Zu schön, um wahr zu sein?

KI-gesteuerte Betrugsmaschen in einer Welt, in der Vertrauen auf dem Prüfstand steht

Künstliche Intelligenz verändert unsere Lebens- und Arbeitsweise. Aber sie gibt Betrüger:innen auch neue Werkzeuge an die Hand, um uns zu täuschen. Von gefälschten Stimmen, die genau wie unsere Liebsten klingen, bis hin zu überzeugenden Videos, in denen jemand Dinge sagt, die er nie gesagt hat – KI-gesteuerte Betrugsmaschen werden immer schwerer zu erkennen. Cyberkriminelle nutzen unsere Emotionen und unser Vertrauen aus und setzen manipulative Taktiken ein, um uns zu beeinflussen oder unter Druck zu setzen.

Wie funktioniert KI-Betrug?

KI-gestützte Betrugsmaschen bauen auf denselben psychologischen Tricks auf, die Betrüger:innen schon immer angewendet haben. Ihr Ziel ist es nach wie vor, Sie dazu zu bringen, etwas zu tun, was Sie normalerweise nicht tun würden, wie zum Beispiel auf einen bösartigen Link zu klicken, sensible Informationen weiterzugeben oder Geld zu überweisen. Was sich geändert hat, ist, wie einfach es für sie geworden ist, überzeugend zu klingen und zu wirken.

Hier sind einige gängige Arten von KI-Betrug:

Deepfake-Identitätsdiebstahl

Betrüger:innen verwenden KI, um realistische Audio- oder Videodateien einer vertrauten Person – Ihrer Chefin, Ihres Partners oder sogar Ihrer Kinder– zu erstellen, um Sie zum Beispiel dazu zu bringen, Geld zu senden oder Zugangsdaten weiterzugeben. Diese Identitätsbetrügereien können in Videoanrufen, Voicemails oder Social-Media-Nachrichten auftreten.

Telefonbetrug durch Klonen von Stimmen

Kriminelle nutzen KI, um Stimmen aus kurzen Audioausschnitten (wie Voicemails oder YouTube-Clips) zu klonen. Mit nur wenigen Sekunden Audio können sie einen Anruf tätigen, der unheimlich vertraut und dringend klingt.

Romantik- und Beziehungsbetrug
Chatbots, die sich als echte Personen ausgeben, bauen mit der Zeit Beziehungen auf, gewinnen langsam Ihr Vertrauen und Ihre persönlichen Daten, bevor sie Sie um Geld oder Gefälligkeiten bitten.

Betrug per E-Mail
KI erleichtert die Erstellung gezielter Phishing-E-Mails, die scheinbar von jemandem aus Ihrem Unternehmen stammen und oft mit Deepfake-Anrufen oder Sprachnachrichten kombiniert werden.

Massenbetrug per Anruf und Nachricht
KI ermöglicht es Kriminellen, Tausende von personalisierten Nachrichten oder Anrufen gleichzeitig zu versenden, die alle mit Informationen personalisiert sind, die sie online oder durch Datenlecks gefunden haben.

Investmentbetrug
KI wird verwendet, um gefälschte, professionell aussehende Websites, Fake News oder gefälschte Empfehlungen zu erstellen, die Betrugsmaschen legitim erscheinen lassen, insbesondere im Zusammenhang mit Kryptowährungen oder „zu gut, um wahr zu sein“ Angeboten.

Erkennen Sie die Anzeichen

KI-gesteuerte Betrugsmaschen sind so konzipiert, dass sie echt wirken. Hier sind einige Warnsignale, auf die Sie achten sollten:

- **Ungewöhnliches Verhalten:** Jemand, den Sie kennen, verhält sich seltsam: Der Tonfall ist merkwürdig, die Sprache ungewöhnlich oder die Forderungen ergeben keinen Sinn.
- **Emotionale Manipul**ation oder Dringlichkeit: Sie werden aufgefordert, sofort zu handeln, da sonst ernsthafte Konsequenzen drohen. Betrüger:innen nutzen oft Angst, Liebe oder Aufregung, um Ihr Urteilsvermögen zu beeinträchtigen.
- **Kanalwechsel:** Sie werden dazu gedrängt, das Gespräch schnell auf eine andere Plattform zu verlagern (z. B. von E-Mail zu WhatsApp).
- **Profil zu perfekt:** Online-Profile wirken übermässig geschliffen, mit wenig Interaktionshistorie oder Bildern, die anderswo im Internet zu finden sind – oft passen sie nicht zur angegebenen Identität der Person.

Denken Sie daran: Es geht nicht darum, „gefälschte Videos”, sondern verdächtige Situationen zu erkennen.

Was können Sie tun?

- **Halten Sie inne und atmen Sie tief durch.** Betrüger:innen wollen Sie zu schnellem Handeln verleiten. Wenn Sie sich Zeit nehmen, können Sie besser Warnsignale erkennen.
- **Überprüfen Sie immer alles.** Vor allem, wenn jemand Sie um etwas Unerwartetes bittet. Nutzen Sie einen anderen Kanal, um zu bestätigen, dass die Anfrage echt ist. Wenn jemand Geld, Daten oder dringende Massnahmen verlangt, überprüfen Sie die Identität der Person über einen separaten Kommunikationskanal (z. B. durch einen Anruf unter der bekannten Nummer).
- **Verwenden Sie ein Codewort. V**ereinbaren Sie mit Ihrer Familie oder Ihren Kollegen ein Geheimwort, um zu bestätigen, dass es sich wirklich um sie handelt. Lesen Sie unsere Kurzinformation zur Verwendung von Codewörtern.
- **Teilen Sie nicht zu viel online.** Betrüger:innen sammeln persönliche Daten aus sozialen Medien, um ihre Angriffe zu personalisieren.
- **Seien Sie vorsichtig bei neuen Kontakten.** Nehmen Sie sich Zeit für neue Online-Beziehungen oder Personen, die um Hilfe bitten.
- **Melden Sie den Vorfall und holen Sie Hilfe.** Wenn Ihnen etwas verdächtig vorkommt oder Sie sich unsicher sind, wenden Sie sich an Ihr IT-Team oder Ihren Sicherheitsbeauftragten. Im privaten Bereich wenden Sie sich an die zuständigen Behörden.

Be mindful. Stay safe.

Bei KI-Betrug geht es nicht nur um Technologie, sondern auch um Psychologie. Seien Sie achtsam, halten Sie inne, bevor Sie reagieren, und denken Sie daran: Es ist in Ordnung, doppelt zu überprüfen. In einer Welt voller digitaler Illusionen ist digitale Achtsamkeit Ihre stärkste Verteidigung.

Erfahren Sie mehr

🔗 Deepfakes when video evidence lies (source: iBarry)
🔗 ENISA Threat Landscape 2024 (source: ENISA)
🔗 Facing Reality: Law Enforcement and the Challenge of Deepfakes (source: Europol)
🔗 Impact of AI on cyber threat from now to 2027 (source: NCSC UK)

GÉANT