er nicht. Er googelt den Broker. Es gibt eine Homepage, Referenzen, Impressum, Büroadresse. Sieht sehr professionell aus. Matt transferiert erste Summen auf das Konto der Brokerfirma. Die Aussicht auf schnell verdientes Geld macht ihn unvorsichtig. Als er endlich merkt, dass er reingelegt wurde, wendet er sich an einen Privatermittler.

Jochen Meismann, 63, vom Detektivbüro A-Plus in Dorsten ist einer der erfahrensten Scam- ▶

Fahnder in Deutschland. 2000 Fälle hat er mit seinen zwölf Mitarbeitern und dem weltweiten Netzwerk der World Association of Detectives (WAD) schon gelöst. „Wir machen das seit 25 Jahren“, sagt er, „aber jetzt ist es völlig verrückt geworden. Jeden Tag melden sich mindestens zwei neue Klienten, die abgezockt wurden.“

Matt hatte bereits über 100 000 Euro verloren, als er sich bei Meismann meldete. Für den wohlhabenden Mann eine zwar schmerzhafte, aber nicht existenzbedrohende Summe.

Michael Schneiders Leben ist hingegen ein anderes, seit er in die Fänge der Onlinebetrüger geriet. Ende Februar sitzt der 63-Jährige, der aus Scham auch anders genannt werden will, auf der Geburtstagsfeier eines Freundes. Die Stimmung ist ausgelassen, und Schneider erwähnt, dass er eine größere Geldsumme angelegt habe. „Die Rendite ist wirklich gut“, schwärmt er. Ein Bekannter wird neugierig, Schneider nimmt sein Smartphone und will die Seite der BVV Asset Management AG aus der Schweiz zeigen, die Firma, bei der er 450 000 Euro investiert hat. Doch auf dem Bildschirm erscheint eine Warnung der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). „Diese Firma ist nicht berechtigt, Festgeldgeschäfte anzubieten.“ Schneider war geschockt. Es ging um die Ersparnisse von 30 Jahren als Kälteanlagenbauer.

Alles begann mit dem Verkauf eines Hauses. Der Ingenieur wollte den Erlös sicher und gewinnbringend anlegen. Die niedrigen Zinsen der Hausbank frustrieren ihn. Er suchte Alternativen. Ein Link im Internet bringt ihn schließlich auf die Spur der BVV Asset Management AG „Ich habe mich dort angemeldet, um Informationen zu erhalten“, erzählt Schneider. Kurz darauf meldete sich ein Mitarbeiter telefonisch. Die Gespräche wirkten professionell, die Angebote seriös.

Scheider steigt mit 60 000 Euro ein. Es wählt ein Festgeldangebot mit einer Rendite von 4,7 Prozent – nicht spektakulär, aber attraktiv genug, um Vertrauen zu schaffen. „Ich konnte alles online nachvollziehen“, sagt Schneider. „Es gab eine Webseite, auf der ich mich einloggen konnte, und die Ansprechpartner waren immer erreichbar.“ Wenige Wochen später ruft die BVV Asset Management erneut an. Diesmal geht es um eine Festgeldanlage über 200 000 Euro mit knapp sechs Prozent Rendite. Die Beträge würden auf mehrere Banken verteilt und seien zusätzlich versichert. Schneider überweist.

So geht es weiter. Ein Dr. Schmidt, angeblich hochrangiger Mitarbeiter der BVV Asset Management, offeriert ein „exklusives Aktiengeschäft“. Schneider könne früh einsteigen und mit einer Verdopplung seines Einsatzes rechnen – oder im schlimmsten Fall das Geld verzinst zurückerhalten. Klang gut.

Am Ende hat Schneider sein gesamtes Vermögen in drei Anlagen investiert: zwei Festgeldgeschäfte und das angebliche Aktiengeschäft. „Die Dokumente sahen alle echt aus“, sagt er. „Es gab Verträge mit Unterschriften und Stempeln von Banken.“ Und dann saß er da auf dem Geburtstag – wie gelähmt, während die Realität langsam einsickerte.

