KULTUR NEU ENTDECKEN

SWR KULTUR

Das Wissen

Raffinierter Online-Betrug – Wie wir uns vor neuen Tricks schützen können

Von Frank Drescher

Sendung vom: Montag, 02. September 2024, 8:30 Uhr
Redaktion: Lukas Meyer-Blankenburg
Regie: Günter Maurer
Produktion: SWR 2024

Auf Dating-Apps oder Job-Portalen suchen Online-Betrüger Kontakt zu potenziellen Opfern. Ihre Maschen sind schwer zu durchschauen. Wer betrogen wird, sollte schnellstmöglich handeln.

MANUSKRIPT

Sprecher:
Mit perfiden Methoden zerstören Online-Betrüger die Leben ihrer Opfer. Sie lauern in den sozialen Netzwerken, auf Fake-Shops und Jobbörsen – oder in Dating-Apps, wie im Fall von Laura. Statt der großen Liebe erlebt sie einen Alptraum: Sie gerät ins Visier von Kriminalpolizei und Staatsanwalt. Und eine Bank will 30.000 Euro von ihr. Ihren echten Namen will sie hier nicht hören, das war die Bedingung für das Gespräch mit „Das Wissen“. Die Scham ist groß, wir haben sie für die Sendung nachgesprochen.

Musikakzent

Sprecherin Laura:
Ich bin auf einen Betrug reingefallen, bei dem ich 30.000 Euro Kredit aufgenommen habe, ohne es zu merken. Es ist schrecklich. Man fühlt sich in der Lebensqualität eingeschränkt, weil das einen ja ständig verfolgt, weil man ständig in Austausch steht mit dem Anwalt, man wird ständig mit irgendwelchen Briefen konfrontiert.

Ansage:
Raffinierter Online-Betrug – Wie wir uns vor neuen Tricks schützen können. Von Frank Drescher.

Sprecher:
2023 erfasste das Bundeskriminalamt mehr als 230.000 Betrugsfälle, die über das Internet angebahnt wurden – fast ein Drittel mehr als noch zehn Jahre zuvor. Laura ist eine davon. Ihr Fall zeigt: Die Täter sind skrupellos, ihre Methoden besonders hinterhältig – und darum nur schwer zu erkennen für die Opfer. Doch es gibt Tricks, um ihnen rechtzeitig auf die Schliche zu kommen. Dazu gleich mehr.

Musikakzent

Sprecher:
Lauras Geschichte fängt harmlos an. Sie ist 20 Jahre alt und Single. Auf einer Dating-App entdeckt sie das Profil von einem Mann, der sich Nico nennt. Das Profilbild zeigt einen muskulösen jungen Typen um die 30 auf einer Yacht, hinter ihm nur das Meer. Nico schreibt, er sei ein Start-Up-Unternehmer.

Sprecherin Laura:
Es waren halt relativ authentische Bilder, nicht großartig bearbeitet. Und es war halt einfach eine attraktive Person, wo man halt einfach gesagt hat: Die würde ich gern mal näher kennenlernen und halt gucken, was sich so ergibt.

Sprecher:
Es kommt zum „Match“: Über die Dating-App signalisieren beide, aneinander interessiert zu sein. Schnell schlägt Nico vor:

Zitat Betrüger:
Lass uns mal bitte WhatsApp schreiben. Ist angenehmer für mich.

Sprecher:
Schon hier hätte Laura skeptisch werden können. Wenn das Dating-Match einen anderen Kommunikationskanal vorschlägt, sollte das Anlass zur Vorsicht sein, sagt die Wiener Forscherin Louise Beltzung. Sie arbeitet am Österreichischen Institut für angewandte Telekommunikation, kurz ÖIAT. Dort hat sie das Verhalten von Online-Betrügern untersucht. Um diese anzulocken, hat Louise Beltzung fiktive Profile auf Dating-Apps angelegt.

O-Ton 01 Louise Beltzung, Sozialwissenschaftlerin:
Sie wollten dann von uns in vielen Fällen auch, dass wir unser Profil dort löschen und ihnen dann auch Beweisfotos schicken. Also, das war ein wichtiges Thema, so dieses: „Okay, jetzt hast du ja jemanden gefunden. Und jetzt, bitte zeig mir, dass Du nicht mehr auf Tinder bist.“ Damit sichern sich die Personen, dass wir nicht auf der Plattform selbst danach irgendwie was rückverfolgen können.

