Gerçek Olmayan Yansıma

Yüz hatlarınıza ulaşmak için için yüz tanıma yazılımlarına sızılıyor

Tahmin: *Bilgisayar korsanları son kullanıcı yüz tanıma yazılımlarını hedef alacak ve şirketler davranış tabanlı sistemlerle karşılık verecektir*

Kimlik hırsızlığı en eski numara olmakla beraber, saldırganlar son kullanıcı oturum bilgilerini çalmak için yeni güvenlik açıkları bulmaya devam ediyor. “SIM değişimi” sahtekarlığının ortaya çıkmasıyla birlikte iki faktörlü kimlik doğrulama (2FA) güvenilirliğini kaybetti. Parmak izi ve yüz tanıma gibi biyometrik kimlik doğrulama yöntemleri şimdilik daha iyi güvenlik sağlıyor olsalar da risk teşkil ediyorlar.

Çift faktörlü ve biyometrik kimlik doğrulama

sihirli değnek

değil.

224 milyon $

Saldırganların AT&T hesabında “SIM değişimi” yaparak 24 milyon $ değerinde kripto parasını çaldığını iddia eden Michael Terpin'in talep ettiği toplam tazminat.

450 $

Parmak izinizi kağıda çıkarmanın maliyeti.

5,6 milyon

ABD Personel Yönetim Ofisi ihlali ile parmak izleri çalınan kişilerin sayısı.

9,78 milyar $

2023 itibariyle yüz tanıma yazılımlarının tahmini küresel pazar payı.

Kimlik avı

hala bir saldırganın en iyi arkadaşı olmaya devam ediyor.

12,4 milyon

Kimlik avının potansiyel kurban sayısı (2016 - 2017).

%56

Karşılaştıkları en önemli güvenlik tehdidinin hedeflenmiş kimlik avı saldırıları olduğunu belirten BT güvenliği karar vericilerinin oranı.

yüz tanıma yenilgiye uğradı

2016 yılında, Kuzey Carolina Üniversitesi’ndeki güvenlik ve bilgisayar görüntüsü uzmanları sosyal medyada herkese açık olarak paylaşılan dijital fotoğrafları kullanarak yüz tanıma sistemlerini yenilgiye uğratmıştır.