Die Website: nicht mehr erreichbar. Die Telefonnummern der Firma: tot. Dr. Schmidt verschwunden. Schneider wurde klar: Das Geld ist weg. Seine finanzielle Existenz. Alles, was er besitzt.

Ob die Täter je gefasst werden können oder Schneider sein Geld zurückbekommt, ist unklar. Er macht sich aktuell keine Hoffnungen. Was bleibt: ein gigantischer Verlust: „Das war mein ganzes Leben. Ich wusste nicht mehr weiter. Wenn in dem Moment ein Zug gekommen wäre, hätte ich gedacht: Gut, dann ist es eben vorbei.“

Wenn der Tod Erlösung verspricht

Die Auswirkungen auf sein Leben sind drastisch. „Ich konnte nicht mehr essen, nicht schlafen, nicht arbeiten. In der ersten Woche habe ich fünf oder sechs Kilo abgenommen.“

Um die finanziellen Löcher zu stopfen, verkauft Schneider sein Motorrad und sein Auto. „Ich bin jetzt bei null. Ich kann mein tägliches Leben bezahlen, aber wenn größere Forderungen kommen, weiß ich nicht, was ich machen soll.“ Er beschreibt die Situation als eine, für die es keine Hilfe gibt: „Wenn man Opfer eines Gewaltverbrechens wird, gibt es Anlaufstellen. Aber bei so etwas? Mir wäre lieber gewesen, man hätte mich zusammengeschlagen. Das wäre nach drei Wochen verheilt.“

Gut möglich, dass Schneiders Fall noch auf dem Tisch von Nino Goldbeck landet. Der Oberstaatsanwalt der Zentralstelle Cybercrime Bayern in Bamberg spricht von „einer gnadenlosen Skrupellosigkeit, mit der Geschädigten buchstäblich der letzte Cent aus der Tasche gezogen wird“. Opfer seien um Haus und Hof gebracht worden, Erbschaften hätten sich in Schall und Rauch aufgelöst, und die Betrogenen seien gezielt in die Überschuldung manövriert worden. Neben dem finanziellen Verlust bleiben „immense psychische Schäden“. Goldbeck: „Es gibt Fälle, in denen sich Menschen nach einem solchen Betrug das Leben genommen haben.“

Die Gegner der Strafverfolger sind hochprofessionell: „In einem unserer Ermittlungskomplexe arbeiteten in einem Callcenter in Sofia in der Hochphase mehr als 100 Personen“, erinnert sich der Oberstaatsanwalt. In anderen Fällen waren es sogar mehr als 500 – verteilt auf mehrere Länder. Entsprechend hoch sind die kriminell erwirtschafteten Umsätze. Detektiv Meismann berichtet von Kunden, die Millionen verloren haben.

Neben asiatischen und afrikanischen Staaten sind in Europa Russland und die Ukraine Schwerpunkte der Kriminellen: „Bei vielen dieser Länder gehen die Täternetzwerke vermutlich davon aus, dass die behördliche Aufsicht und die Strafverfolgung weniger streng sind“, so Goldbeck. Das Problem der deutschen Ermittler: An den Tatorten sind sie machtlos. „Wir können dort vor Ort selbst gar nichts unternehmen.“ Alles liege an der Kooperation der Behörden. Nur sei die „internationale Rechtshilfe per se erst einmal ein zähes Geschäft“. Und Russland sowieso außen vor. Allerdings haben ▶

»Ein gesundes Misstrauen ist das A und O«

Tanja Nauschütz, Anwältin für Anlegerschutz und Onlinebetrug

31

Millionen Cyberangriffe gibt es in Deutschland täglich

32

Prozent beträgt die Aufklärungsquote bei Cyberbetrug. Bei Mord sind es 98 Prozent

450

Fälle von Love Scamming gab es in Bayern vergangenes Jahr

Angstmache: Falsche Polizisten werden von Internetbetrügern losgeschickt, um alten Menschen ihre Wertsachen abzunehmen

Im Netz der Betrüger

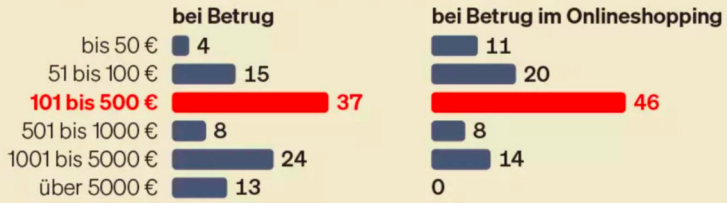
Ob Fake Shops, Datenklau oder Kontaktaufnahme falscher IT-Polizisten, das Internet ist der beste Komplize der Kriminellen

Woher die Cyberangriffe kommen...

