✉ info@archerround.au

☎ 1800 841 224

https://www.archerround.com

ARCHER & ROUND

30 years of Cybersecurity Excellence

Archer & Round Cybersecurity Report

# The Rise of AI-Driven Cyber Threats

June 2025 Edition

## Executive Summary

Artificial Intelligence (AI) is rapidly transforming the cybersecurity landscape — for both defenders and attackers. While AI-powered tools are strengthening threat detection and response, cybercriminals are equally leveraging AI to scale attacks, automate phishing campaigns, and develop highly sophisticated malware. This report explores how AI is reshaping the threat environment and provides practical steps businesses can take to strengthen their defences against this emerging wave of cyber threats.

## Key Findings

**AI is Lowering the Barrier to Entry for Cybercrime.**
AI-based tools are enabling less-skilled threat actors to launch complex attacks, including automated phishing, password guessing, and social engineering at scale.

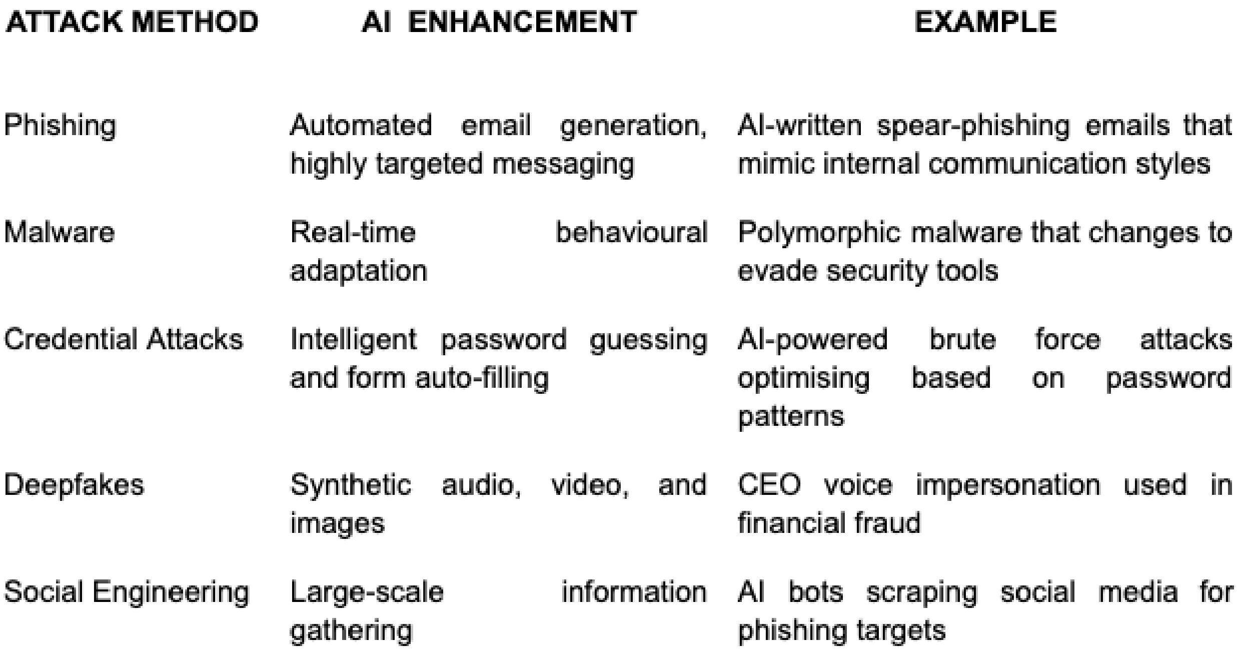
**Deepfakes Are Rapidly Becoming a New Attack Vector.**
AI-generated audio, video, and text are increasingly used to impersonate executives, commit fraud, and manipulate organizations.

**Malware is Becoming More Adaptive.**
AI-powered malware can now modify its behavior in real time to avoid detection by traditional security tools.

**AI-Enhanced Phishing is Outpacing Human Detection.**
Automated spear-phishing campaigns using generative AI create highly personalized emails that are harder to identify and filter.

**Defenders Are Also Getting Smarter.**
AI is improving anomaly detection, enabling faster threat response, and powering advanced Security Information and Event Management (SIEM) platforms.

# How Attackers Are Using AI



| ATTACK METHOD | AI ENHANCEMENT | EXAMPLE |
|---|---|---|
| Phishing | Automated email generation, highly targeted messaging | AI-written spear-phishing emails that mimic internal communication styles |
| Malware | Real-time behavioural adaptation | Polymorphic malware that changes to evade security tools |
| Credential Attacks | Intelligent password guessing and form auto-filling | AI-powered brute force attacks optimising based on password patterns |
| Deepfakes | Synthetic audio, video, and images | CEO voice impersonation used in financial fraud |
| Social Engineering | Large-scale information gathering | AI bots scraping social media for phishing targets |

## Case Study: Deepfake CEO Fraud

In 2024, a UK-based company was defrauded of over £200,000 after a fraudster used a deepfake audio clip to convincingly impersonate the CEO during a phone call, instructing a finance employee to urgently transfer funds. Investigations later confirmed the voice was synthetically generated using AI tools.

Source: World Economic Forum, 2024 Cybersecurity Outlook

## What Businesses Can Do

**1. Implement Advanced Email Filtering**
Use AI-driven email security solutions capable of detecting behavioural anomalies and sophisticated phishing.

**2. Employee Awareness and Simulation Training**
Educate staff on emerging deepfake and AI-powered phishing techniques. Run regular phishing simulations using up-to-date tactics.

**3. Multi-Factor Authentication (MFA) Everywhere**
Reduce the impact of compromised credentials by enforcing MFA across all systems.

**4. Adopt AI-Powered Threat Detection**
Deploy SIEM and Endpoint Detection and Response (EDR) platforms that leverage machine learning to identify complex threats in real time.

**5. Establish Verification Protocols**
Require secondary verification (via a different communication channel) for sensitive requests like financial transfers, especially if they come via voice or text.

## Looking Ahead: The AI Arms Race

According to the **Australian Cyber Security Centre (ACSC)** and the **European Union Agency for Cybersecurity (ENISA)**, the cybersecurity industry is entering an "AI arms race" where both attackers and defenders will increasingly rely on AI. Organisations that proactively adopt AI-powered defences and maintain strong cybersecurity hygiene will be best positioned to withstand this evolving threat landscape.

**Recommended Resources:**

- Australian Cyber Security Centre – Emerging Threats
- ENISA Threat Landscape 2024
- MIT Technology Review – AI in Cybersecurity

**Archer & Round Cyber Intelligence Team**
Safe | Secure | Reliable
Contact us: info@archerround.com