Sprecher:
Außerdem versuchten die Betrüger so, etwas Gemeinsames mit ihren Opfern herzustellen, sagt Louise Beltzung. Dazu gehört auch, dass sie mit ihren Opfern erst einmal wochenlang viel über allerlei harmlose Dinge chatten und vielleicht auch mal telefonieren. So stellen sie ein Gefühl der Vertrautheit her. Was Betrüger dabei im Schilde führen, weiß die promovierte Kriminalpsychologin Helga Ihm aus Osnabrück. Das Verhalten von Betrügern gehört zu ihren Spezialgebieten:

O-Ton 02 Helga Ihm, Kriminalpsychologin:
Die Täter, die verfolgen nicht selten die Masche, dass sie ihre zu schädigenden Personen isolieren. Die wollen ja nicht, dass die eine Beratung bekommen. Und die wollen ja nicht, dass die Person, die sie ansprechen, dann sagt: Moment mal, ich gehe mal auf meine Bank, und ich hinterfrage das mal.

Sprecher:
Auch Laura hinterfragt zunächst nicht viel. Ihr gefällt Nico. Er lässt durchblicken, dass er viel Geld mit seinem angeblichen Start-Up-Unternehmen verdient.

Als die beiden eines Abends miteinander chatten, erwähnt er beiläufig, dass er gerade viel Stress in der Firma habe, weil ihm Personal für ein wichtiges Projekt fehle. Ob Laura vielleicht bereit wäre, ihm zu helfen?

Sprecherin Laura:
Was ist das denn für ein Projekt?

Zitat Betrüger:
Wir überprüfen verschiedene Partnerprogramme im Auftrag von den jeweiligen Geschäftsführern. Ist nicht viel eigentlich und würde mir mega helfen. Das Einzige, was du brauchst, ist ein Perso für die Verifizierung zum Schluss.

Sprecherin Laura:
Okay, dann bin ich mal gespannt.

Sprecher:
Laura soll angeblich das Kundendienstpersonal von Online-Banken verdeckt testen und anschließend darüber Berichte verfassen. Sie fragt nach:

Musikakzent

Sprecherin Laura:
Verpflichte ich mich damit zu irgendwas?

Zitat Betrüger:
Natürlich nicht. Keine Sorge.

Sprecher:
Dann schickt der Mann, der sich Nico nennt, Laura einen Arbeitsauftrag. Ein PDF-Dokument mit täuschend echt wirkendem Firmenbriefkopf, komplett mit Bankverbindung und Steuernummer – und der Aussicht auf 75 Euro Aufwandsentschädigung. Das einzig Echte an dem Dokument ist aber nur die E-Mail-Adresse, an die Laura später ihre Test-Berichte schicken wird. Dann fragt „Nico“ sie nach ihrem vollständigen Namen – und auch nach Geburtsdatum, Anschrift, Arbeitgeber, Gehalt und Bankverbindung.

Sprecherin Laura:
Wofür musst Du das denn wissen?

Zitat Betrüger:
Muss es in dem Auftrag eintragen.

Sprecher:
In Wahrheit gibt sich Nico jetzt im Internet als Laura aus. Er legt eine E-Mail-Adresse auf ihren Namen an. Damit beginnt er eine Kontoeröffnung bei der Online-Bank Kontist. Außerdem eröffnet Nico mit der E-Mail-Adresse eine Online-Kreditvermittlung über das Vergleichsportal Check24. Die führt zu einem 30.000-Euro-Online-Kredit der SWK-Bank in Mainz. Laura hingegen schickt er einen zweiten Arbeitsauftrag, für eine angebliche „Kundensimulation“ bei Check24. Laura hat Nico bis dahin nie persönlich getroffen. Sie vertraut ihm trotzdem.

Sprecherin Laura:
Dadurch, dass der sehr sympathisch auf mich gewirkt hatte und ich ja auch hilfsbereit sein wollte, habe ich gedacht, dass ich das ja machen kann. Da war mir aber nicht bewusst, was das auslöst.