Straftaten, die zu Schäden in Deutschland führen

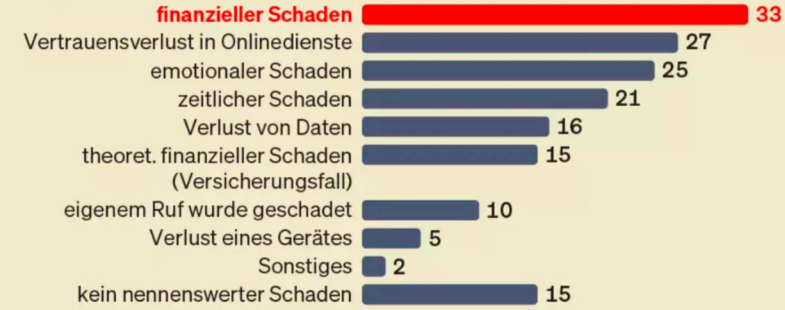
Quelle: BSI

Ist Ihnen durch die Straftat ein Schaden entstanden?
Finanzieller Schaden in Höhe von, Angaben in Prozent, 2025



Der Betrug Bei Summen ab 500 Euro werden die Onlinekäufer vorsichtiger

Welcher Schaden entstand Ihnen durch Onlinebetrug?
Angaben in Prozent, 2025



Der Schaden Die Verbrecher wollen Geld. Die Opfer leiden neben dem finanziellen Verlust nach dem Betrug oft unter psychischen Problemen

Wie schätzen Sie Ihre persönliche Gefahr ein, von Kriminalität im Internet betroffen zu sein?
Angaben in Prozent, 2025

Die Selbstüberschätzung Die meisten Verbraucher fühlen sich sicher im Netz. Vor allem die bis 22-Jährigen und die über 69-Jährigen machen sich keine Sorgen

Gefahrenlage: Wer im Internet kauft, kommuniziert oder Bankgeschäfte erledigt, lockt Betrüger an

sich die Bamberger über die Jahre ein spezialisiertes Netzwerk in vielen Ländern aufgebaut. Das hilft, schneller an Informationen zu gelangen und sich gegenseitig zu unterstützen.

Neben der simplen Lust auf hohe Profite nutzen die Täter auch gern den Wunsch nach Liebe und Sex. Wilfried M., 55, gut situierter Geschäftsmann aus Nordrhein-Westfalen, lernt nach seiner Scheidung im Internet eine attraktive Frau kennen. Audrey erzählt, sie lebe gerade in Afrika. Dort hätte ihr kürzlich verstorbener Vater eine große Plantage betrieben.

Das perfide Spiel mit Gefühlen

Die beiden chatten ein paar Wochen miteinander, die Gespräche werden intimer, die Fotos, die sie schickt, bald auch. Zunächst nur halb nackt, später ganz, rekelt sie sich am Pool hinter dem Herrenhaus auf dem Anwesen. M. ist fasziniert von der Unbekümmertheit und Offenheit seiner Internetbekanntschaft. Und was noch besser ist: Sie scheint mindestens so wohlhabend zu sein wie er. Schließlich wird sie die Ländereien ihres Vaters erben. Dass sie finanziell unabhängig ist, findet M. gut. Er will ja nicht den Sugardaddy spielen und ausgenommen werden.

»Jeden Tag melden sich mindestens zwei neue Klienten, die abgezockt wurden«

Jochen Meismann, Scam-Fahnder, Detektei A-Plus

Und dann kommt das Problem. Nichts Gravierendes eigentlich. Audrey braucht nur Geld für Anwälte und Finanzamt, um die Erbschaft antreten zu können. 150 000 Euro insgesamt. Leider ist sie gerade nicht flüssig, wäre nett, wenn er kurz mal aushelfen könnte. Sobald die Erbsache erledigt sei, komme sie sofort nach Deutschland und zahle alles zurück, denn dann sei sie ja wirklich reich.

