

Das hat er so nie gesagt

Betrugsmasche. Kriminelle fälschen Videos mit Promis und locken Anleger per WhatsApp auf betrügerische Trading-Plattformen. Wer dort Geld anlegt, sieht es nie wieder.

Friedrich Merz wirft sich für Traderium AI ins Zeug, per Video. „Ich ermutige alle, die sich für moderne Investitionsmöglichkeiten interessieren, sich mit dieser Plattform auseinanderzusetzen“, sagt er. Sie könne „finanzielle Freiheit für viele Menschen greifbar“ machen.

Kann ja wohl nicht wahr sein! Ist es auch nicht. Denn Kriminelle haben mithilfe von künstlicher Intelligenz (KI) die Stimme von Merz nachgeahmt und ihm die Aussagen in den Mund gelegt. Die Bilder sind echt, aber im Original-Video legt Merz vor Wirtschaftsführern seine Pläne als Kanzler dar.

Solche „Deep Fakes“ sind eine gefährliche neue Masche Krimineller. Mit Hilfe der Promi-Bilder sollen Menschen dazu verleitet werden, Geld bei betrügerischen Internetbrokern einzuzahlen oder Gruppen auf WhatsApp beziehungsweise Telegram beizutreten. Die „Investment-Tipps“, die sie dort bekommen, schaden ihnen aber nur.

Deep-Fake-Videos von Prominenten

Wir haben das gefälschte Merz-Video ein paar Leuten gezeigt und sie nach ihrem Eindruck gefragt. Eine Frau mittleren Alters fand

die Umsetzung überzeugend, bezweifelte aber, dass der Bundeskanzler so etwas sagen würde. Zwei junge Erwachsene wiederum erkannten zwar die Fälschung rasch an Fehlern bei der Lippsynchronisation und Sprüngen in Ton und Bild – konnten sich aber vorstellen, dass der früher in der Finanzbranche tätige Spitzenpolitiker Broker empfiehlt.

Fortschritte bei der KI dürften es schon bald schwer machen, Fakes zu entlarven, vor allem wenn Videos eher nebenbei auf kleinen Handy-Bildschirmen angesehen werden.

Ganoven nutzen soziale Medien

Auf den ersten Blick echt wirken oft auch angebliche Medienberichte über Fernsehsendungen, in denen Prominente „aus Versehen“ Anlagegeheimnisse ausgeplaudert haben, oder Werbeanzeigen, in denen sie ankündigen, Investmenttipps zu teilen.

Das soll Vertrauen wecken. Denn ohne das Einverständnis der Promis würden solche Aussagen ja wohl kaum auf Facebook und Instagram gezeigt, oder? Weit gefehlt. Die unfreiwilligen Werbeträger würden das Ganze nur zu gern unterbinden, es gelingt ihnen aber nicht immer. Der Spiegel-Online-Kolumnist Christian Stöcker schrieb im Juli 2025, seine Instagram-Follower und er hätten in den vergangenen Wochen „an die zehn Fake-Accounts“ zu seiner Person gemeldet. Doch die Instagram-Mutter Meta habe zum Teil nur sehr verzögert reagiert.

Auf unsere Anfrage äußerte sich Meta nicht direkt zu dem konkreten Fall, ließ aber über eine Agentur auf seinen umfangreichen Kampf gegen Fake-Accounts hinweisen. Wer davon betroffen sei, könne dies über die App oder ein Formular im Hilfebereich melden.

Landet die Sache vor Gericht, dauert es meist, bis ein Ergebnis vorliegt. Daher hilft es, wenn sich Betroffene öffentlich von dem vermeintlichen „Testimonial“ distanzieren.



Unser Rat

Hinterfragen. Prominente empfehlen unbekannte Internetbroker? Banken werben für WhatsApp-Gruppen? Gehen Sie davon aus, dass das nicht echt ist. Wie Sie weitere Warnzeichen erkennen, lesen Sie im Kasten auf Seite 40.

Mitteilen. Melden Sie Betreibern sozialer Netzwerke missbräuchliche Beiträge, senden Sie der Finanzaufsicht Belege zu dubiosen Angeboten (bafin.de, Suchbegriff „allgemeines Kontaktformular“).

Anzeigen. Haben Sie durch Betrug Geld verloren, erstatten Sie Strafanzeige online (test.de/onlineanzeige) oder bei einer Polizeidienststelle – und liefern Sie Belege mit.