Sprecher:
Ist Laura selbst schuld? Vor einem vorschnellen Urteil sollte man sich hüten. Viele Betrüger wissen genau, wie sie ihre Opfer psychologisch manipulieren können, um ihr Vertrauen zu gewinnen, beobachtet Kriminalpsychologin Helga Ihm.

O-Ton 03 Helga Ihm:
Dem Täter geht es darum, das Opfer so schnell wie möglich dazu zu bringen, compliant zu sein, also dieses Ja zu bringen: Ja, ich möchte hilfsbereit sein. Ja, ich möchte dich unterstützen. Wenn er den Eindruck gewinnt, im Rahmen der Kontaktaufnahme, dass es sich um eine Person handelt, die da eine hohe Compliance hat, also eine hohe Willfährigkeit hat, was Gutes zu tun mit dem anderen, was gemeinsam zu tun, dann ist in der Tat der Köder, den der Täter ausgeworfen hat, da ins Volle gegangen.

Sprecher:
Aber noch ist Nico nicht am Ziel. Er hat zwar ein Online-Konto auf Lauras Namen bei der einen Bank beantragt und einen Kredit, ebenfalls auf ihren Namen, bei einer anderen. Jetzt muss er Laura dazu bringen, sich gegenüber den Banken als Kundin zu identifizieren. Dafür verwenden beide Banken das sogenannte Video-Ident-Verfahren.

Dabei müssen Konto- oder Kreditinteressenten erst nach dem Online-Antrag ein Videotelefonat mit einem spezialisierten Dienstleister der Banken führen und ihren Ausweis in die Kamera halten. Das Problem dabei: Diese Reihenfolge im Verfahren begünstigt Betrug. Denn die Auftragsbestätigungen der Banken sind an Nico gegangen – also an jemand anderen, als die Banken annehmen. Aber die Auftragsbestätigungen enthalten die Zugangsdaten für das Video-Ident-Verfahren. Und die können Betrüger dann ihren Opfern weitergeben und sie glauben machen, dass diese Zugangsdaten einem ganz anderen Zweck dienen würden.

Wegen dieser Betrugsanfälligkeit steht das Video-Ident-Verfahren seit Jahren in der Kritik von Sicherheitsfachleuten, wie das SWR-Verbrauchermagazin Marktcheck enthüllt hat. Trotzdem will die Finanzaufsichtsbehörde BaFin vorerst daran festhalten.

So kann Nico Laura weismachen, er gebe ihr die Zugangsdaten für den verdeckten Service-Test im Auftrag seiner Firma. Ein guter Betrüger erzählt immer auch eine gute Geschichte, sagt Kriminalpsychologin Helga Ihm.

O-Ton 04 Helga Ihm:
Wenn Täter den Weg wählen über die Dating-Plattformen, damit sie Leute dazu bringen, ihnen eine Vermögensverfügung zu Geld zu geben, dann müssen sie hier ja mit einer gewissen Geschichte kommen. Sie nehmen ja Kontakt zu diesem Menschen auf. Dann müssen Sie irgendeine Geschichte präsentieren, die in der zu schädigenden Person auch eine gewisse Vorstellung hervorruft, also gewisse Illusionen hervorruft.

Sprecher:
Die Illusion in Lauras Fall ist: ihre Annahme, verdeckte Kundenservice-Testerin zu sein. Nun kündigt Nico Laura an, dass bald 30.000 Euro auf ihrem Girokonto eingehen werden.

Zitat Betrüger:
Für die Rücküberweisung habe ich Dir ein einmaliges Konto bei uns eingerichtet. Verwendungszweck: privat. Bitte 29.500 Euro zurücküberweisen. 500 Euro sind für Dich. Für Deine Hilfe. Als Empfänger bitte Deinen Namen nehmen, damit das zugeordnet werden kann. Sollte Deine Bank bei Dir anrufen und fragen, ob das so passt, sagst: „Ja, das passt“. Sagst halt, ist Dein zweites Konto.

