Anlagebetrug im Internet mit Hilfe von künstlicher Intelligenz

SEIEN SIE WACHSAM UND SCHÜTZEN SIE SICH!

Online-Anlagebetrug ist nicht neu. Künstliche Intelligenz (KI) macht ihn aber cleverer und dadurch schwerer zu erkennen. Um Sie zu betrügen, verwenden Kriminelle gefälschte Nachrichten und Websites, falsche Promi-Profile und sogar KI-generierte Stimmen oder Videos, die wie Ihre Bankberaterinnen und-berater, Freundinnen und Freunde oder Familie aussehen und klingen.

Sie kontaktieren Sie mit täuschend echt erscheinenden Profilen, E-Mails, unerwarteten Anrufen und Messaging-Apps.

Sie können Risiken wie finanziellen Verlusten, Identitätsdiebstahl und emotionalen Belastungen ausgesetzt sein. Seien Sie vorsichtig und beachten Sie die folgenden Tipps, um sich zu schützen:

Seien Sie wachsam gegenüber Online-Anlagebetrug und Betrugsversuchen, die mit Hilfe von KI betrieben werden, beispielsweise Identitätsdiebstahl, Phishing, Investment- und Versicherungsbetrug und Love Scam. Erfahren Sie mehr über verschiedene Betrugsmaschen auf Seite 5, 6, und 7.

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

Warnzeichen beachten:
Lesen Sie, wie Sie verdächtige Verhaltensweisen, Nachrichten oder Angebote *erkennen können* (s. Seite 2);

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

Erfahren Sie, was zu tun ist, wenn Sie Opfer von Betrug werden
(s. Seite 4).

Warnzeichen

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

Ein unerbetener Anruf von einer unbekannten Nummer.

Zeitdruck: Ein dringendes Ersuchen um Geld oder persönliche Informationen. Dieses kann auch von jemandem kommen, der vorgibt ein Familienmitglied, ein Freund oder sogar eine öffentliche Person zu sein.

Eine Anfrage, sich auf Ihren PC einzuloggen, eine App herunterzuladen, einen QR-Code zu scannen oder auf einen Link zu klicken.

Die Frage nach persönlichen Informationen oder Bankdaten (etwa Passwörter, Kreditkartennummern, Internet-Banking-Anmeldeinformationen oder Sicherheitscodes).

Antrag auf Zahlung über nicht nachverfolgbare Wege (wie Kryptos, Geschenkkarten, Überweisungen oder Prepaid-Debitkarten).

Eine verdächtige oder falsche E-Mail-Adresse oder Link (unter anderem 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. Beachten Sie, dass KI es Betrügerinnen und Betrügern ermöglicht, diese Fehler zu minimieren.

Eine Website, die professionell aussieht, aber keine verifizierten Kontaktdaten oder kein Impressum enthält.

Sprachliche Intonation die unnatürlich klingt, keine Pausen hat und übermäßig fließend oder wie von einem Roboter wirkt. Achten Sie auf das „Klonen von Stimmen“. Beachten Sie, dass KI-generierte Sprache sehr natürlich klingen kann.

Videos, bei denen die Stimme wie von einem Roboter oder übermäßig glatt klingt, Lippenbewegungen und Gesichtsausdrücke möglicherweise nicht zum gesprochenen Text passen oder widersprüchliche Hintergründe, Beleuchtungen und Schatten. Dies kommt oft bei KI-generierten Videos (Deepfakes) vor.

So können Sie sich schützen

1 **Teilen Sie nie persönliche Daten oder Bank-Informationen:**

Seriöse Unternehmen fragen nicht nach Ihren PINs, Passwörtern, Internet-Banking-Anmeldeinformationen oder Sicherheitscodes, weder per E-Mail, noch via Social Media oder Telefon.

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 – Betrügerinnen und Betrüger schaffen absichtlich ein Gefühl der Dringlichkeit (etwa IT-Probleme mit Ihrer Bank, Notrufe von Ihren Freundinnen oder Freunden und Familienmitgliedern, bedrohliche Sprache usw.). Wenn Sie auch nur geringfügige Zweifel haben, handeln Sie nicht; beenden den Anruf und überprüfen die Quelle oder Identität sorgfältig.

