# 5 REAL-WORLD AI-POWERED THREATS

Real incidents. Real impact. Real lessons.

01

## DEEPFAKE VOICE FRAUD

**Real Incident: UK (2019)**

Fraudsters used an AI-cloned voice of a company executive to convince a CEO to transfer €220,000 to a fraudulent account.

02

## DEEPFAKE VIDEO CONFERENCE SCAM

**Real Incident: Hong Kong (2024)**

An employee transferred US$25 million after joining a video meeting where every "colleague" was an AI-generated deepfake.

03

## AI-GENERATED PHISHING

**Real-World Trend:**

Threat actors increasingly use Large Language Models (LLMs) to generate grammatically correct, multilingual, and highly personalized phishing emails that are harder to detect.

04


## AI-ASSISTED PASSWORD CRACKING

**Real Example: PassGAN**

Researchers demonstrated that PassGAN, a generative AI model trained on leaked passwords, can predict human-created passwords more effectively than traditional rule-based attacks.

*Source: Hitaj, Gasti, Ateniese & Perez-Cruz, PassGAN: A Deep Learning Approach for Password Guessing (2019).*

05

## SYNTHETIC IDENTITY FRAUD

**Real-World Trend:**

Banks and financial institutions are seeing AI-generated faces, forged identity documents, and synthetic identities used to bypass remote KYC verification.

Europol and other agencies have identified synthetic identity fraud as a rapidly growing AI-enabled threat.

www.ampcuscyber.com | letsconnect@ampcuscyber.com