Sprecher:
Die Verhaltensmaßregel dient dazu, die Sicherheitsvorkehrungen von Lauras Hausbank zu umgehen. Und bei dem Konto, von dem er spricht, handelt es sich um das, das Laura bei Kontist im Rahmen ihres vermeintlichen Jobs für Nicos Scheinfirma eröffnet hat – und auf das nur Nico Zugriff hat. – Laura überweist die 29.500 Euro dorthin. Danach überweist Nico 7.500 Euro nach Litauen. Dann schlagen die Geldwäschemechanismen bei der hinter Kontist stehenden Solarisbank Alarm, die restlichen 22.500 Euro werden sichergestellt. Und bei Laura ruft die Kriminalpolizei an.

Sprecherin Laura:
Ich konnte in dem Moment gar nichts mehr sagen. Mir sind nur die Tränen aus den Augen gekommen. Ich hab’ dann nur gesagt: ‚Ich ruf‘ zurück.’ Ich bin dann einfach nur aus meiner Arbeitsstelle raus, bin in Tränen ausgebrochen und ich dachte wirklich, die Welt geht unter. Es war wirklich ganz, ganz schlimm.

Sprecher:
Zum Stress mit der Polizei kommt für Laura die Scham, einem Betrüger aufgesessen zu sein. Viele Betrugsopfer machten sich selber Vorwürfe. Schließlich würden Verbraucherschützer ständig davor warnen, private Daten Unbekannten zu überlassen. Diese Scham hemmt viele Betrugsopfer, Hilfe zu suchen. Das scheint insbesondere für Männer zu gelten, vermutet Elvira Pfleiderer. Sie ist Mitglied im Arbeitskreis der Opferhilfen in Deutschland und arbeitet als Traumapädagogin beim Verein Seehaus aus Leonberg. Der hilft Verbrechensopfern mit den Folgen der Tat zurechtzukommen. Die Betrugsgeschädigten, die bei ihr Rat suchen, sind ausnahmslos Frauen.

O-Ton 05 Elvira Pfleiderer, Traumapädagogin:
Ich denke, die Dunkelziffer im Bereich von Betrugsopfern liegt sehr, sehr hoch, weil eben dieses Schamgefühl so hoch ist. Und da glaube ich, dass eben Männer nochmal eine Stufe höher, dieses Schamgefühl ist, dass man Opfer von einem Betrugsdelikt geworden sind. Es gibt ja sehr, sehr unterschiedliche Betrugsdelikte. Und auch Männer sind natürlich von Betrugsdelikten betroffen.

Sprecher:
Die Geschädigten schwerer Betrugsfälle haben in der Regel lange mit den Folgen zu kämpfen und finden oft nur schwer Hilfe, beobachtet Traumapädagogin Elvira Pfleiderer.

O-Ton 06 Elvira Pfleiderer:
Das ist ein langer und sehr, sehr schmerzhafter Prozess, weil so viel auch in diese vermeintliche Beziehung ja investiert wurde und es zu akzeptieren, dass man betrogen wurde. Und dass diese Beziehung überhaupt nicht besteht. Dass das eine Betrugsstrategie war, das ist oft auch sehr, sehr schmerzlich und auch ein längerer Prozess und um überhaupt bereit sein, daran zu arbeiten, muss ich ja erst einmal akzeptieren, dass ich Opfer eines Betrugsdeliktes geworden bin.

Sprecher:
Manche Opfer entwickeln auch Schuldgefühle, weil sie glauben, selbst an dem Betrug mitgewirkt zu haben. Zu Unrecht, sagt Kriminalpsychologin Helga Ihm.

O-Ton 07 Helga Ihm:
Schuld, denke ich, ist da das falsche Mittel, mit dem man arbeitet. Schuld sind die Täter, die das initiieren. Betrug ist ja so definiert, dass die Interaktion zwischen Täter und Opfer zum Erfolg des Täters führt, weil er Täuschungshandlungen einsetzt. Aber dass Täuschung funktioniert, das sind eben die psychologischen Mechanismen von uns Menschen.

Sprecher:
Angesichts der Vielzahl von Online-Betrugsfällen hat sich die Wiener Forscherin Louise Beltzung gefragt, warum die üblichen Verbraucherschutz-Warnungen vor der Datenweitergabe an Unbekannte oft ins Leere laufen. Ein wichtiger Aspekt: Betrüger agierten immer professioneller, sagt sie, es handele sich um hochgradig organisierte Kriminalität.

