ONLINE-FINANZBETRUG UND ABZOCKE IN EINER WELT DER KÜNSTLICHEN INTELLIGENZ

BLEIBEN SIE WACHSAM UND SCHÜTZEN SIE SICH

Online-Finanzbetrug und Abzocken sind nicht neu, aber künstliche Intelligenz (KI) hat sie intelligenter und schwerer zu erkennen gemacht. Kriminelle verwenden jetzt gefälschte Nachrichten und Websites, falsche Promi-Profile und sogar KI-generierte Stimmen oder Videos, die wie Ihr Banker, Ihre Freunde oder Ihre Familie aussehen, um Sie zu betrügen.

Sie erreichen Sie oft über soziale Medien, Messaging-Apps, E-Mails und unerwartete Anrufe, die echt klingen.

Sie können Risiken wie finanzielle Verluste, Identitätsdiebstahl und emotionale Belastungen ausgesetzt sein. Seien Sie vorsichtig und folgen Sie diesen wichtigen Tipps, um sicher zu bleiben:

Bleiben Sie wachsam gegenüber bestehenden Online-Finanzbetrug und Betrugsversuchen, die durch KI betrieben werden, z. B. Imitation, Phishing, Investment- und Versicherungsbetrug und sogar Liebesbetrug und Abzocke. Weitere Information über die verschiedenen Arten von Betrug und Abzocken erfahren Sie auf den Seiten 5, 6 und 7.

Und über Betrug und Abzocken, die spezifisch für Krypto sind, im Factsheet über Krypto Betrügereien und Abzocken ( ).

Erkennen Sie Warnzeichen: Lernen Sie, verdächtige Verhaltensweisen, Nachrichten oder Angebote zu erkennen (Seite 2).

Schützen Sie sich: Sichern Sie Ihre personenbezogenen Daten (Seite 3).

Wissen, was zu tun ist, wenn Sie Opfer von Betrug oder einer Abzocke werden (Seite 4).

Warnzeichen

Ein Versprechen, das zu gut scheint, um wahr zu sein.

Ein unerwarteter Anruf von einer unbekannten Nummer.

Eine dringende Anfrage nach Geld oder persönlichen Informationen, einschließlich von jemandem, der vorgibt, ein Familienmitglied, ein Freund oder sogar ein Prominenter zu sein.

Eine Anfrage, um die Kontrolle über Ihr Gerät zu übernehmen, eine App herunterzuladen, einen QR-Code zu scannen oder auf einen Link zu klicken.

Eine Anfrage nach persönlichen Informationen oder Bankdaten (z. B. Passwörter, Kreditkartennummern, Internet-Banking-Anmeldeinformationen oder Sicherheitscodes).

Antrag auf Zahlung über nicht nachweisbare Wege (z. B. Kryptos, Geschenkkarten, Überweisungen oder Prepaid-Debitkarten).

Eine verdächtige oder falsche E-Mail-Adresse oder ein Link (z. B. Rechtschreibfehler in der URL oder ungewöhnliche Webadressen).

Ein Anhang aus einer unbekannten Quelle, insbesondere .exe, .scr, .zip oder eine makroaktivierte Office-Datei (.docm, .xlsm).

Schlechte Grammatik oder Formatierung in einem offiziell aussehenden Dokument, obwohl KI es Betrügern ermöglichen kann, diese Fehler effektiver zu verstecken.

Eine Website, die professionell aussieht, aber keine verifizierten Kontaktdaten oder Firmenregistrierungs-informationen hat.

Intonation, die unnatürlich klingt, keine Pausen hat und übermäßig fließend oder robotisch wirkt. Achten Sie auf das „Klonen von Stimmen“, obwohl KI-generierte Sprache auch sehr natürlich klingen kann.

Videos, bei denen die Stimme robotisch oder übermäßig glatt klingen kann, Lippenbewegungen und Gesichtsausdrücke können mit der Sprache falsch ausgerichtet sein, oder Hintergrund, Beleuchtung und Schatten können inkonsistent sein. Dies sind oft KI-generierte Videos (Deepfakes).

