NACHRICHTEN AG

30. August 2024

Vorsicht vor Deepfake-Betrug: Wenn Promis Investitionen anpreisen

Experten warnen vor gefälschten Werbevideos mit Promis, die Verbraucher über dubiose Plattformen zu Investments verleiten.

Immer raffiniertere Betrugsmaschen drängen ins Internet, und aktuell stehen gefälschte Videos ganz oben auf der Liste. Mit diesen Deepfake-Videos zielen Kriminelle darauf ab, ahnungslose Nutzer um ihr Geld zu bringen. Diese Videos wirken so überzeugend, dass selbst erfahrene Internetnutzer ins Wanken geraten können.

Eine neue Warnung kommt vom europäischen IT-Sicherheitsanbieter Eset, der auf gefährliche Betrugsversuche aufmerksam macht. In diesen gefälschten Videos sind prominente Persönlichkeiten zu sehen, die vermeintlich für lohnenswerte Investmentangebote werben. In den manipulierten Clips erscheinen Figuren wie der CDU-Vorsitzende Friedrich Merz und SAP-Mitbegründer Dietmar Hopp. Das Versprechen? Hohe Gewinne bei minimalem finanziellen Einsatz, ein verlockendes Angebot, das viele verunsichern könnte.

Technologische Tricks der Betrüger

Die Betrüger bedienen sich echter Nachrichtenbeiträge als Grundlage für ihre Machenschaften. Mittels künstlicher Intelligenz (KI) werden diese Informationen analysiert, um die Software zu trainieren, die letztendlich die gefälschten Videos produziert. Eset erklärte, dass die Kriminellen, von denen angenommen wird, dass sie aus Russland oder der Ukraine

stammen, die KI nutzen, um individuelle und verführerische Inhalte zu schaffen, die zum Investieren anregen.

Besonders beunruhigend ist die Tatsache, dass diese Kampagne nicht nur in Deutschland aktiv ist, sondern auch in anderen Ländern wie Kanada, Japan, Südafrika und den Niederlanden. Laut Eset sind aktuell viele deutsche Verbraucher die Hauptopfer dieser gefälschten Werbevideos.

„Politiker und öffentliche Persönlichkeiten sind ein wahres Ziel für solche KI-basierenden Betrüger“, erklärte Eset-Forscher Ondrej Novotny. Diese Personen haben eine breite Bandbreite an Bildern und Videos, die die Betrüger nutzen können, um die Illusion eines seriösen Testimonials zu kreieren. Das Ergebnis ist ein scheinbar vertrauenswürdiger Rat für das Investieren, der den Nutzern das Gefühl gibt, dass es sich um eine sichere Entscheidung handelt.

Doch die Warnung von Eset ist unmissverständlich: Nutzer sollten sich nicht verleiten lassen. Das Risiko, auf diese Machenschaften hereinzufallen, ist enorm. In früheren Fällen, die in anderen Ländern registriert wurden, erhielten die Opfer sogar telefonische Einschüchterungsversuche von den Betrügern, die sie dazu drängen wollten, größere Summen zu investieren.

Erkennungsmerkmale von Deepfakes

Eset hat auch einige Tipps bereitgestellt, um gefälschte Videos zu erkennen. Oft sind diese Deepfakes von minderer Qualität und haben gravierende Fehler, wie etwa eine schlechte Lippensynchronisation. Dennoch könnten diese Merkmale geschickte Betrüger nicht daran hindern, ihre Videos zu verwenden, denn sie benötigen nur einen kleinen Teil der Empfänger, die auf die falle hineintappen und ihr Geld überweisen. „Das ist für die Kriminellen ein einfaches Geschäft mit minimalem Aufwand“, so Novotny weiter.

Die Technologie hinter Deepfakes wird zunehmend zugänglicher, und das bedeutet, dass auch die Gefahr von Missbrauch steigt. Verbraucherschützer und IT-Experten appellieren daher an alle Internetnutzer, wachsam zu sein und sich nicht von scheinbar lukrativen Angeboten blenden zu lassen. Die Anzeichen sind oft nicht offensichtlich genug, um sofortige Alarmglocken läuten zu lassen, daher ist Vorsicht geboten.

In einer Zeit, in der viele Menschen nach finanziellen Möglichkeiten suchen, könnten diese betrügerischen Systeme verheerende Folgen haben. Verbraucher sollten immer kritisch sein und die Quelle von Informationen überprüfen, bevor sie irgendwelche finanziellen Entscheidungen treffen. Bleiben Sie vorsichtig und informieren Sie sich, um nicht Opfer dieser modernen Betrugsmaschen zu werden.

Details