M. will erst mal Papiere sehen, bevor er Geld überweist, und einen Ausweis. Beides bekommt er prompt: Kopien der Post vom Gericht, die Korrespondenz mit den Notaren und einen Scan des Passes mit dem vollständigen Namen: Audrey Raines.

Wenn M. ein TV-Serien-Fan wäre, wüsste er vielleicht, dass Audrey Raines der Name einer Figur aus dem beliebten Format „24“ mit Kiefer Sutherland ist. Er weiß es aber nicht und schickt das Geld nach Afrika. Dort wird es plötzlich sehr ruhig. Die reiche Erbin ist verschwunden. Und mit ihr auch das Geld. M. schaltet Detektiv Meismann ein.

Der Scam-Ermittler macht für pauschal 395 Euro einen Basischeck der verschwundenen Dame. Meldedaten prüfen, Rückwärtssuche der Fotos auf Yandex.com, ein paar Telefonate – dann ist Audrey als Fake enttarnt. Alle Infos, alle Briefe, alle Dokumente – gefälscht.

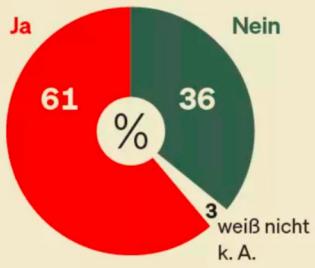
FOTO: MICHAEL KNEISSLER

Das Jedermann-Prinzip

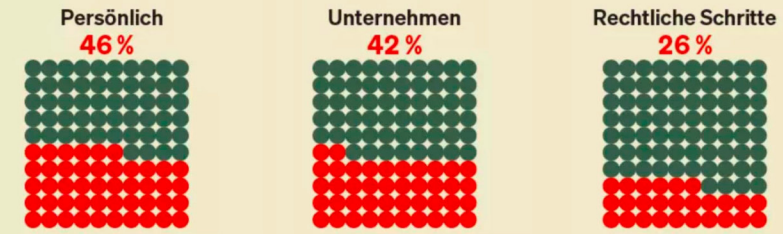
Wer im Internet kauft, wer Mails empfängt, SMS schreibt oder Bankgeschäfte online erledigt: Jeder ist ein potenzielles Opfer für die Kriminellen – und oft bemerkt er es erst zu spät

Quelle: Bitkom, BSI

Die Opfer
Wurden Sie in den letzten 12 Monaten online betrogen?



Die Reaktion
Aus Scham schweigen immer noch viele Betroffene gegenüber der Polizei

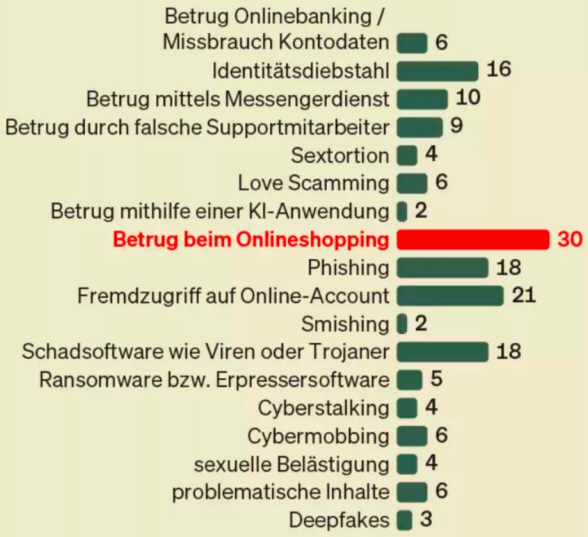


Ich habe das Gespräch mit Freunden oder Familie gesucht

Ich habe das Unternehmen kontaktiert, dessen Plattform für die kriminelle Aktivität genutzt wurde

Ich habe Strafanzeige bei der Polizei erstattet

In welchen Bereichen wird im Internet betrogen?
Angaben in Prozent, 2025



Die Schwerpunkte
Am meisten wird beim Onlineshopping betrogen. Immer öfter kapern Verbrecher auch fremde Onlineaccounts, um etwa einzukaufen und Händler zu betrügen, oder sie installieren Viren, um Daten abzuschöpfen

In diesem Fall vermutlich von den Profis der legendären Black Axe aus Nigeria. Zwölf ihrer Mitglieder stehen gerade in München wegen Bildung einer kriminellen Vereinigung und Geldwäsche vor Gericht. Sie haben zahlreiche Opfer ausgeplündert. Einige haben Haus und Hof verkauft, um ihre Internetliebe zufriedenzustellen.

