Un reflejo falso

Se infiltra software de reconocimiento facial para robarle la imagen de su rostro

Predicción: *Los hackers manipularán software de reconocimiento facial de usuarios finales y las organizaciones responderán con sistemas basados en el comportamiento*

El robo de credenciales es el truco más viejo que conocemos y los atacantes son implacables en la búsqueda de nuevas vulnerabilidades en el inicio de sesión de usuarios finales. La doble autenticación (2FA) se ha visto comprometida con la introducción de "cambios de SIM" mientras que los métodos de autenticación biométrica, como huellas digitales y reconocimiento facial, resultan mejor en comparación pero todavía son vulnerables.

La autenticación doble y biométrica no son

balas de plata.

$224 millones

Fue el total en daños que reclamó Michael Terpin, quien alega que los atacantes robaron $24 millones en criptomonedas al perpetrar un "cambio de SIM" en su cuenta de AT&T.

$450

es el costo de crear una versión en papel de su **huella digital** (o la de otra persona).

5.6 millones

es la cantidad de personas cuyas **huellas digitales fueron robadas** en la fuga de la Oficina de Administración de Personal de Estados Unidos.

$9,780 millones

Mercado global estimado de **software de reconocimiento facial** para el 2023.

El Phishing

sigue siendo el mejor amigo de los atacantes.

12.4 millones

de víctimas potenciales de phishing de 2016 a 2017.

56%

de las personas que toman decisiones relacionadas con la seguridad informática afirman que los ataques de phishing dirigidos fueron la principal amenaza de seguridad que enfrentaron.

burlaron sistemas de reconocimiento facial

En 2016, especialistas de seguridad y de visión por computadora de la Universidad de Carolina del Norte burlaron sistemas de reconocimiento facial usando fotografías digitales públicas, disponibles en redes sociales.