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

- Überprüfen Sie immer, woher Nachrichten, Anrufe, E-Mails und Links kommen – auch wenn sie scheinbar seriös aussehen und von einer Freundin bzw. einem Freund, ihrer Familie oder sogar einer berühmten Person zu kommen scheinen. Rufen Sie beispielsweise Ihre Familie und Freunde mit einer bekannten Nummer über einen vertrauenswürdigen Kanal an oder schreiben eine SMS. Prüfen Sie Nachrichten auf Rechtschreibfehler, seltsame URLs oder fehlende Sicherheitsindikatoren (beispielsweise ob der Website-Link ein „s“ in „HTTPS“ enthält, um sicherzustellen, dass die Website sicher ist, und nach hinzugefügten oder fehlenden Buchstaben im Firmennamen der URL).

- Öffnen Sie keine Links aus unerbetenen Nachrichten, installieren Sie nur offizielle Anwendungen über vertrauenswürdige Apps und scannen Sie keine unbekannten QR-Codes.

- Vereinbaren Sie mit Ihrer Familie ein „sicheres Passwort“ – mit dem 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 (wie Eltern, Schwester oder Bruder, Kind).

- Verwenden Sie verifizierte Kontaktdaten, um das Unternehmen oder die Person direkt zu erreichen und verlassen Sie sich nie auf die Kontaktinformationen der oder des mutmaßlichen Kriminellen (etwa unabhängige Suche nach dem Firmennamen, Verwendung verifizierter Geschäftsverzeichnisse, zuvor bestätigte Kontaktmethoden). Betrügerinnen und Betrüger können behaupten, autorisiert zu sein oder die Website eines autorisierten Unternehmens nachahmen. Prüfen Sie, ob Ihre nationale Finanzmarktaufsichtsbehörde Warnungen veröffentlicht hat (↖) oder der Anbieter in die I-SCAN-Liste der IOSCO (iosco.org/i-scan/) aufgenommen wurden. Überprüfen Sie bei Kryptoanbietern, ob sie in der EU zugelassen sind (beispielsweise im ESMA-Register (↖).

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

Mit fortschreitender KI-Technologie werden Betrügereien immer raffinierter. Wenn Ihnen etwas ungewöhnlich erscheint oder Sie eines der oben genannten Warnzeichen erkennen, überdenken Sie Ihre Entscheidung, bevor Sie handeln.

5 **Installieren Sie nie Remote-Zugriffssoftware und teilen Sie niemals Ihren Bildschirm:**

Kreditinstitute und Finanzdienstleister werden dies nicht von Ihnen verlangen.

6 **Halten Sie Geräte und Konten sicher:**

Verwenden Sie starke und eindeutige Passwörter, halten Sie diese geheim und verwenden Sie dieselben Anmeldeinformationen nicht mehrfach auf verschiedenen Plattformen. Aktivieren Sie wenn möglich die Multi-Faktor-Authentifizierung. In einem Beitrag des BSI fnden Sie Tipps zu Passwörtern (↖). Halten Sie Ihre Software und Ihren Antivirenschutz immer 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, ist es wahrscheinlich nicht wahr.

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

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

Was tun, wenn Sie Opfer von Finanzbetrug geworden sind?

Brechen Sie Transaktionen sofort ab,

Um weitere Überweisungen auf verdächtige Konten zu blockieren und zusätzliche Verluste zu verhindern. Vermeiden Sie jeden Kontakt mit den Betrügerinnen und Betrügern, ignorieren Sie deren Anrufe und E-Mails und blockieren Sie Absender und Rufnummer.

Kontaktieren Sie Ihr Kreditinstitut oder Ihren Finanzdienstleister:

Informieren Sie Ihr Kreditinstitut oder Ihren Finanzdienstleister sofort über offizielle Kontaktkanäle und erkundigen Sie sich zu Optionen zum Einfrieren Ihres Kontos oder Rückgängigmachen von Transaktionen.