Die Plattformen ducken sich weg

Angebahnt werden die verhängnisvollen Kontakte auf den namhaften Onlineplattformen. Man tue doch so viel gegen die Verbrecherbanden, behaupten sie. Meta, der Mutterkonzern von Facebook und Instagram, investiert nach eigenen Angaben weltweit Milliarden in KI-basierte Erkennungssysteme und beschäftigt über 40 000 Sicherheitskräfte. Trotzdem hat das Unternehmen massive Probleme mit Onlinekriminalität.

Am 23. Juli reichte der Finanz-Influencer Thomas Kehl mit seinem Unternehmen Finanzfluss Klage gegen Meta beim Landgericht Frankfurt ein. Grund sind mindestens 186 Fake-Accounts, die seinen Namen und sein Bild nutzen, um über Instagram und Facebook Nutzer in betrügerische WhatsApp-Investmentgruppen zu locken. Trotz mehrfacher Meldungen seien viele der Fake-Profile teils über zehn Tage aktiv geblieben, andere wurden kommentarlos abgelehnt. Meta weist die Kritik von sich. Massenhaft aufgebaute Fake-Accounts würden häufig bereits Minuten nach Erstellung gesperrt, erklärt eine Sprecherin.

Wozu diese Profile genutzt werden, weiß der Fotograf Martin G., der auf Instagram Zigtausende Follower hat. Eine davon ist Nathalie W. Ihr gefallen die Fotos so gut, dass sie fast jeden neuen Post kommentiert – und immer mit großer Begeisterung über die gezeigten Porträts von Prominenten.

Aber dann kommentiert sie wieder ein Foto: „Du fotografierst immer noch wunderbar, aber menschlich bist du eine Enttäuschung."

Martin G. kann sich den Sinneswandel nicht erklären und fragt nach. Nathalie W. schickt ihm darauf Screenshots. Sie zeigen einen Fake-Account, der mit seinem Instagram-Namen und Foto operiert. Ein Betrüger hatte seinen Namen gekapert, um mit der Followerin direkt per WhatsApp Kontakt aufzunehmen. Zunächst gingen ein paar nette Nachrichten hin und her – belanglos. Bis der vermeintliche Martin G. eine unverschuldete Notlage schilderte und seine neue Bekanntschaft bat, ihm doch mit etwas Geld auszuhelfen.

Betrüger nutzen jede Plattform, um abzusahnen. Beim Verkaufs- ▶

178,6
Mrd. Euro beträgt der Gesamtschaden für die deutsche Wirtschaft

3398
Euro verlieren die Opfer in Deutschland im Schnitt durch den Betrug

90
Prozent ist die Dunkelziffer bei Internetbetrug. Viele Opfer schweigen aus Scham

portal Kleinanzeigen dominieren Phishing und Vorkassebetrug. Eine besonders ausgeklügelte Abzockmasche ist der sogenannte Dreiecksbetrug. Dabei werden sowohl seriöse Verkäufer als auch Käufer geschädigt: Ein Betrüger bietet zum Beispiel für ein inseriertes Smartphone und bittet den Anbieter um dessen PayPal-Daten. Zeitgleich stellt er das Handy in einer eigenen, gefälschten Anzeige online. Ein möglicher Käufer erhält die Zahlungsinfos des ursprünglichen Verkäufers und glaubt an einen seriösen Deal.

Für kurze Zeit sieht auch alles echt aus: Das Geld fließt tatsächlich auf das Konto des ursprünglichen Verkäufers, der daraufhin das Smartphone verschickt – aber nicht an den Käufer, sondern an die vom Täter angegebene Adresse, oft eine leere Wohnung mit falschem Namen am Briefkasten. Der Ganove kassiert die Ware, der Käufer wartet vergeblich.

