

# Deepfake và Những Ảnh Hưởng Đến Xã Hội



# Deepfake là gì?

1

## Công nghệ AI giả mạo

Deepfake là công nghệ tiên tiến sử dụng **Trí tuệ nhân tạo (AI)** và **học sâu (Deep Learning)** để tạo ra các nội dung giả mạo như video, hình ảnh hoặc âm thanh cực kỳ chân thực, khó phân biệt thật giả.

2

## Ghép nối từ ngữ

Thuật ngữ "Deepfake" được tạo thành từ sự kết hợp của "Deep Learning" (học sâu) và "fake" (giả mạo), phản ánh bản chất của công nghệ này.

3

## Thay thế thực tế

Với Deepfake, khuôn mặt, giọng nói của một người có thể bị thay thế hoàn hảo bằng một hình ảnh hoặc âm thanh giả mạo khác, tạo ra những cảnh tượng hoặc đoạn hội thoại chưa từng xảy ra.

# Công nghệ đằng sau Deepfake



Deepfake hoạt động dựa trên các thuật toán **Machine Learning** phức tạp và **mạng Nơ-ron nhân tạo**. Chúng được huấn luyện để phân tích và tái tạo tỉ mỉ các đặc điểm riêng biệt của khuôn mặt và giọng nói con người.

Khả năng chân thực của Deepfake tỉ lệ thuận với lượng dữ liệu gốc. Càng nhiều video, hình ảnh và âm thanh của mục tiêu được cung cấp, hệ thống AI càng học hỏi sâu sắc và tạo ra sản phẩm giả mạo khó phát hiện.

Các phần mềm như DeepFaceLab, FaceSwap hay Microsoft Designer đã tích hợp sẵn công nghệ AI, giúp việc tạo Deepfake trở nên dễ dàng và phổ biến hơn bao giờ hết.

# Ứng dụng tích cực của Deepfake



## Giải trí đa dạng

Deepfake mở ra cánh cửa cho sự sáng tạo trong ngành giải trí, từ việc tạo hiệu ứng đặc biệt sống động trong phim ảnh, video âm nhạc cho đến các chiến dịch quảng cáo độc đáo.



## Giáo dục & Đào tạo

Trong giáo dục, deepfake có thể mô phỏng các nhân vật lịch sử, tạo video hướng dẫn tương tác hoặc tái hiện các sự kiện quá khứ một cách sống động, nâng cao trải nghiệm học tập.



## Hỗ trợ phục hồi

Công nghệ này còn có tiềm năng hỗ trợ phục hồi hình ảnh hoặc giọng nói cho những người không may bị mất khả năng giao tiếp, giúp họ tái hòa nhập cuộc sống.

- Tuy nhiên, mọi ứng dụng tích cực đều cần được kiểm soát chặt chẽ để ngăn chặn nguy cơ lạm dụng và bảo vệ tính toàn vẹn của thông tin.

# Những tác hại và rủi ro nguy hiểm

## Lừa đảo tài chính

Điển hình là vụ việc nhân viên một công ty đa quốc gia bị lừa 25 triệu USD qua cuộc gọi video Deepfake giả mạo giám đốc tài chính, cho thấy mức độ tinh vi của tội phạm.

## Tin giả, bôi nhọ danh dự

Deepfake có thể được dùng để phát tán hình ảnh, video khiêu dâm giả mạo (ví dụ như trường hợp của Taylor Swift) hoặc tin giả, gây tổn hại nghiêm trọng đến danh dự, uy tín cá nhân.

## Ảnh hưởng chính trị & xã hội

Việc xuất hiện các video giả mạo lãnh đạo, quan chức có thể gây mất niềm tin xã hội sâu sắc, thao túng dư luận, thậm chí ảnh hưởng đến kết quả bầu cử và ổn định chính trị.