Schritte, um sich zu schützen

1 **Teilen Sie niemals persönliche oder Bankinformationen:**

Legitime Unternehmen werden niemals nach Ihren PINs, Passwörtern, Internet-Banking-Anmeldeinformationen oder Sicherheitscodes per E-Mail, Text, Social Media oder Telefon fragen.

2 **Nehmen Sie sich Zeit und denken Sie nach, bevor Sie handeln:**

Beeilen Sie sich nicht, Geld zu senden, Informationen auszutauschen oder auf Links zu klicken. Betrüger schaffen absichtlich ein Gefühl der Dringlichkeit (z. B. IT-Probleme mit Ihrer Bank, Notrufe mit Ihren Freunden und Familienmitgliedern, bedrohliche Sprache usw.). Bei Zweifeln, auch wenn sie geringfügig sind, handeln Sie nicht: Beenden Sie den Anruf und überprüfen Sie die Quelle oder Identität sorgfältig.

3 **Überprüfen Sie die Quelle/Identität sorgfältig:**

- Überprüfen Sie immer, woher Nachrichten, Anrufe, E-mails und Links kommen- auch wenn sie offiziell aussehen, von einem Freund oder ihrer Familie oder sogar einer öffentlichen Figur zu kommen scheinen. Rufen Sie beispielsweise Ihre Familie und Freunde mit einer bekannten Nummer über einen vertrauenswürdigen Kanal an oder schreiben Sie eine SMS. Nach Rechtschreibfehlern, seltsamen URLs oder fehlenden Sicherheitsindikatoren suchen (z. B. überprüfen, ob der Website-Link ein „s“ in „HTTPS“ enthält, um sicherzustellen, dass die Website sicher ist, und nach hinzugefügten oder fehlenden Buchstaben im Firmennamen suchen).

- Öffnen Sie keine Links aus unerwünschten Nachrichten, installieren Sie nur offizielle Applikationen über vertrauenswürdige App-Stores und scannen Sie keine unbekannten QR-Codes.

- Vereinbaren Sie mit Ihrer Familie ein „sicheres Wort“- eine geheime Phrase, mit der Sie Ihre Identität bestätigen können, wenn jemand mit einer vertrauten Stimme Sie mit einer dringenden Bitte um Geld anruft und behauptet, ein Familienmitglied zu sein (z. B. Eltern, Schwester/Bruder, Kind).

- Verwenden Sie verifizierte Kontaktdaten, um das Unternehmen oder die Person direkt zu erreichen, und verlassen Sie sich niemals auf die Kontaktinformationen des mutmaßlichen Betrügers (z. B. unabhängige Suche nach dem Firmennamen, Verwendung verifizierter Geschäftsverzeichnisse, zuvor bestätigte Kontaktmethoden). Betrüger können behaupten, zugelassen zu sein oder die Internetseite eines zugelassenen Unternehmens nachzuahmen. Prüfen Sie, ob von Ihrer nationalen Finanzbehörde Warnungen ausgesprochen oder in die I-SCAN-Liste der IOSCO (iosco.org/i-scan/) aufgenommen wurden. Überprüfen Sie bei Kryptoanbietern, ob sie in der EU zugelassen sind (z. B. im ESMA-Register ( ).

4 **Achten Sie auf mögliche KI-Tricks:**

Mit fortschreitender KI-Technologie werden Betrügereien überzeugender denn je- auch mit den besten Sicherheitstipps. Wenn sich etwas ungewöhnlich anfühlt oder Sie eines der oben beschriebenen Warnzeichen erkennen, halten Sie inne und bewerten Sie es erneut.

5 **Installieren Sie niemals Fremdzugriffssoftware oder teilen Sie niemals Ihren Bildschirm:**

Banken und Finanzinstitute werden dies niemals von Ihnen verlangen.

6 **Sichern Sie Geräte und Konten :**

Verwenden Sie starke und eindeutige Passwörter, halten Sie sie geheim und vermeiden Sie die Wiederverwendung derselben Anmeldeinformationen auf verschiedenen Plattformen. Aktivieren Sie nach Möglichkeit die Multi-Faktor-Authentifizierung. Hier finden Sie einige Passwörter-Tipps ( ). Halten Sie Ihre Software und Ihren Antivirenschutz auf dem neuesten Stand und aktiviert.