Mit Hightech gegen die Betrüger

Um sich gegen den Betrug zu stemmen, nutzt etwa Kleinanzeigen nach eigenen Angaben automatisierte Inseratsvergleiche, SMS-Verifizierung, Zwei-Faktor-Authentifizierung und kontextsensitive Chatwarnhinweise. Vorfälle werden nach Anzeige an Polizei oder Cybercrime-Einheiten weitergeleitet.

Auf ImmoScout24 sind falsche Wohnungsangebote mit Vorkassebetrug ebenso verbreitet wie Identitätsdiebstahl. Kopien von Vermögensnachweisen oder Ausweisen freuen jeden Hacker. Mit einem Frühwarnsystem versucht die Immobilienplattform, solche Betrügereien zu verhindern. Laut Firmenangaben gab es 2024 aufgrund einer speziellen Software 55 Prozent weniger Fake-Inserate als im Jahr zuvor.

Bei den Verbraucherzentralen landen immer mehr Beschwerden. Allein 10 000 über Fake Shops im Jahr 2024. Im Vergleich zu 2023 bedeutet das ein Plus von mehr als 40 Prozent, erklärt der Bundesverband der Verbraucherzentralen. Der Trend setzt sich fort. Im ersten Halbjahr 2025 erfassten die 16 regionalen Verbraucherzentralen knapp 5400 Hinweise zu Fake Shops. Das heißt im Vergleich zum Vorjahr einen weiteren Anstieg um 17 Prozent.

»Die Polizei braucht mehr IT-Fachkräfte«

Marcel Emmerich, Innenexperte, MdB Grüne

9 000 000 000 000

Euro Gesamtschaden entsteht weltweit durch Cyberbetrug

1

Billion Euro davon allein durch Love Scamming

Hinzu kommen 2900 Beschwerden zu erfundenen Dienstleistungen – dreimal mehr als im ersten Halbjahr 2024. Dabei handelt es sich unter anderem um Hilfsangebote bei Nachsendeaufträgen, Führungszeugnissen oder bei Fragen zum Rundfunkbeitrag. „Weil wir so viele Meldungen dazu erhalten, können wir häufig gar nicht intensiver beraten“, sagt Julia Gerhards, Referentin für Verbraucherrecht und Datenschutz bei der Verbraucherzentrale Rheinland-Pfalz.

„Internetbetrug hat in den letzten Jahren in nahezu allen Begehungsformen zugenommen“, betont Günter Krings, Unions-Vizefraktionschef im Bundestag. Neue Gesetze hält er nicht für nötig, die vorhandenen müssten konsequenter angewandt werden. Der Innen- und Rechtsexperte: „Das setzt eine gute Ausstattung der Ermittlungsbehörden voraus, aber noch mehr eine bessere Mitarbeit der Opfer.“ Es sei falsch, aus Scham über die eigene Leichtgläubigkeit von Anzeigen abzusehen.

Der grüne Bundestagsabgeordnete Marcel Emmerich schlägt einen eigenen Straftatbestand für „digitale Beziehungstäuschungen“ vor. „Wenn eine Straftat eine eigene Periodisierung bekommt, wird das auch bei den Ermittlern herausgehoben behandelt werden“, sagt der Innenexperte. Zudem brauche die Polizei mehr IT-Fachkräfte.

Am Ende bleibt die Panik

Selbst erfolglose Betrugsversuche hinterlassen tiefe Spuren. In einem schicken Berliner Altbau lebt der frühere Lehrer Markus H. in einer Parterrewohnung. Davor ein Spielplatz, Sackgasse, man kennt sich, hilft sich. Die Fenster stehen auch mal tagsüber offen. Vorbei. 25 Jahre Grundvertrauen zerstört in gerade einmal 25 Minuten.