O-Ton 08 Louise Beltzung:
Da geht es um mehr als nur eine gutgemachte Website oder ein gut gestaltetes E-Mail. Da wird wohl Bindung aufgebaut zwischen Kriminellen und den Opfern. Und uns war wichtig, ein besseres Verständnis zu haben dafür, was zwischen diesen Personen passiert oder was da aufgebaut wird. Ein Verhältnis, um besser auch mit Prävention sich einklinken zu können und besser intervenieren zu können und den Schaden sozusagen zu minimieren.

Musikakzent

Sprecher:
Darum hat Louise Beltzung gemeinsam mit ihrer Kollegin Julia Krickl fiktive Profile auf Dating-Apps eingerichtet, um sogenannte „Love-Scammer“, also: Liebesbetrüger, anzulocken. Schnell erhielten die Forscherinnen Matches mit verdächtigen Anfragen. Obwohl die Männer jeweils vorgaben, schwer beschäftigte Manager zu sein, Krypto-Investoren oder Unternehmer, die wegen ihrer Arbeit nie Zeit für ein persönliches

Treffen hätten, reagierten sie stets erstaunlich schnell auf Chat-Nachrichten. Wer also bei Flirtpartnern einen solchen Widerspruch zwischen Reden und Handeln bemerkt, könnte ahnen, dass da etwas im Argen liegt. Julia Krickl:

O-Ton 09 Julia Krickl, Sozialwissenschaftlerin:
Was wir wissen von gewissen Scam-Fabriken in Südostasien ist, dass quasi ein Fake-Profil aufgebaut wird, und über dieses Fake-Profil kommunizieren die Opfer mit unterschiedlichen Tätern. Das heißt, es gibt unterschiedliche Personen, die dieses eine Fake-Profil aufrechterhalten und da dann auch einfach immer ansprechbar sind.

O-Ton 10 Louise Beltzung:
Und ich glaube, das ist der wichtige Punkt, dass viele dieser Scammer, mit denen wir gesprochen haben oder geschrieben haben, aber durchaus sehr bemüht waren, sehr nett waren, sehr individualisiert angesprochen haben und sich die Zeit genommen haben, ein Verhältnis mit uns aufzubauen oder eine Beziehung mit uns aufzubauen, die noch nicht von Anfang an wollte, dass wir etwas investieren, das heißt, das kam erst mit der Zeit.

Sprecher:
Einige der dabei entstandenen Chat-Dialoge haben Louise Beltzung und Julia Krickl mit „Das Wissen“ geteilt. Sie geben Aufschluss darüber, woran sich mutmaßliche Betrüger rechtzeitig erkennen lassen – und ermöglichen so den Schutz vor neuen Tricks.

Beispiel 1: Um sicherzugehen, dass Sie es mit einer echten Person ohne betrügerische Absichten zu tun haben, bitten Sie die Person um ein persönliches Date.

Sprecherin Zitat:
Was ich jetzt wirklich brauch', ist eine Umarmung oder eine starke Schulter zum Anlehnen.

Sprecher 2 Zitat Betrüger:
Ja, das versteh' ich. Aber wenn ich mich nicht zuerst um meine Arbeit kümmere, kann ich mich nicht uneingeschränkt um dich kümmern. Das wäre respektlos dir gegenüber. Gib mir Zeit, Liebes.

Sprecher:
Wer immer wieder um Aufschub bittet oder Ausreden dafür sucht, warum ein persönliches Date gerade nicht möglich ist, ist verdächtig.

Beispiel 2: Bitten Sie Ihre Kontaktperson um ein Videotelefonat. Auch die Forscherinnen Louise Beltzung und Julia Krickl taten das bei ihrer Untersuchung und erlebten Betrüger, die ihnen mit den verrücktesten Ausreden kamen, weshalb ein Videotelefonat gerade nicht möglich sei. Einer etwa meinte, seine Schwester sei während ihres gemeinsamen Videochats mit ihm mit ihrem Auto tödlich verunglückt. Daher sei er nicht mehr zu Videotelefonaten imstande.

Sprecherin Zitat:
Das tut mir so leid.