7 **Seien Sie vorsichtig mit unerwarteten und zeitlich begrenzten Investitionsmöglichkeiten:**

Wenn es zu gut klingt, um wahr zu sein, dann ist es das wahrscheinlich auch.

8 **Denken Sie nach, bevor Sie Informationen in sozialen Medien teilen:**

Chat-Gruppen, Foren, Social-Media-Beiträge und Fotos können wertvolle Wissensquellen für Betrüger sein. Wenn Sie zu viel über sich selbst oder Ihre Investitionen preisgeben, können Sie ein einfaches Ziel sein.

Was tun, wenn Sie Opfer von Betrug oder Abzocke geworden sind?

Stoppen Sie sofort Transaktionen,

Um weitere Überweisungen auf verdächtige Konten zu blockieren und zusätzliche Verluste zu vermeiden. Stoppen Sie jeden Kontakt mit den Betrügern – ignorieren Sie ihre Anrufe und E-Mails und blockieren Sie den Absender.

Wenden Sie sich an Ihre Bank oder Ihr Finanzunternehmen:

Informieren Sie Ihre Bank oder Ihr Finanzunternehmen sofort über offizielle Kontaktkanäle, um Optionen zum Einfrieren oder Rückgängigmachen von Transaktionen zu erkunden.

Ändern Sie Ihre Passwörter auf allen Ihren Geräten und Apps/Websites.

Betrüger kaufen durchgesickerte Passwörter online und probieren sie auf mehreren Konten aus. Nur ein Passwort zu ändern, reicht nicht aus. Stellen sie sicher, dass sie alle geändert werden, damit Betrüger sie nicht wiederverwenden können.

Meldung und Warnmeldung:

Melden Sie den Vorfall der Polizei sowie gegebenenfalls der CSSF (https://www.cssf.lu/de/) und informieren Sie Ihr Netzwerk (z. B. Freunde und Familie), um das Bewusstsein zu schärfen. Diese Maßnahmen können Ihnen helfen, sich selbst und andere zu schützen.

Vorsicht vor „Rückgewinnungsbetrug“-Betrug („recovery rooms“):

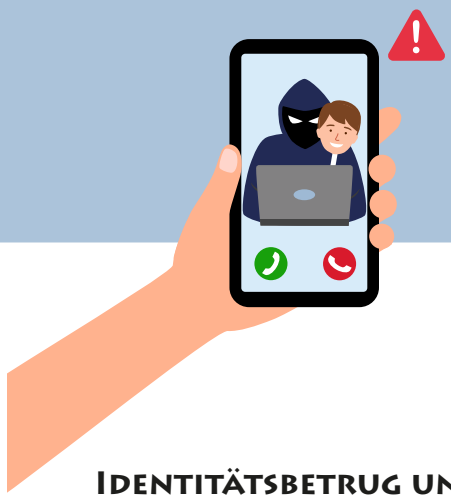
Der Betrüger kann sich mit Ihnen in Verbindung setzen, wissend, dass Sie Opfer eines früheren Betrugs sind, und behaupten, eine Behörde zu sein (z. B. Polizei, Steuer- oder Finanzbehörde usw.) und anbieten, Ihr verlorenes Geld gegen eine Gebühr zurückzufordern. Dies ist oft ein weiterer Versuch, Sie zu betrügen. Denken Sie daran: Einmal betrogen zu werden, hindert Sie nicht daran, erneut betrogen zu werden.

Europäische Bankenaufsichtsbehörde, Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung, Europäische Wertpapier- und Marktaufsichtsbehörde, 2025

