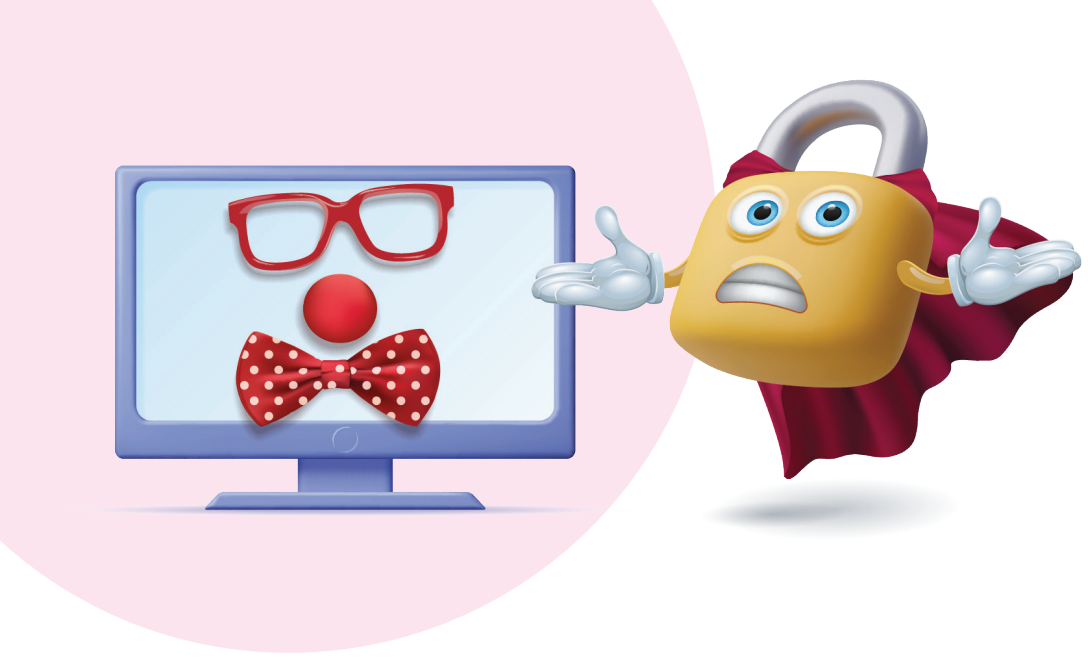


DaTi + SiCuRi

L'IA AL SERVIZIO DEI CYBER CRIMINALI

Truffe con IA

I cyber criminali utilizzano l'IA per **realizzare attacchi di phishing ed e-mail fraudolente truffe più credibili**.

L'IA consente ai cyber criminali di elaborare e-mail di phishing fino al **40%** più velocemente

Deepfake

I cyber criminali utilizzano **immagini o video manipolati con l'IA (deepfake)**, per ingannare le vittime simulando false dichiarazioni o eventi.

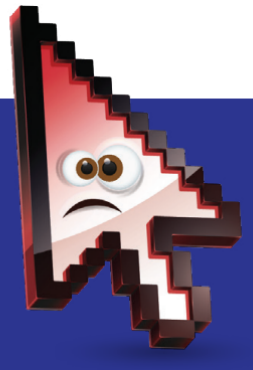
L'IA generativa viene impiegata per creare profili LinkedIn, curriculum e contenuti falsi utilizzati nelle campagne di impersonificazione e social engineering

Clonazione vocale con IA

I cyber criminali utilizzano l'IA per **replicare la voce di una persona**, a partire da registrazioni esistenti per indurre le persone a rivelare informazioni personali o compiere operazioni di pagamento.

Nel 2025 il vishing è diventato il **2°** vettore di compromissione iniziale più diffuso.