Sprecher 2 Zitat Betrüger:
Ich kann das Lächeln meiner Schwester während des Videocalls nicht vergessen.

Sprecher:
Kommt ein Videotelefonat wiederholter Nachfragen zum Trotz nicht zustande, nehmen Sie lieber Abstand.

Beispiel 3: Die Kontaktperson bringt das Thema Kryptowährungen ins Spiel und schwärmt Ihnen vor, wie leicht sich damit angeblich Geld verdienen lasse.

Sprecherin Zitat:
Arbeit nervt.

Sprecher 2 Zitat Betrüger:
Such dir einen Nebenjob, wie ich mit Kryptowährungen. Ich kann dir einfach helfen, Süße. Dir zeigen, wie du Gewinn machen kannst. Ich manage deinen Account einfach.

Sprecher:
Die Aussicht auf schnell und leicht zu machendes Geld lockt viele. Hier sollte man besonders vorsichtig sein – selbst dann, wenn Sie den Eindruck haben, schon viel Zeit mit einer Person im Chat verbracht zu haben und meinen, diese zu kennen. Was den hier vorgestellten, verkürzten Chat-Auszügen voranging, waren oft wochenlange Plauder-Chats über alltägliche Themen. So stellen Betrüger sicher, dass sie aus Sicht der Opfer keine Unbekannten mehr sind. Die Ausreden und Versprechungen, die hier in der verkürzten Version oft abseitig und leicht durchschaubar wirken, erscheinen so viel weniger zweifelhaft. Kriminalpsychologin Helga Ihm:

O-Ton 11 Helga Ihm:
Je häufiger der Kontakt oder je besser der Kontakt gestaltet wird, je sympathischer man sich gegenseitig wird, umso wahrscheinlicher wird's auch, dass die Person zum Schluss bereit ist, die wahren Absichten des Täters zu befriedigen, indem es dann zur Übergabe kommt, entweder von Geldmitteln oder hier haben sie ja erzählt, dass der Täter hier auch so gewisse Umwege geht, dass er erst mal die Personalien haben möchte und man zum Schluss merkt: Hoppla, das war ich ja gar nicht. Also schon ein perfider Weg, Kontakt zu einem Menschen aufzunehmen.

Musikakzent

Sprecher:
Aber auch ein sehr zeitintensiver Weg. Viele Kriminelle versuchen daher, schneller an die persönlichen Daten ihrer Opfer zu gelangen: Etwa durch fingierte Stellen- oder Wohnungsinserate. Hier gilt es, vor dem Versand von Bewerbungsunterlagen zu klären: Haben Sie von der Firma schon einmal gehört? Hat sie eine Webseite? Lässt

sich die dort angegebene Anschrift in einem Kartendienst wie Google Maps finden? Zeigt das Satellitenbild irgendwelche Auffälligkeiten?

Und falls Sie trotzdem einen Reinfall erleben: Behalten Sie die Nerven. Lassen Sie den Betrüger im Unklaren darüber, dass Sie den Betrug bemerkt haben. Löschen Sie nichts von Ihren elektronischen Geräten. Gehen Sie erst zur Polizei. Und dann direkt zur nächsten Verbraucherzentrale. Oft lässt sich unmittelbar nach Vollendung des Betrugs noch manches Übel schneller abwenden als später. – Hinweise, die Sabine vielleicht geholfen hätten. Betrüger haben sie, die so wie Laura nur in dieser Folge von Das Wissen so heißt, dazu gebracht, dreimal das Video-Ident-Verfahren bei zwei Banken zu durchlaufen. Jetzt hat sie Kredite im Wert von 55.000 Euro am Hals – und steht vor der Privatinsolvenz. Was besonders an ihr nagt: Sie arbeitet im Finanzsektor – und hat das Unheil trotzdem nicht kommen sehen:

Sprecherin Sabine:
Ich hätte niemals damit gerechnet. Also wirklich, dass... ich kann das bis heute nicht begreifen, dass ich so gehandelt habe, dass ich so viel von mir preisgegeben habe. Und ich kann das bis heute nicht verstehen.

