A counterfeit reflection

Facial recognition software is infiltrated to steal your face

***Prediction:** Hackers will game end-user face recognition software, and organizations will respond with behavior-based systems*

Credential theft is the oldest trick in the book, and attackers are relentless in finding new vulnerabilities to steal end-user logins. Two-factor authentication (2FA) has been undermined with the introduction of "SIM swaps," while biometric authentication methods like fingerprints and facial recognition fare better but are still vulnerable.

Two-factor and biometric authentication are not

silver bullets

$224 million

Total damages sought by Michael Terpin, who allege that attackers stole $24 million in cryptocurrency by conducting a "SIM swap" on his AT&T account

$450

The cost to create a paper version of your (or someone else's) **fingerprint**

5.6 million

The number of people whose **fingerprints were stolen** in U.S. Office of Personnel Management breach

$9.78 billion

Estimated global market of **facial recognition software** by 2023

Phishing

is still an attacker's best friend

12.4 million

potential victims of phishing from 2016 to 2017

of IT security decision makers say that targeted phishing attacks were the top security threat they faced

defeated facial recognition

In 2016, security and computer vision specialists from the University of North Carolina defeated facial recognition systems using publicly available digital photos from social media