Das gefälschte Gesicht

Gesichtserkennungssoftware wird infiltriert, um Ihr Gesicht zu stehlen

Vorhersage: *Hacker werden Software zur Gesichtserkennung austricksen. Unternehmen werden deshalb auf verhaltensbasierte Systeme setzen.*

Der Diebstahl von Anmeldeinformationen ist einer der ältesten Tricks überhaupt, und Angreifer sind unermüdlich dabei, neue Schwachstellen auszumachen, um an die Anmeldedaten von Endbenutzern zu kommen. Die zweistufige Authentifizierung wurde durch Aufkommen des sogenannten „SIM Swapping“ untergraben. Biometrische Authentifizierungsmethoden wie Fingerabdrücke und Gesichtserkennung sind zwar besser, aber dennoch anfällig.

Zweistufige und biometrische Authentifizierung sind keine

Patentrezepte.

224 Mio. USD

Gesamtschadenersatzansprüche von Michael Terpin, nachdem er nach einem Angriff auf sein AT&T-Konto Kryptowährung im Wert von 24 Mio. USD durch „SIM Swapping“ verloren hatte.

450 USD

Kosten für die Erstellung einer Papierversion Ihres **Fingerabdrucks** (oder des einer anderen Person).

5,6 Mio.

Anzahl der Personen, deren **Fingerabdrücke** bei einer Datenschutzverletzung beim Amt für Personalverwaltung der Vereinigten Staaten **gestohlen wurden**.

9,78 Mrd. USD

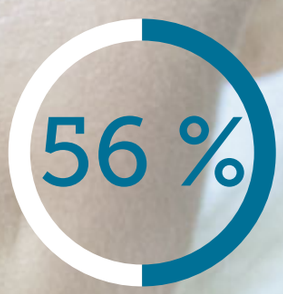
Geschätzter globaler Markt für **Gesichtserkennungssoftware** bis 2023.

Phishing

ist weiterhin die beliebteste Angriffsmethode.

12,4 Mio.

potenzielle Phishing-Opfer in den Jahren 2016 und 2017.



der Entscheider im Bereich der IT-Sicherheit geben an, dass gezielte Phishing-Angriffe die größte Sicherheitsbedrohung darstellen.

Haben Gesichtserkennung überwunden

2016 bezwangen Spezialisten der University of North Carolina für Sicherheit und maschinelles Sehen Gesichtserkennungssysteme mit öffentlich zugänglichen digitalen Fotos aus sozialen Medien.