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.

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

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

- **5.6 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:

- **$224 million**

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

- **$450**

Potential victims of phishing from 2016 to 2017:

- **12.4 million**

The estimated global market of facial recognition software by 2023:

- **$9.78 billion**