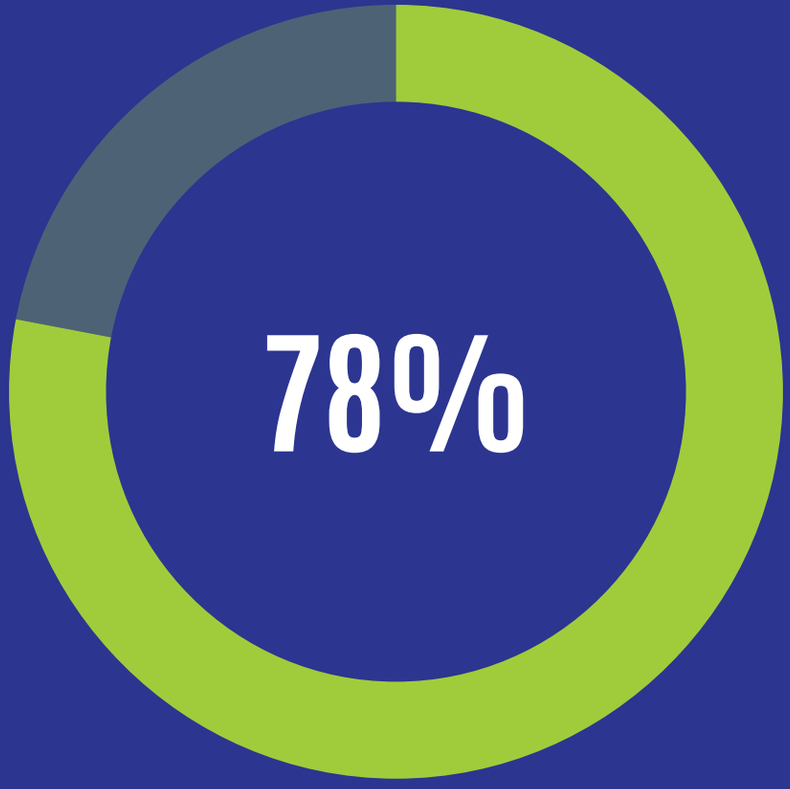
Fonte:
https://tech-adv.com/blog/ai-cyber-attack-statistics/,
Corwdstrike 2025 Global Threat Report



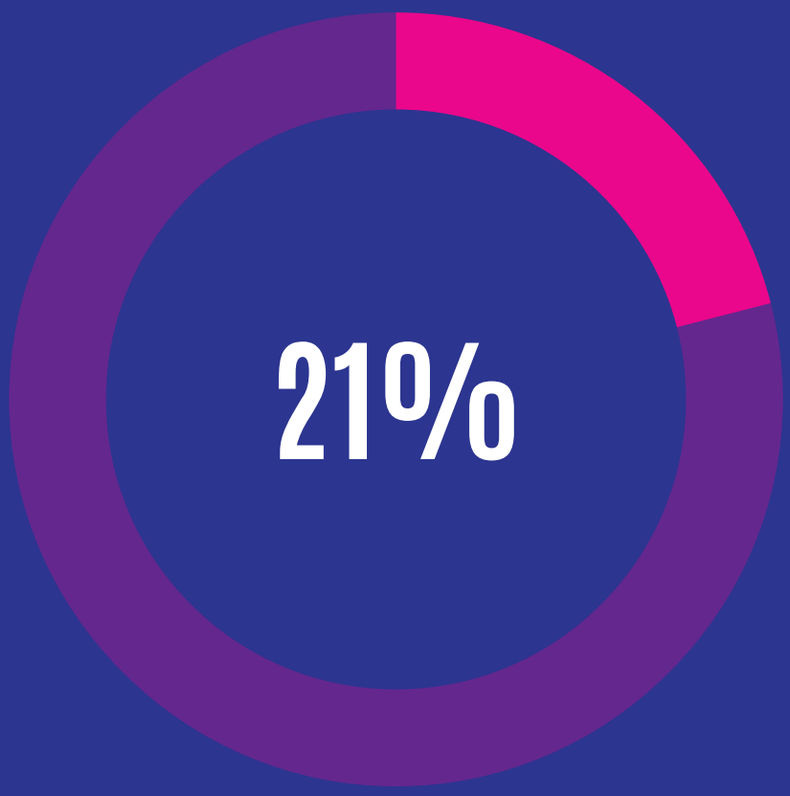
L'IMPATTO DELL'AI SULL'EFFICACIA DEGLI ATTACCHI

Gli attacchi di phishing generati dall'AI sono sempre più difficili da riconoscere. I dati mostrano che il **78% degli utenti apre e-mail di phishing** create con l'Intelligenza Artificiale e il **21% interagisce con i contenuti o i collegamenti** presenti nel messaggio.