**FAKE**

Bild echt, Stimme gefälscht, Botschaft betrügerisch:

„Traderium AI ermöglicht es Nutzern, mit einem vergleichsweise kleinen Startkapital von nur 250 Euro eine nachhaltige Einkommensquelle aufzubauen.“

Dieses Zitat wurde Friedrich Merz untergeschoben.

Deep Fake. Kriminelle ließen eine KI die Stimme von Kanzler Friedrich Merz imitieren und ersetzten die echte Rede vom Davoser Weltwirtschaftsgipfel 2025 durch eine Werbebotschaft.

So stellte die ZDF-Moderatorin Marietta Slomka im Heute Journal vom 12. August 2025 klar, angebliche Tipps von ihr im Internet, wie man mit Kryptowährungen zum Millionär werde, seien „Fakes, die auf Betrugsseiten locken sollen“.

Nicht immer sind bekannte Namen im Spiel. Manche Betrüger werben damit, dass sie KI für Handelserfolge einsetzen. Tatsächlich nutzen viele seriöse Investmenthäuser KI. Doch die Kriminellen behaupten das nur, sammeln aber bloß Anlegergeld ein und lassen es dann blitzschnell verschwinden.

Tipp: Prüfen Sie, ob Sie Warnzeichen entdecken, wie wir sie auf Seite 40 auflisten. Aktuelle Betrugsfälle finden Sie unter test.de/warnliste und test.de/cybertrading-betrug.

Masche: Langsam Vertrauen aufbauen

Die Sache ist verführerisch: Geringe Mindestsummen wie 250 Euro lassen das Risiko überschaubar wirken. Viele Interessierte un-

terschätzen aber, wie versiert die Kriminellen darin sind, Vertrauen aufzubauen und die Gier anzufachen. Experten sprechen von „Social Engineering“. Es gelang den Betrügern in einigen Fällen sogar, ihre Opfer noch zu Geldzahlungen zu bewegen, nachdem die Polizei diese bereits gewarnt hatte.

„Vielen fällt es schwer, sich einzugestehen, dass sie auf Betrüger hereingefallen sind“, berichtet Anwältin Tanja Nauschütz aus München, die bereits für Betrugsoffer Schadenersatz erstreiten konnte (test.de/fibonetix).

Ausgezahlt werden höchstens Minibeträge. Oft melden sich später weitere Abzocker. Sie bieten etwa an, das verlorene Geld zurückzuholen. Tatsächlich verschwindet auch der Betrag, den sie dafür verlangen.

In den WhatsApp- und Telegram-Gruppen läuft es ähnlich, auch wenn die Masche etwas anders daherkommt. Mitglieder erhalten vermeintlich heiße Anlagetipps, oft zu Aktien, wo schon geringe Orders Kurssprünge

bewirken. Die Betrüger haben sich zuvor entsprechend eingedeckt und können mit Gewinn verkaufen – die Kunden nicht mehr.

Betrüger versprechen Exklusivität

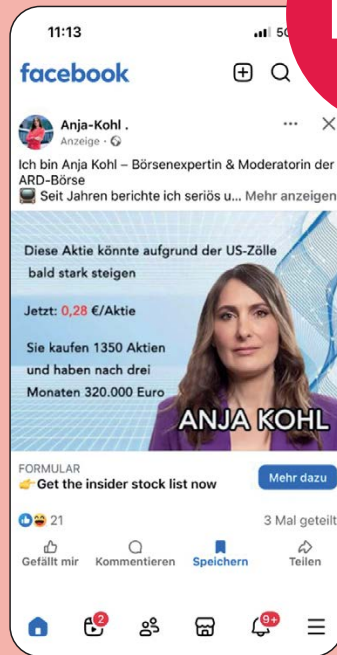
Oft locken die Kriminellen mit einem angeblich begrenzten Zugang zu einer tollen Handelsplattform oder App, auch testweise. Teils bekommen die Mitglieder sogar Kapital zur Verfügung gestellt, hat die Bundesanstalt für Finanzdienstleistungsaufsicht beobachtet, die vor etlichen solcher Angebote warnt.

Die Masche ist extrem erfolgreich, die Schäden sind immens, selbst wenn die Werbung mal nicht perfekt ist. So behauptet die gefälschte Stimme im Fake-Video von Merz auch, dass viele Anleger mit dem Handelssystem „monatliche passive Einnahmen von über 4 Euro erzielen.“ Für die versprochene finanzielle Freiheit reicht das nicht. ■ →

Text: Renate Daum; Faktencheck: Betina Chill

FAKE

Fake auf Facebook.
Diese Werbung ist angeblich von der Börsenjournalistin Anja Kohl. In Wirklichkeit stecken Betrüger dahinter.