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

Kriminelle kaufen durchgesickerte Passwörter online und probieren sie auf mehreren Konten aus. Nur ein Passwort zu ändern, reicht nicht aus. Ändern Sie alles Passwörter, damit Betrügerinnen und Betrüger sie nicht wiederverwenden können.

Meldung und Warnmeldung:

Melden Sie den Vorfall der Polizei oder Ihrer nationalen Finanzaufsichtsbehörde und informieren Sie Ihre Bekannten (wie Freunde und Familie), um deren Bewusstsein zu schärfen. Diese Maßnahmen können Ihnen helfen, sich selbst und andere zu schützen.

Vorsicht vor „Rückholbetrug“.

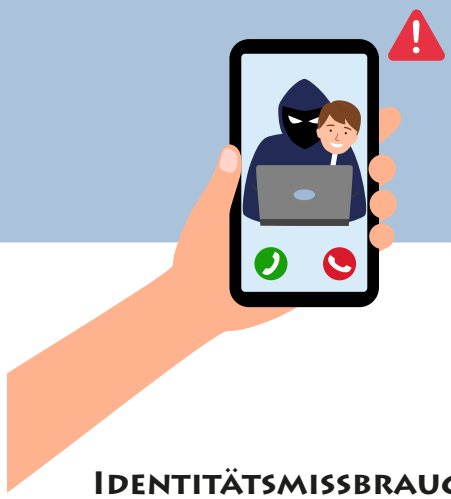
Betrügerinnen und Betrüger nutzen ihr Wissen, um Sie nach einem Betrug und der vermeintlichen Rückgewinnung des verlorenen Geldes zu unterstützen. Dafür geben sie vor, eine Behörde zu sein (etwas Polizei, Steuer- oder Finanzbehörde) und bieten Ihnen an, Ihr verlorenes Geld gegen eine Gebühr zurückzufordern. Dies ist oft ein weiterer Versuch, Sie zu betrügen. Denken Sie daran: Einmal betrogen zu werden, schützt Sie nicht davor, 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-Anlagebetrug und Betrug durch KI



Identitätsmissbrauch mit Deep Fakes

Sie erhalten einen unerwarteten Anruf von jemandem der behauptet Ihre Bank, eine Behörde (wie Polizei, Steuer- oder Finanzbehörde), ein Versicherungsagent, ein IT-Unternehmen oder sogar ein Familienmitglied zu sein. Die Anruferin oder der Anrufer könnte Sie unter Berufung auf verdächtige Kontoaktivitäten oder ihre Versicherungspolice auffordern, Geld zu überweisen, um diese abzusichern. Sie könnten Sie auch bitten, Ihre Bankdaten offenzulegen (etwa Zahlungskartennummer, Internet-Banking-Anmeldeinformationen oder Passwörter), auf einen Link zu klicken oder eine Software zu installieren, mit der Sie das Problem schnell lösen können. Die Anruferin bzw. der Anrufer kann eine gefälschte Nummer verwenden, die oft mit der Telefonnummer ihrer Bank übereinstimmt, um seriös zu erscheinen (spoofing).

Kriminelle können KI verwenden, um gefälschte Videos, Bilder oder Audiodateien zu erstellen, die die Stimme einer Person (zum Beispiel Ihres Bankberaters oder eines Familienmitglieds), das Gesicht (etwa von einer Berühmtheit) oder Bewegungen nachahmen. **Dies wird als „Deepfake“ bezeichnet.**

Was passieren könnte:

Indem sie bzw. er persönliche Informationen erwähnt und ein Gefühl der Dringlichkeit erzeugt, ermutigt die Betrügerin bzw. der Betrüger Sie zu Handlungen, die Sie eigentlich nicht beabsichtigen – wie das Senden von Geld, das Klicken auf einen schädlichen Link oder die Installation einer Malware auf Ihrem Gerät. Damit geben Sie der Betrügerin bzw. dem Betrüger direkten Zugriff auf Ihre Bankdaten. Mit diesen Informationen können die Kriminellen Ihr Passwort ändern, auf Ihr Bankkonto zugreifen und Ihr Geld stehlen. Denken Sie daran: Nur weil jemand 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 Ihrem Kreditinstitut oder einem Finanzdienstleister stammt und Sie vor „verdächtigen Aktivitäten“ auf Ihrem Konto warnt. Das Logo, das Layout und die Sprache sehen professionell aus. In der Nachricht werden Sie aufgefordert auf einen Link zu klicken, um Ihr Konto zu überprüfen oder Ihr Passwort zurückzusetzen. Der Link führt zu einer gefälschten Website die täuschend ähnlich zu Ihrem gewohnten Internet-Banking aussieht. Ohne es zu merken, geben Sie Ihre Daten in eine Website ein, die Ihre persönlichen Daten stiehlt.

