AI-Generated Media Drives Real-World Fraud, Identity Theft, and Business Compromise

Trend Micro uncovers the criminal playbook for deepfake-enabled cybercrime

DALLAS, July 9, 2025 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today released a new report exposing the scale and maturity of deepfake-enabled cybercrime. As generative AI tools become more powerful, affordable, and accessible, cybercriminals are rapidly adopting them to support attacks, ranging from business fraud to extortion and identity theft.

To read the full report*, Deepfake it 'til You Make It: A Comprehensive View of the New AI Criminal Toolset*please visit*: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/deepfake-it-til-you-make-it-a-comprehensive-view-of-the-new-ai-criminal-toolset*

The report shows how deepfakes have moved beyond hype into real-world exploitation, undermining digital trust, exposing companies to new risks, and accelerating the business models of cybercriminals.

David Sancho, senior threat researcher at Trend: "AI-generated media is not just a future risk, it's a real business threat. We're seeing executives impersonated, hiring processes compromised, and financial safeguards bypassed with alarming ease. This research is a wake up call—if businesses are not proactively preparing for the deepfake era, they're already behind. In a world where seeing is no longer believing, digital trust must be rebuilt from the ground up."

The research found that threat actors no longer need underground expertise to launch convincing attacks. Instead, they are using off-the-shelf video, audio, and image generation platforms, many of which are marketed to content creators, to generate realistic deepfakes that deceive both individuals and organizations. These tools are inexpensive, easy to use, and increasingly capable of bypassing identity verification systems and security controls.

The report outlines a growing cybercriminal ecosystem where these platforms are used to execute convincing scams, including:

- CEO fraud has become increasingly harder to detect as attackers use deepfake audio or video to impersonate senior leaders in real-time meetings.
- Recruitment processes are being compromised by fake candidates who use AI to pass interviews and gain unauthorized access to internal systems.
- Financial services firms are seeing a surge indeepfake attempts to bypass KYC (Know Your Customer) checks, enabling anonymous money laundering through falsified credentials.

The criminal underground is actively trading tutorials, toolkits, and services to streamline these operations. From step-by-step playbooks for bypassing onboarding procedures to plug-and-play face-swapping tools, the barrier to entry is now minimal.

As deepfake-enabled scams grow in frequency and complexity, businesses are urged to take proactive steps to minimize their risk exposure and protect their people and processes. This includes educating staff on social engineering risks, reviewing authentication workflows, and exploring detection solutions for synthetic media.

About Trend Micro
Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's AI-powered cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, Trend's platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 70 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---