Logo gefälscht.
Betrüger werben auf Facebook mit der ING-Bank. Wer solche Fakes findet, kann der ING die URL melden: Mail an info@ing.de.

Warnzeichen erkennen

So entlarven Sie windige Angebote

Über eine „Studio-Eskalation bei Maischberger“ berichtete angeblich am 2. September 2025 die Seite tagesschau.de. In der Sendung „gestern Abend“ habe Bundeskanzler Friedrich Merz live vorgeführt, wie er binnen Minuten mithilfe der Plattform Veratix360 Geld verdient. Registrieren sei nur bis zum 3. September möglich. An diesem Beispiel zeigen wir, woran Sie dubiose Angebote erkennen können.

Typische Anzeichen für Fakes

Bereits ein K.-o.-Kriterium reicht meist, um dubiose Angebote zu erkennen.

- **Falsche Internetadresse.** In diesem Fall begann die URL nicht mit „tagesschau.de“, sondern mit „newsupdate-direkt.click“.
- **Meldung unauffindbar.** Geben Sie die Überschrift in eine Suchmaschine ein oder suchen Sie direkt beim fraglichen Medium (hier: tagesschau.de). Lässt sich die Meldung nicht finden, liegt ein Fake vor.
- **Veranstaltung fand gar nicht statt.** Laut ARD-Webseite hatte „maischberger“ von Mitte Juli bis Mitte September Pause.
- **Auffälliger Link zum Angebot.** Im Fall Veratix360 verwies der Bericht direkt auf die Registrierungsseite des Anbieters. Das ist bei echten Medienberichten unüblich.

- **Anbieter erzeugt Zeitdruck.** Seien Sie misstrauisch, wenn „Deadlines“ drohen.
- **Werbung mit Promis.** Meist wissen die Betroffenen nichts davon. Fakt ist: Merz hat Veratix360 nie lobend erwähnt.

Seriosität des Anbieters prüfen

Alles beginnt mit einem Check der Webseite des Anbieters.

- **Impressum.** Fehlt bei Veratix360. Liegt ein Impressum vor, checken Sie, ob es wichtige Informationen wie Firma, Adresse, Aufsichtsbehörde, Handelsregister und Handelsregisternummer enthält. Überprüfen Sie gegebenenfalls die Angaben – etwa den Handelsregistereintrag (über die Seite handelsregister.de). Selbst wenn alles dem Anschein nach stimmt, ist das noch kein Beleg für Seriosität: Kriminelle klauen nämlich oft die Daten echter Firmen.
- **Erlaubnis.** Hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) dem Broker erlaubt, seine Geschäfte zu betreiben? Suchen Sie auf bafin.de nach „Unternehmensdatenbank“ und geben dort die Firma ein. Veratix360 fehlt darin.
- **Fakten.** Stimmen die Inhalte auf der Webseite, etwa Angaben zu Presseberichten oder Partnern? Veratix360 nutzt eine

Art Bundesadler als Logo und trägt dick auf: „Die deutsche Regierung verkündet mit Stolz den Start von Veratix360 – einem offiziellen Projekt Deutschlands.“ Unter einem Foto von Finanzminister Lars Klingbeil prangt ein Zitat: Veratix360 eröffne „den Weg zum Aufbau persönlichen Vermögens und zur Stärkung der deutschen Wirtschaft“. Zu Veratix360 ist bei offiziellen Stellen aber nichts zu finden.

■ **Warnungen.** Hinweise zu unseriösen Anbietern finden Sie bei der BaFin oder der Stiftung Warentest. Veratix360 steht auf unserer Warnliste (test.de/warnliste).

Werbung in sozialen Netzwerken

Schwerer ist es, Fake-Werbung in sozialen Netzwerken zu erkennen. Checken Sie:

- **Stimmen die Logos?** Etwa wenn mit Banken geworben wird.
- **Gibt es Widersprüche?** Beispiel: Ein Prominenter wirbt angeblich für den Beitritt zu einer WhatsApp-Gruppe, teilt aber anderswo mit, WhatsApp nicht zu nutzen.
- **Warnungen.** Googeln Sie: Gibt es die „Finanzexperten“ überhaupt, die angeblich mit den Prominenten zusammenarbeiten? Oft werden Sie bei Ihrer Suche auf Warnungen vor Fakes stoßen.