Sprecher:
Sabine hatte im Internet auf ein Werbebanner geklickt, das mit einem geheimen Geldanlagesystem lockte – angepriesen als Geschäftsidee aus der Fernseh-Show „Die Höhle der Löwen“. Deren Juroren hätte das System angeblich so überzeugt, dass sie es geheim halten würden und deshalb die Ausstrahlung der Sendung verhindert hätten. Eine frei erfundene Geschichte. Aber Sabine wird neugierig und hinterlässt ihre Mailadresse und Mobilnummer. Bald meldet sich ein angeblicher Finanzberater bei ihr, Matthias D. Schon mit einer Investition von 251 Euro könne Sabine das System nutzen, das angeblich automatisch durch An- und Verkauf von Kryptowährungen Gewinne erziele.

Sprecherin Sabine:
Das schien mir eigentlich ganz... ja, risikofrei zu sein, weil ich ja nur diese 251 Euro investieren wollte, nur, um das mal auszuprobieren.

Musikakzent

Sprecher:
Das Geld überweist Sabine nach Litauen. Daraufhin erhält sie die Zugangsdaten für die angebliche Krypto-Investmentplattform und kann zusehen, wie sich der Wert ihrer vermeintlichen Investition innerhalb weniger Wochen erst auf 2.700 Euro mehr als verzehnfacht – und ein paar Wochen später völlig durch die Decke geht, auf 55.000 Euro.

Sprecherin Sabine:
Mir war das alles so überhaupt gar nicht geheuer. Und ich habe gesagt, ich möchte gerne aussteigen.

Sprecher:
Die Betrüger verleiten sie dazu, sich dem Video-Ident-Verfahren zu unterziehen. Die Banken, bei denen sie das machen soll, seien die Partnerbanken des geheimen Krypto-Investment-Systems, heißt es. Die Betrüger instruieren Sabine, das Geld weiter zu überweisen – angeblich auf ein Konto der britischen Finanzaufsicht, wegen einer vermeintlichen Liquiditätsprüfung. Sabine erstattet Anzeige, aber die führt nicht zur Ergreifung eines Tatverdächtigen. Die Erfahrung, betrogen worden zu sein, der Schuldenberg und die Aussicht auf die Privatinsolvenz haben sie krank gemacht.

Sprecherin Sabine:
Ich habe mich so geschämt. Ich habe das niemanden erzählt, niemanden. Und dadurch totale Stressreaktionen gehabt. Also: Konnte nicht mehr schlafen, hatte Hautausschläge, Kopfschmerzen, Bauchschmerzen. Also, es ging mir richtig schlecht, und das war so schlimm, dass ich also auch depressiv wurde.

Sprecher:
Sabine hat auch versucht, einen Anwalt einzuschalten. Doch der erste, den sie fragte, wollte 3.400 Euro Vorschuss, der zweite 680 Euro pro Stunde. Bei der öffentlichen Rechtsauskunft an ihrem Wohnort Hamburg erfährt sie: Gegen die Banken komme sie nicht an. Diese Hilflosigkeit sei eine leider häufige Erfahrung von Betrugsgeschädigten, sagt Elvira Pfleiderer.

O-Ton 12 Elvira Pfleiderer:
Diese Erfahrung, die die Sabine leider machen musste, ist eine Alltagserfahrung nach einem Betrugsdelikt. Wo bekomme ich jetzt überhaupt Hilfe? Dann sind Menschen neben sehr häufig auch in einer finanziellen bis existenziellen Not wie bei der Sabine.

Sprecher:
Sabine geht deswegen zur Psychotherapie. Laura wiederum geriet ins Visier der Strafverfolger, obwohl sie eigentlich die Betrogene ist. Sie fand einen Anwalt, der sie erfolgreich in dem Strafverfahren wegen Geldwäsche gegen Laura verteidigte.

O-Ton 13 Roland Wenzel, Rechtsanwalt:
Unsere Mandantin hat halt in der Sache überhaupt nicht gewusst, dass ein Vertrag abgeschlossen werden soll, sondern das war ja aus ihrer Sicht eine ja ein testweiser Kontakt, wo sie als Testpersonen fungierte und eben darauf achten sollte, dass das jeweilige Gegenüber eben die richtigen Fragen stellt und die richtigen Aufklärungen vornimmt. Und das war halt ausdrücklich als Testkauf oder Testkontakt ihr so erklärt worden. Und deswegen war für sie vollkommen klar, dass in der Sache überhaupt kein Vertrag geschlossen wird.