## Chiếm đoạt & lừa đảo

Tội phạm mạng sử dụng deepfake để chiếm đoạt tài khoản, lừa đảo người thân qua các cuộc gọi video giả mạo, đặt ra mối đe dọa lớn về an ninh mạng và an toàn thông tin.

## An ninh quốc gia

Ở mức độ vĩ mô, Deepfake có thể tác động tiêu cực đến an ninh quốc gia thông qua việc lan truyền thông tin sai lệch có chủ đích, gây chia rẽ và hoang mang trong cộng đồng.

# Cách nhận biết một video deepfake

01

## Quan sát dấu hiệu bất thường

Chú ý các chi tiết nhỏ: chuyển động môi không khớp lời nói, ánh sáng không tự nhiên, khuôn mặt bị biến dạng nhẹ hoặc mắt nhấp nháy một cách kỳ lạ.

Deepfake thường bỏ sót các yếu tố này.

02

## Kiểm tra nguồn gốc video

Sử dụng công cụ **tìm kiếm hình ảnh đảo chiều** (Google Reverse Image Search) để truy vết nguồn gốc video hoặc hình ảnh. Điều này giúp xác định tính xác thực của nội dung.

03

## Sử dụng phần mềm chuyên dụng

Các phần mềm như **Microsoft Video Authenticator** hay **Intel FakeCatcher** được thiết kế để phát hiện Deepfake bằng cách phân tích các điểm bất thường mà mắt thường khó nhận ra.

04

## Xác thực thông tin đa chiều

Luôn đặt câu hỏi và xác thực thông tin từ các **nguồn chính thống** và đáng tin cậy. Đừng vội tin tưởng hoàn toàn vào bất kỳ hình ảnh hay video nào trên mạng xã hội.

# Trách nhiệm của chúng ta

## Nâng cao cảnh giác

- 1 Không chia sẻ hoặc lan truyền các video, hình ảnh chưa được kiểm chứng. Mỗi lượt chia sẻ có thể góp phần phát tán thông tin sai lệch.

## Bảo vệ thông tin cá nhân

- 2 Hạn chế đăng tải hình ảnh, video riêng tư trên mạng xã hội để tránh bị kẻ xấu lợi dụng tạo Deepfake.

## Xác thực thông tin

- 3 Trước khi tin tưởng và hành động dựa trên bất kỳ thông tin nào, hãy xác thực qua nhiều nguồn uy tín.

## Tham gia xây dựng pháp lý

- 4 Ủng hộ các tổ chức, chính phủ trong việc xây dựng khung pháp lý và công cụ kỹ thuật để phát hiện, xử lý Deepfake.

## Giáo dục cộng đồng

- 5 Cùng nhau giáo dục, nâng cao nhận thức của cộng đồng về nguy cơ và cách phòng tránh FDeepfake.

# Kết luận: Đối mặt với thách thức Deepfake

## Con dao hai lưỡi

Deepfake là một **công nghệ "con dao hai lưỡi"**: nó mang lại tiềm năng sáng tạo to lớn nhưng cũng tiềm ẩn những nguy cơ nghiêm trọng đối với cá nhân và xã hội.

## Tỉnh táo & trang bị

Để đối phó, chúng ta cần tỉnh táo, không ngừng trang bị kiến thức và các công cụ cần thiết để nhận diện, từ đó ngăn chặn những tác hại khôn lường mà Deepfake có thể gây ra.

## Bảo vệ sự thật

Đây là trách nhiệm chung của toàn xã hội trong việc bảo vệ sự thật, củng cố niềm tin và duy trì an toàn trong kỷ nguyên số, nơi thông tin có thể bị thao túng dễ dàng.

"Đừng mù quáng tin vào những gì bạn nhìn thấy – máy ảnh và AI có thể nói dối!"



# Cảm ơn và Hỏi đáp

Mời quý vị đặt câu hỏi và chia sẻ kinh nghiệm về Deepfake.

Cùng nhau xây dựng môi trường số an toàn, minh bạch và đáng tin cậy.