Kriminelle nutzen KI, um überzeugende Phishing-Nachrichten zu erstellen. Sie analysieren Social-Media-Daten um ihre Opfer zu identifizieren und den Inhalt für jede Zielgruppe anzupassen.

Was passieren könnte:

Die Betrügerin bzw. der Betrüger greift auf ihr Bankkonto zu und stiehlt ihr Geld oder erstellt ein gefälschtes Profil mit ihren persönlichen Daten um Betrug zu begehen.

Investment- 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 bei einem bekannten Versicherungsunternehmen zeigt. Die Anzeige enthält ein Foto einer berühmten Person 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. Dort erhalten Sie scheinbar professionelle Ratschläge und Dokumente. Sie werden ermutigt, erst einen kleinen Betrag zu investieren, später größere Beträge, oder Geld auf ein scheinbar sicheres Konto zu zahlen.

Kriminelle nutzen KI-Tools, um die gefälschten E-Mails sehr überzeugend zu gestalten. Sie verwenden auch KI-gestützte Social-Media-Bots, um gefälschte Konten zu erstellen, die mit Ihnen interagieren, Fehlinformationen verbreiten und echte Verhaltensweisen simulieren, um Ihr 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 das Versicherungsrisiko nicht abgedeckt ist. Sie erkennen, dass Sie durch eine betrügerische Handlung Geld direkt an eine Betrügerin oder einen Betrüger geschickt haben. Leider können Sie Ihr Geld nicht zurückbekommen und Ihre persönlichen und finanziellen Daten können für weitere betrügerische Handlungen verwendet werden (etwa Unterzeichnung von Verträgen in Ihrem Namen, die dazu führen, dass Sie noch mehr Geld verlieren).

Love Scam

Sie werden in sozialen Medien, Dating-Apps oder per SMS von jemandem kontaktiert, den Sie im wirklichen Leben noch nie getroffen haben. Diese Person führt häufige, persönliche und romantische Gespräche mit Ihnen und baut Vertrauen mit Hilfe von gefälschten Profilen auf. Im Laufe der Zeit verschiebt sich das Gespräch in Richtung Geld oder finanzielle Möglichkeiten, wie Krypto-Investitionen und dem Versprechen von hohen Renditen bei geringem Risiko. Die Person bittet Sie, Geld auf ein Konto zu überweisen oder richtet mit Ihnen ein Konto ein. Sie werden zu einer kleinen Ersteinzahlung überredet und später ermutigt, mehr zu investieren.

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

Was passieren könnte:

Die Betrügerin bzw. der Betrüger zieht so viel Geld wie möglich ab, stellt dann die gesamte Kommunikation mit Ihnen ein 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 von Ihnen weitergegebenen persönlichen Daten verwendet werden, um Ihre Freundinnen, Freunde und Familie zu kontaktieren oder für Identitätsdiebstahl, der finanzielle oder rechtliche Konsequenzen für Sie haben kann. So könnte ein Betrüger Einkäufe tätigen oder Kredite in Ihrem Namen aufnehmen. Sie könnten auch für Schulden oder Verbrechen verantwortlich gemacht werden, die unter Ihrem Namen begangen wurden, bis das Gegenteil bewiesen ist.

Fake Shops

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

Kriminelle verwenden KI, um täuschend echt aussehende Bankwebsites, Auftragsbestätigungen und Rechnungen zu erstellen. KI hilft ihnen, den Sprachgebrauch, 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. Die Betrügerin bzw. der Betrüger erhält Ihre Login-Informationen auf Ihr Bankkonto und stiehlt Ihr Geld.