Una Conseguenza della Contraffazione

Il software di riconoscimento facciale viene infiltrato per rubarti la fisionomia.

Previsione: *Gli hacker manipoleranno i software di riconoscimento facciale dell'utente finale, e le organizzazioni risponderanno sistemi basati su comportamento*

Il furto di credenziali è il trucco più vecchio del mondo, e gli aggressori sono accaniti nel cercare nuovi punti deboli. L'autenticazione a due fattori (2FA) è stata indebolita dall'introduzione del "SIM swap", mentre i metodi di autenticazione biometrica come il riconoscimento facciale e di impronte digitali sono migliori ma comunque vulnerabili.

Le autenticazioni biometrica e a due fattori non sono

soluzioni perfette.

$224 milioni

Danni totali visti da Michael Terpin, che afferma che gli aggressori hanno rubato $24 milioni in criptovaluta conducendo un "SIM swap" sul suo profilo AT&T.

$450

il costo della creazione di una versione cartacea delle tue (o di qualcun altro) **impronte digitali**.

5,6 milioni

Il numero di persone alle quali sono state **rubate le impronte digitali** nella violazione dell'US Office of Personnel Management.

$9,78 milioni

Stima del mercato globale di **software di riconoscimento facciale** per il 2023.

Il phishing

è ancora il migliore amico degli aggressori.

12,4 milioni

vittime potenziali di kit di phishing dal 2016 al 2017.

Di decisori in ambito sicurezza dicono che attacchi di phshing mirati sono stati la minaccia di sicurezza maggiore che hanno affrontato.

superato il test di riconoscimento facciale

Nel 2016, gli specialisti della visione di sicurezza e computer dell'Università del Nord Carolina hanno sconfitto i sistemi di riconoscimento facciale usando foto digitali pubbliche dai social media.