So lange dauerte der Anruf eines Kriminellen, der sich als Hauptkommissar Anton Dübelmann ausgab und dessen Komplizen H. zuvor offenbar online ausgeforscht hatten. Dübelmann spielte seine Rolle fast perfekt. Geschickt wechselte er zwischen dem Schüren von Angst und dem Aufbau von Verständnis. „Er erzählte mir, ich stehe auf einer Liste von Einbruchsopfern“, erinnert sich der 79-Jährige.

Der Druck war so groß, dass der falsche Kommissar H. schließlich mit dem Telefon am Ohr durch die Dreizimmerwohnung lotste und sich die Wertsachen aufzählen ließ. Immer wenn der Betrüger Zweifel in der Stimme seines Opfers wahrnahm, verschärfte er den Ton: „Wenn Sie nicht mitmachen, kann ich Ihnen nicht helfen. Die Täter sind bereits in unmittelbarer Nähe.“ Als der Rentner seine beiden Kreditkarten in einen Umschlag stecken und vor seine Eingangstür legen sollte, dämmerte es ihm: Abzocke.

Er legte auf.

Kein finanzieller Schaden. Lob von (echten) Ermittlern. Aufatmen? Nein. Der 79-Jährige ist am Ende. Er schläft kaum noch und wenn, spuken maskierte Räuber durch seine Albträume. Seit zwei Wochen lebt er im Dunkeln. Die Fenster sind verbarrikadiert, bei jedem Schlagen einer Autotür zuckt er zusammen. Letztens lieferte ein Paketbote, den er nicht kannte, im Haus aus. Markus H. erlitt eine Panikattacke: Vielleicht soll er ja doch überfallen werden? Oder die Verbrecher wollen sich rächen – weil er nicht auf sie reingefallen ist?

Nie hätte der 79-Jährige gedacht, dass ihn einmal solche Angst packen könnte. Er muss sogar therapeutische Hilfe in Anspruch nehmen. Geschockt flüstert er: „Ich habe die Krebsdiagnose weggesteckt, mich durch die monatelange Behandlung gekämpft. Aber das“, sagt er, „das ist dreimal schlimmer.“ ■

FOCUS-LESERDEBATTE

Wie sind Sie schon im Internet betrogen worden?

Schreiben Sie uns an leserbriefe@focus-magazin.de

FOTO: DPA

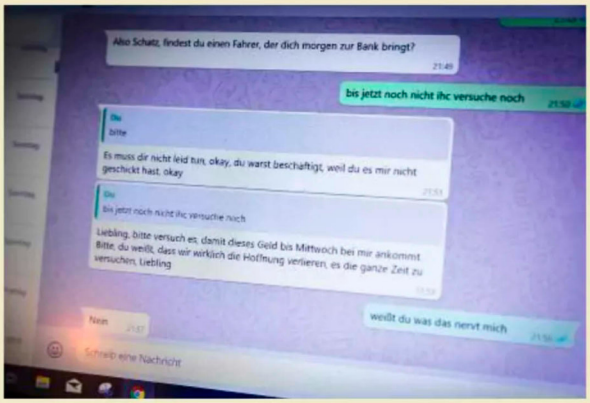
Täuschend echt: die Maschen der Onlinekriminellen

Phishing, Love Scamming, Fake Shops: Im Internet sind die Betrugsmöglichkeiten grenzenlos

Phishing-Mails

Anrede als Warnzeichen Phishing-Mails nennen keine Kundennamen. Banken fordern keine persönlichen Infos

Love Scamming



Zu schön, um wahr zu sein Love Scammer locken mit attraktiven Profilen, schwören ewige Liebe, meiden persönliche Treffen und täuschen schließlich finanzielle Nöte vor

Fake Shops

Echt und doch falsch Statt Qualitätsware liefert bergxperten.de laut Verbraucherzentrale nur Billigschrott aus China

FOTOS: LARS BERG/LAIF

So schützen Sie sich vor Internetbetrug

1. Misstrauisch bleiben
„Ein gesundes Misstrauen ist das A und O", betont Tanja Nauschütz, Anwältin im Bereich Finanzbetrug. Besonders bei unrealistisch hohen Gewinnversprechen sollten Sie aufpassen.

2. Bei der BaFin erkundigen
Bevor Sie Geld anlegen, überprüfen Sie die Plattform. „Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) warnt regelmäßig vor unseriösen Anbietern", so Nauschütz.