Luxemburg: Amt für Veröffentlichungen der Europäischen Union, 2025

PDF ISBN 978-92-9407-251-1 doi:10.2853/6290723 DZ-01-25-139-DE-N

Arten von Online-Finanzbetrug und Abzocke durch KI



Identitätsbetrug und Verwendung von Deep Fake

Sie erhalten einen unerwarteten Anruf von jemandem, der behauptet, Ihre Bank, eine Behörde (z. B. Polizei, Steuer- oder Finanzbehörde usw.), ein Versicherungsmakler, ein IT-Unternehmen oder sogar ein Familienmitglied zu sein. Der Anrufer könnte Sie auffordern, Geld zu überweisen, um es sicher zu verwahren, unter Berufung auf verdächtige Aktivitäten auf ihrem Konto oder ihrer Versicherungspolice. Sie können Sie auch bitten, Ihre Bankdaten offenzulegen (z. B. Zahlungskartennummer, Internet-Banking-Anmeldeinformationen oder Passwörter), auf einen Link zu klicken oder eine Software zu installieren, die vorgibt, das Problem schnell lösen zu können. Der Anrufer kann eine gefälschte Nummer verwenden, die oft mit der Telefonnummer ihrer Bank übereinstimmt, um legitim zu erscheinen (Spoofing).

Betrüger können KI verwenden, um gefälschte Videos, Bilder oder Audiodateien zu erstellen, die die Stimme einer Person (z. B. Ihres Bankiers oder eines Familienmitglieds), das Gesicht (z. B. einer Berühmtheit) oder Bewegungen nachahmen. **Dies wird als „Deepfake“ bezeichnet.**

Was passieren könnte:

Indem er persönliche Daten erwähnt und ein Gefühl der Dringlichkeit schafft, täuscht der Betrüger Sie in Aktionen, die Sie nicht beabsichtigen, wie das Senden von Geld auf sein Konto, das Klicken auf einen bösartigen Link oder die Installation einer Malware auf Ihrem Gerät. Dies kann dem Betrüger direkten Zugriff auf Ihre Bankdaten geben. Mit diesen Informationen können sie Ihr Passwort ändern, auf Ihr Bankkonto zugreifen und Ihr Geld stehlen. Denken Sie daran: Nur weil ein Anrufer persönliche Daten über Sie kennt, bedeutet das nicht, dass er vertrauenswürdig ist.

Phishing und Social Engineering

Sie erhalten eine E-Mail oder Nachricht, die anscheinend von Ihrer Bank oder einem Finanzunternehmen stammt und Sie vor „verdächtigen Aktivitäten“ auf Ihrem Konto warnt. Das Logo, das Layout und die Sprache sehen professionell aus, und die Nachricht wird möglicherweise im selben Verlauf wie andere Unterhaltungen Ihrer Bank angezeigt. Die Nachricht fordert Sie auf, auf einen Link zu klicken, um Ihr Konto zu überprüfen oder Ihr Passwort zurückzusetzen. Der Link führt zu einer gefälschten Website, die mit Ihrem Internet-Banking identisch aussieht. Ohne es zu merken, geben Sie Ihre Daten in eine Website ein, die Ihre persönlichen Daten stehlen soll.

Betrüger nutzen KI, um überzeugende Phishing-Nachrichten zu erstellen, indem sie Social-Media-Daten analysieren, um ihre Opfer zu identifizieren und den Inhalt für jedes Ziel anzupassen.

Was passieren könnte:

Der Betrüger greift auf ihr Bankkonto zu und stiehlt Ihr Geld oder erstellt ein gefälschtes Profil mit ihren persönlichen Daten, um Betrug zu begehen.

Anlage- oder Versicherungsbetrug

Sie sehen eine Werbung in den sozialen Medien oder auf einer Website, die eine „befristete Anlagemöglichkeit mit geringem Risiko“ oder einen „befristeten Rabatt“ für eine Versicherung eines bekannten Unternehmens verspricht. Die Anzeige enthält ein Foto eines Prominenten und Empfehlungen, die oft gefälscht sind. Nachdem Sie Interesse bekundet haben, indem Sie auf einen Link klicken oder ein Formular ausfüllen, werden Sie kontaktiert und zu einer Plattform oder einem Messaging-Kanal weitergeleitet, auf der Sie professionell aussehende Ratschläge und Dokumente erhalten. Sie werden ermutigt, einen kleinen Betrag zu investieren, gefolgt von größeren Beträgen, oder die Prämie auf ein scheinbar sicheres Konto zu zahlen.

Betrüger nutzen KI-Tools, um diese gefälschten Vorschläge oder E-Mails sehr überzeugend und schwer zu erkennen zu machen. Sie verwenden auch KI-gestützte Social-Media-Bots, um gefälschte Konten zu erstellen, die mit Ihnen interagieren, Fehlinformationen verbreiten und echte Verhaltensweisen simulieren, um Vertrauen zu gewinnen und Ihre Entscheidungen zu beeinflussen.