Sprecher:
Lösen ließe sich der Fall wohl, wenn das sichergestellte Geld an die kreditgebende Bank zurückfließen würde. Dass das immer noch nicht passiert ist, zeigt auch, wie schwer sich Strafverfolger mit solchen Online-Betrugsfällen tun. Die Täter agieren im

Netz und oft international. In Deutschland wird es mit der Strafverfolgung manchmal schon schwer, wenn mehrere Bundesländer eingebunden sind – wie in Lauras Fall.

Sprecherin Laura:
Im Endeffekt schwebt man halt die ganze Zeit in einer Unsicherheit. Man weiß halt nicht: Werden die 22.000 Euro freigegeben? Man macht sich halt immer Gedanken darüber, dass man vielleicht sogar Probleme mit dem Arbeitgeber bekommt, weil im Endeffekt drohen die jeden Monat mit einer Lohnpfändung.

Sprecher:
Unterdessen können der oder die Täter unbehelligt weitermachen. Dabei haben sie Spuren hinterlassen: Eine führt nach Bayern zu einem Büroservice für Briefkastenfirmen. Eine andere ist der in Deutschland registrierte E-Mail-Server, an den Laura ihre Testberichte schickte. Für den Server muss jemand Registrierungsgebühren bezahlt haben. Doch die Staatsanwaltschaft Koblenz hat diese Spuren nicht verfolgt. Warum? Auf Anfrage von „Das Wissen“ erklärt sie:

Zitat:
Nach allgemeiner kriminalistischer Erfahrung bestehen diesbezüglich auch keine Erfolgsaussichten, einen Täter ermitteln zu können, da die Täter wie in sämtlichen gleichgelagerten Fällen, hochprofessionell aus dem Ausland agieren und zur Registrierung falsche Personalien verwenden.

Sprecher:
Lauras Anwalt Roland Wenzel hat dafür wenig Verständnis.

O-Ton 14 Roland Wenzel:
Die Staatsanwaltschaft hat einfach die notwendigen Ermittlungsschritte, um hier auf die tatsächlichen Betrüger zu kommen, gar nicht gemacht. Und dann zu sagen: „Ja, wahrscheinlich werden wir die gar nicht ermitteln können. Deswegen probieren wir es erst gar nicht“, halte ich gerade im Hinblick auf diese Art und Weise der Kriminalität auch teilweise für gefährlich, weil die Täter natürlich merken, uns droht hier gar keine Verfolgung.

Sprecher:
Wie „Das Wissen“ aus Polizeikreisen erfahren hat, liegt das auch an der schieren Menge der Online-Betrugsfälle. Sie überfordert die Strafverfolger. – Online-Betrug ist ein weit verbreitetes Phänomen geworden. Die offizielle Zahl an Betrugsfällen zeigt vermutlich nur einen Teil der tatsächlichen Betrugsdelikte an. Viele Betroffene trauen sich aus Scham oft nicht, Hilfe zu suchen. Oder sie wissen schlicht nicht, an wen sie sich wenden sollen. Hierfür gibt es in den meisten Bundesländern mittlerweile Opferberatungsstellen, die weiterhelfen können. Online gilt der Grundsatz: persönliche Daten, wie den vollen Namen, die Anschrift oder die Personalausweisnummer, niemals weiterzugeben an Personen, die man nicht persönlich aus der analogen Welt kennt. Wer den Verdacht hat, betrogen zu werden, sollte den oder die Betrüger darüber im Unklaren lassen, keine Chatverläufe oder Dokumente von den eigenen elektronischen Geräten löschen und zur Polizei gehen sowie zur nächsten Verbraucherzentrale. Oft lässt sich unmittelbar nach Vollendung des Betrugs noch manches Übel abwenden.

Abspann:

Das Wissen (mit Musikbett)

Sprecher:
Raffinierter Online-Betrug. Von Frank Drescher. Sprecher: Barbara Stoll. Redaktion: Lukas Meyer-Blankenburg. Regie: Günter Maurer.

Abbinder