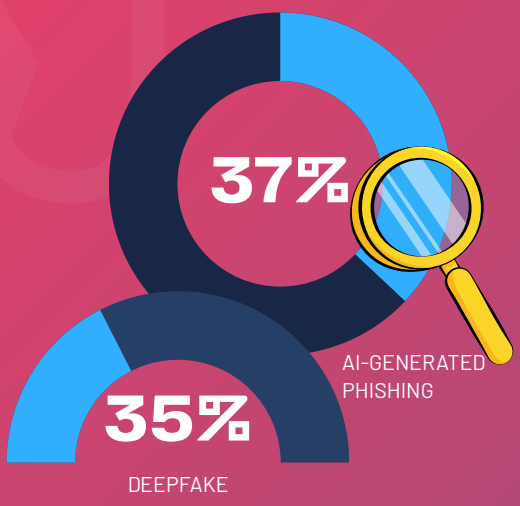
HACK3R_
RANGERS

AI IN 2026: THE MAIN SECURITY CONCERNS

MAIN TYPES OF
AI-DRIVEN ATTACKS:



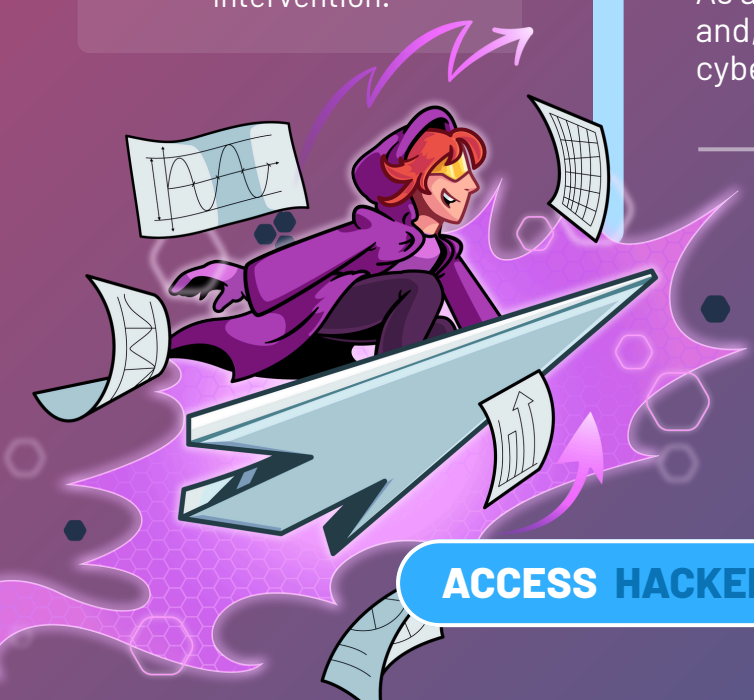
2025 COST OF A
DATA BREACH, IBM

In 2025, a **single deepfake** resulted in a loss of

US$25 MILLION

for a company after an employee was deceived by a deepfake of the CFO during a meeting.

At the end of 2025, the world witnessed the first cyberattack almost 100% orchestrated by AI with minimal human intervention.



HYPER-PERSONALIZED PHISHING ATTACKS

Generative AI has reached a level of sophistication where **texts, voices, and images are almost indistinguishable from reality**.

The time required to create a convincing phishing email has **dropped from 16 hours to just 5 minutes**, allowing attackers to scale social engineering campaigns with much greater speed and efficiency (2025 Cost of a Data Breach, IBM).

DEEPFAKES ARE A REAL AND IMMINENT THREAT

Deepfakes have become an especially concerning threat. They are no longer limited to manipulated videos, but now include complete simulations capable of interacting in real time. **AI-driven cybercrime is already causing real damage to companies around the world**.

A NEW THREAT: AUTONOMOUS AI

The threat has evolved from human use of AI to autonomous AI. Now, the technology is **capable of planning attacks, identifying vulnerabilities, and infiltrating systems almost on its own**.

As a result, the barriers to entry have decreased and, more than ever, **anyone** can become a cybercriminal.

A well-trained employee can be the difference between a successful attack and business continuity. Hacker Rangers prepares your team to recognize and fight social engineering scams on a daily basis.

ACCESS HACKERRANGERS.COM AND GET A DEMO