3. Keine Zahlungen ins Ausland tätigen
Zwar gibt es natürlich auch seriöse Auslandsanlagen, doch das Betrugsrisiko ist größer. Und: Wenn etwas schiefgeht, fällt es schwerer, das Geld zurückzuholen.

4. Bei Verdacht nichts anmerken lassen
Die Täter beginnen sofort, Beweise zu vernichten, wenn sie das Gefühl haben, ein Opfer hat Verdacht geschöpft. Deshalb raten Experten, sich unmittelbar Hilfe zu holen und die Betrüger im Glauben zu lassen, dass sie nicht aufgeflogen sind. Aber: Zahlen Sie auf keinen Fall weiter.

5. Wenn's passiert ist – schnell handeln!
Betroffene sollten alle Beweise sichern – Screenshots, Überweisungsbelege und E-Mails – und sich so schnell wie möglich auch an spezialisierte Kanzleien wenden. Nauschütz: „Viele Polizeidienststellen sind mit solchen Fällen überfordert."

6. Die Onlinebekanntschaft überprüfen
Checken Sie Fotos mithilfe der Rückwärtssuche auf Google. Geben Sie den angeblichen Namen und andere Informationen Ihres Onlineflirts mit dem Zusatz „Scammer" oder „Liebesbetrüger" in eine Suchmaschine ein.

7. In der Kennlernphase nicht zu viel verraten
Fragen zum Vermögen, Einkommen, Geldanlagen, Schmuck, Auto, Erbschaft, Haus oder Eigentumswohnung sind tabu.

8. Niemals Geld an Fremde schicken
Selbst nach längerem Chatten mit einer Internetbekanntschaft sollten Sie niemals Geld schicken, solange Sie die Person nicht persönlich getroffen haben – auch nicht, wenn diese Ihnen gefühlsduselige Nachrichten schreibt.

9. So wenige Daten angeben wie nötig
„Wir haben in vielen Fällen das Recht, bei Onlinediensten Pseudonyme statt Klarnamen zu wählen", betont Digitalexpertin Julia Gerhards. Vor Datenlecks ist leider niemand zu 100 Prozent sicher. Deshalb gilt: Je weniger Ihrer Daten im Netz kursieren, desto besser.

10. Tools zum Datencheck nutzen
Das Hasso-Plattner-Institut bietet beispielsweise den Identity Leak Checker, mit dem Sie überprüfen können, ob Ihre E-Mail-Adresse in Verbindung mit weiteren persönlichen Daten wie der Adresse oder der Telefonnummer im Internet veröffentlicht wurde.

11. Suchergebnisse scannen
Fake-Dienstleister wie nachsendung-post.de erscheinen oft oben in der Google-Suche. Hier auf den Zusatz „Gesponsert" achten. Es handelt sich dann um kostenpflichtige Anzeigen. Vertrauenswürdiger ist das echte Ranking.

12. Websites gegenrecherchieren
Täter sind mittlerweile oft so professionell, dass Fake Shops nur schwer erkennbar sind. Deshalb lohnt es sich, einen Blick ins Impressum oder sogar ins Handelsregister zu werfen. Außerdem: Sind die Geschäftsbedingungen aufgeführt? Ist die Seite professionell gestaltet? Gibt es negative Erfahrungsberichte?

13. Gütesiegel kontrollieren
Gütesiegel wie Trusted Shops listen vertrauenswürdige Anbieter. Doch Vorsicht: Viele Fake Shops kopieren die Siegel einfach auf ihre Seite. Deshalb besser direkt auf den Seiten der Siegelanbieter gegenchecken.

14. Nicht in Vorkasse gehen
Bei Fake Shops ist Ware meist nur gegen Vorkasse erhältlich. Zudem locken die Seiten mit Rabattaktionen, die zeitlich begrenzt sind. Nutzen Sie nur sichere Bezahlmethoden.

15. Nicht nebenbei shoppen
In der Bahn mal eben per Smartphone eine neue Hose bestellen? Schlechte Idee! Auf Social Media locken Fake Shops die Nutzer mit ansprechenden Anzeigen auf ihre Seiten.