Uma reflexão sobre falsificação

Softwares de reconhecimento facial foram infiltrados para furtar o seu rosto

Previsão: *Os hackers usarão software para reconhecimento facial de usuários finais e as organizações responderão com sistemas baseados em comportamento*

O furto de credenciais é o truque mais antigo que existe e os invasores são persistentes na busca de novas vulnerabilidades para furtar logins de usuários finais. A autenticação com dois fatores (2FA) foi solapada com a introdução de "SIM swaps", e os métodos de autenticação biométrica, como impressões digitais e reconhecimento facial, têm desempenho melhor, mas continuam vulneráveis.

As autenticações com dois fatores e biométricas não são

soluções mágicas.

US$ 224 milhões

em danos totais foram solicitados por Michael Terpin, que alega que atacantes furtaram US$ 24 milhões em criptomoedas, como resultado de um "SIM swap" em sua conta da AT&T.

US$ 450

custo para criar uma versão em papel de sua **impressão digital** (ou da impressão digital de outra pessoa).

5,6 milhões

número de pessoas cujas **impressões digitais foram furtadas** em uma invasão do Gabinete de Gestão de Pessoal dos EUA.

US$ 9,78 bilhões

Mercado global estimado de **software de reconhecimento facial** até 2023.

O phishing

ainda é o melhor amigo de um invasor.

12,4 milhões

de vítimas potenciais de phishing de 2016 a 2017.

dos tomadores de decisões de TI dizem que os ataques de phishing direcionados foram a principal ameaça de segurança que enfrentaram.

derrotaram sistemas de reconhecimento facial

2016, especialistas em segurança e computação gráfica da Universidade da Carolina do Norte derrotaram sistemas de reconhecimento facial usando fotos digitais disponíveis publicamente em mídias sociais.