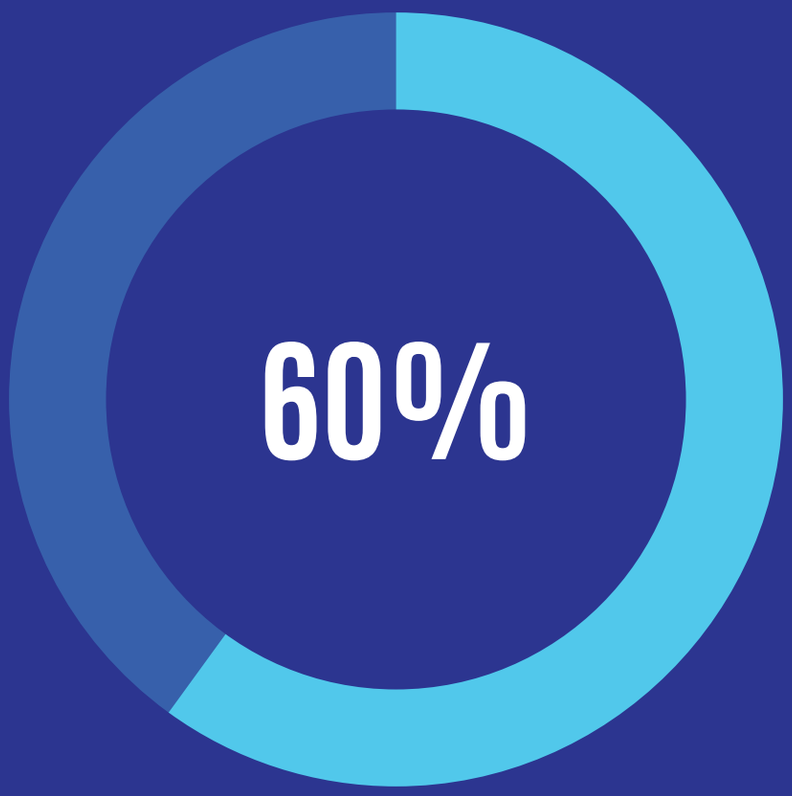
Anche gli attacchi basati sulla clonazione vocale rappresentano una minaccia crescente: le persone riescono a **identificare correttamente una voce generata dall'AI solo nel 60%** dei casi, una percentuale appena superiore a quella ottenibile con una scelta casuale.



Utenti che aprono e-mail
di phishing generate dall'AI

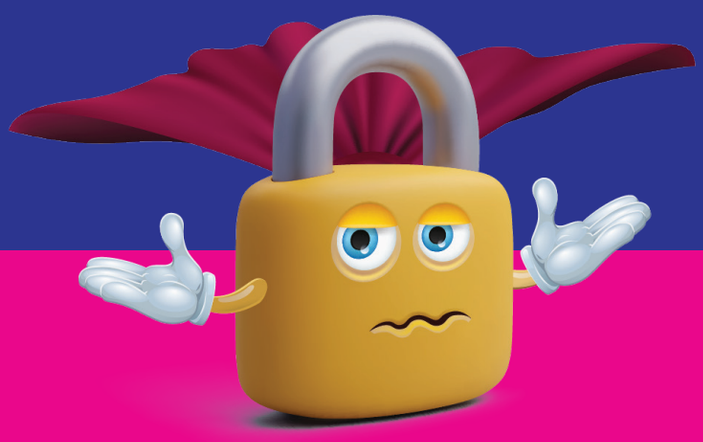


Utenti che cliccano su link
o contenuti dopo aver
aperto l'e-mail



Utenti che riconoscono correttamente voci generate dall'AI

Fonte: Tech Advisor - AI Cyber Attack Statistics 2026



L'AUMENTO DELL'UTILIZZO

DEI DEEPFAKE NELLE FRODI

L'utilizzo dei deepfake nelle frodi è cresciuto in modo esponenziale negli ultimi anni. Se nel 2022 rappresentava una quota marginale dei tentativi di frode, nel primo trimestre del 2025 i deepfake sono stati utilizzati nel 6,5% di tutti gli attacchi fraudolenti a livello globale. **Nel solo primo trimestre del 2025 sono stati registrati più incidenti legati ai deepfake che nell'intero 2024**.

6,5%

Attacchi fraudolenti che coinvolgono deepfake

2.137%

Crescita delle frodi basate su deepfake dal 2022

+3 MILIARDI DI DOLLARI

Perdite economiche attribuite ai deepfake negli Stati Uniti

Fonte: deepidv - Fraudulent ID & Deepfake Benchmark Report 2026

QUANTO SONO REALISTICI I DEEPFAKE OGGI?

Nel 2023, la maggior parte dei deepfake poteva essere riconosciuta attraverso una semplice analisi visiva. Nel 2025, i deepfake più sofisticati risultano invece difficilmente distinguibili dai contenuti autentici. Per questo motivo, oltre 10.000 deepfake sono stati classificati in base al loro livello di qualità.

Livello 1 – Evidentemente falsi

Livello 2 – Identificabili con un'attenta verifica

Livello 3 – Difficili da riconoscere per

utenti non esperti

Livello 4 – Indistinguibili da contenuti autentici

Fonte: deepidv - Fraudulent ID & Deepfake Benchmark Report 2026