Was passieren könnte:

Nachdem Sie versucht haben, Ihr Geld abzuheben oder einen Anspruch geltend zu machen, reagiert der Kontakt nicht mehr. Sie stellen fest, dass das Unternehmen nicht existiert oder dass das Versicherungsrisiko nicht abgedeckt ist. Sie erkennen dann, dass Sie im Rahmen eines betrügerischen Schemas Geld direkt an einen Betrüger geschickt haben. Leider können Sie Ihr Geld nicht zurückbekommen, und Ihre persönlichen und finanziellen Daten können verwendet werden, um weiteren Betrug zu begehen (z. B. Unterzeichnung von Verträgen in Ihrem Namen, die dazu führen könnten, dass Sie noch mehr Geld verlieren).

Liebesbetrug und Abzocke

Sie wurden in sozialen Medien, Dating-Apps oder per Telefon von jemandem kontaktiert, den sie im wirklichen Leben nicht getroffen haben. Diese Person führt häufige, persönliche und romantische Gespräche und baut Vertrauen mit gefälschten Profilen auf. Im Laufe der Zeit verschiebt sich das Gespräch in Richtung Geld oder finanzielle Möglichkeiten, wie Krypto-Investitionen mit Versprechen hoher Renditen und geringem Risiko. Die Person bittet Sie, Geld auf ein Konto zu überweisen oder führt Sie durch die Einrichtung eines Kontos und eine kleine Ersteinzahlung, damit das System legitim aussieht, bevor Sie ermutigt werden, mehr zu investieren.

Betrüger verwenden KI, um gefälschte Profile zu generieren, ihre Opfer in sozialen Medien/Dating-Apps anhand von Daten zu identifizieren, die Sie zur Verfügung gestellt haben, oder Chatbots zu verwenden, um Nachrichten zu generieren.

Was passieren könnte:

Der Betrüger extrahiert so viel Geld wie möglich, schneidet dann die gesamte Kommunikation ab und verschwindet. Die betrügerische Investment-Website oder -App wird offline genommen, so dass Sie nicht auf die angeblichen Investitionen zugreifen können. Zusätzlich zu finanziellen Verlusten können die persönlichen Daten, die Sie weitergegeben haben, verwendet werden, um Ihre Freunde und Familie anzusprechen oder für Identitätsdiebstahl, der finanzielle oder rechtliche Konsequenzen für Sie haben kann (z. B. könnte der Betrüger Einkäufe tätigen, Kredite in Ihrem Namen aufnehmen oder Sie könnten für Schulden oder Verbrechen verantwortlich gemacht werden, die unter Ihrem Namen begangen wurden, bis das Gegenteil bewiesen ist).

Kaufbetrug

Sie stoßen auf ein attraktives Angebot für einen Kauf auf einem Online-Marktplatz. Das Unternehmen, das den Deal anbietet, fordert eine Zahlung außerhalb der offiziellen Plattform an und behauptet, dass es ein „sicheres Zahlungssystem“ verwendet, und sendet Ihnen einen Link, um den Kauf abzuschließen. Der Link leitet Sie an eine betrügerische Bankauthentifizierungsseite weiter, die die offizielle Website der Bank imitiert und ihr Logo und Design verwendet, so dass Sie Ihre Online-Banking-Daten eingeben, um die Zahlung vorzunehmen.

Betrüger verwenden KI, um äußerst überzeugende gefälschte Bankwebsites, Auftragsbestätigungen und Rechnungen zu erstellen. KI hilft ihnen, den Ton, das Branding und den Stil echter Unternehmen nachzuahmen. In einigen Fällen verwenden sie KI-Chatbots, um Fragen zu beantworten und den Deal glaubwürdiger erscheinen zu lassen.

Was passieren könnte:

Die Zahlung über einen Link eines Dritten umgeht den Schutz des Marktplatzes. Der Betrüger erhält ihre Login-Informationen auf Ihr Bankkonto und stiehlt Ihr Geld.