

Die Gefahren von KI-generiertem Bildmaterial und Deepfakes

Worum handelt es sich bei KI-generiertem Bildmaterial und Deepfakes?

KI-generiertes Bildmaterial wird anhand von Milliarden vorhandener Bilder generiert. KI-Generatoren erstellen anhand eines Prompts (in diesem Fall einer Beschreibung) Bilder, indem sie viele dieser Beispiele zu einem einzigen Bild kombinieren. Die Deepfake-Technologie funktioniert ähnlich, jedoch werden hierbei echte Fotos und Videos manipuliert. Beispielsweise lässt sich mit dieser Technologie der Eindruck erwecken, dass eine Person etwas getan oder gesagt hat, ohne dass dies der Fall ist. Beide Technologien können für legitime Zwecke dienen, werden jedoch auch von Cyberkriminellen missbraucht.

Betrug mit Deepfakes

Kriminelle können sich mithilfe der Deepfake-Technologie als Promis oder andere Personen des öffentlichen Lebens ausgeben. So lässt sich beispielsweise der Anschein erwecken, dass Promis ein Produkt empfehlen, obwohl dies nicht der Fall ist. Kriminelle verleiten ihre Opfer damit zum Kauf von Produktfälschungen oder zur Weitergabe von personenbezogenen Daten oder Finanzinformationen. Deepfakes können auch bei Personen aus der Politik missbraucht werden. So kann ein Deepfake-Video den Anschein erwecken, dass Regierungsvertreterinnen oder Regierungsvertreter etwas gesagt oder getan haben, obwohl das gar nicht stimmt. Mit solchen Videos lassen sich Personen auf gefälschte Websites locken oder dazu verleiten, auf Fake-News-Artikel zu klicken.

Betrug mit KI-generierten Bildern und Fotos

Cyberkriminelle setzen KI häufig für Onlinebetrug in Zusammenhang mit einer angeblichen Partnersuche („Love Scamming“ oder „Romance Scamming“) ein. Sie nutzen gefälschte Fotos in Dating-Profilen, um Geld oder Informationen von ihren Opfern zu entwenden. Cyberkriminelle nutzen auch aktuelle Ereignisse für Betrug. Beispielsweise erstellen sie mithilfe von KI realistische Fotos von Katastrophen und anderen Ereignissen. Sie veröffentlichen die Fotos auf gefälschten Websites, um ihre Opfer dazu zu bewegen, Geld an eine Wohltätigkeitsorganisation zu spenden. Die Organisation gibt es in Wirklichkeit selbstverständlich gar nicht und die Cyberkriminellen greifen die Spenden ab.

Wie können Sie sich schützen?

Befolgen Sie die nachstehenden Tipps, um sich vor Betrug mit KI-generiertem Bildmaterial zu schützen:

- KI-generierte Bilder weisen oft subtile Abweichungen oder Fehler auf. Achten Sie in Bildern auf alles, was ungewöhnlich erscheint. Eine Hand mit mehr als fünf Fingern oder ungewöhnliches Licht bzw. ungewöhnliche Schatten sind häufige Anzeichen dafür, dass Bilder mit KI erstellt wurden.
- Klicken und handeln Sie keinesfalls unbedacht. Wenn ein Foto oder ein Bild bizarr oder zu schön ist, um wahr zu sein, handelt es sich womöglich um Betrug.
- Überprüfen Sie Behauptungen, wenn möglich, an anderer Stelle. Sehen Sie beispielsweise ein Video, in dem eine prominente Persönlichkeit für ein Produkt wirbt, sollten Sie auf der offiziellen Website der betreffenden Person prüfen, ob diese tatsächlich in Verbindung mit dem Produkt steht.

