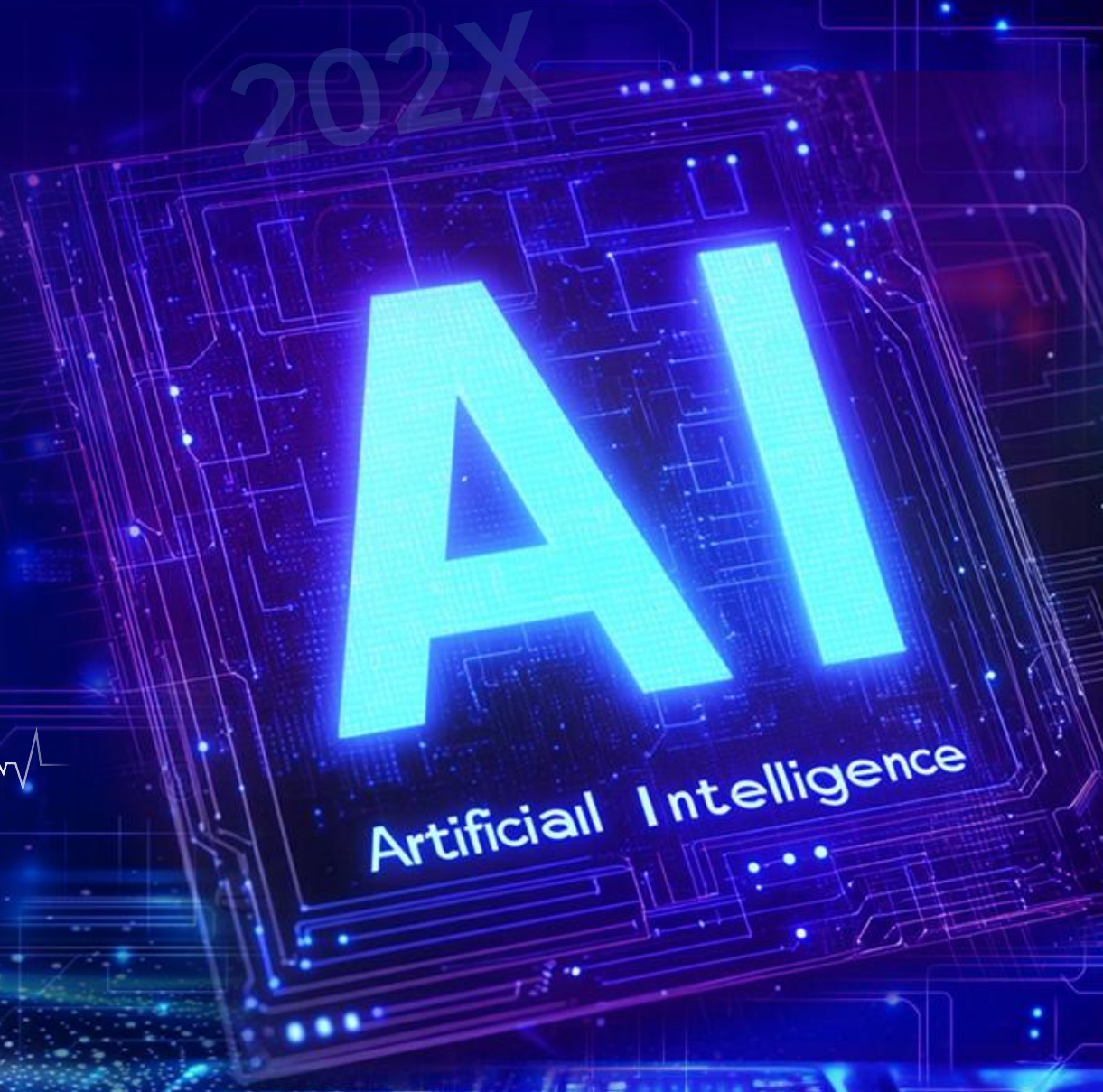
AI Scams:
Basics, Cases & Prevention

Senior Inspector LEUNG Sin-yi Cindy



01

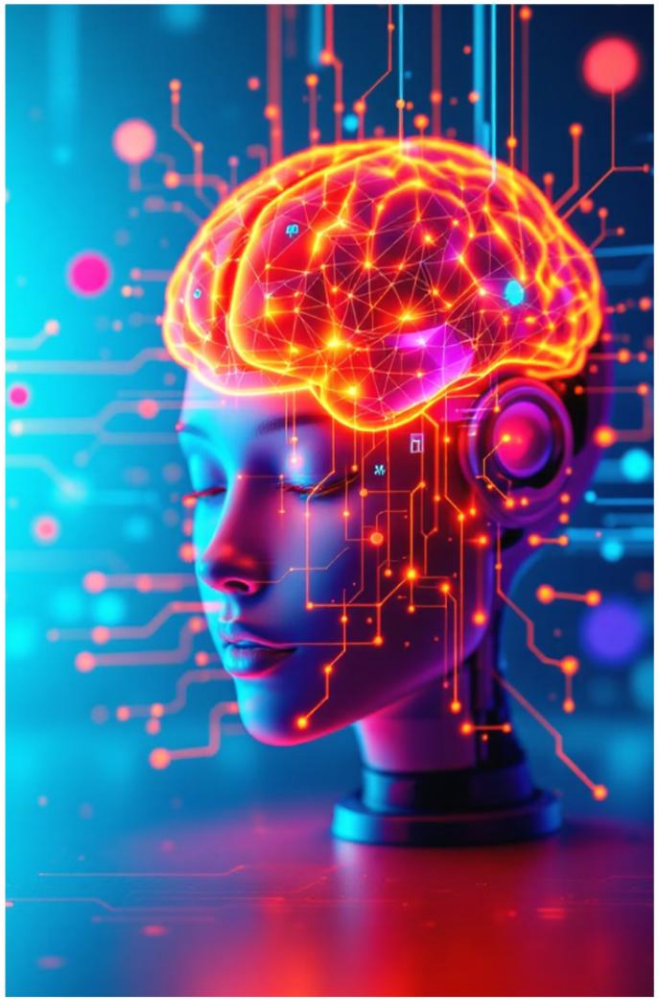
Introduction to AI Scams

Definition of AI Scams

Basic Concept

AI scams are fraudulent activities that use artificial intelligence to deceive people. They exploit AI's ability to mimic human behavior and create convincing false content.

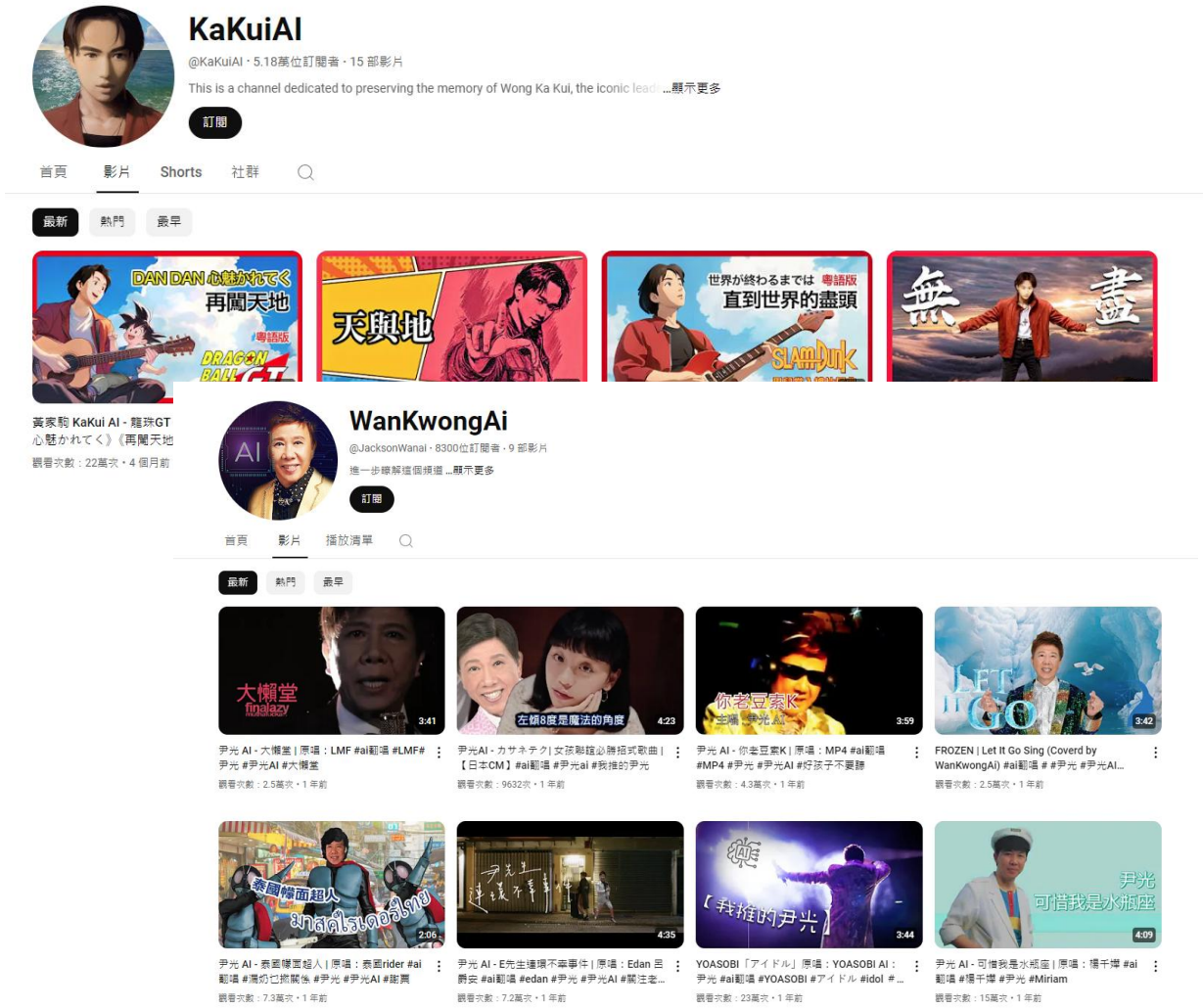
These scams can take many forms, including fake videos, websites, emails, and chatbots, all designed to trick victims into giving away sensitive information or money.



02

Common Types of AI Scams

Deepfake Videos/Audios



Deceptive Nature

Deepfake videos and audios can convincingly imitate people’ s voices and appearances. They are used to create fake news or impersonate individuals in financial scams.

Deepfake Videos/Audios

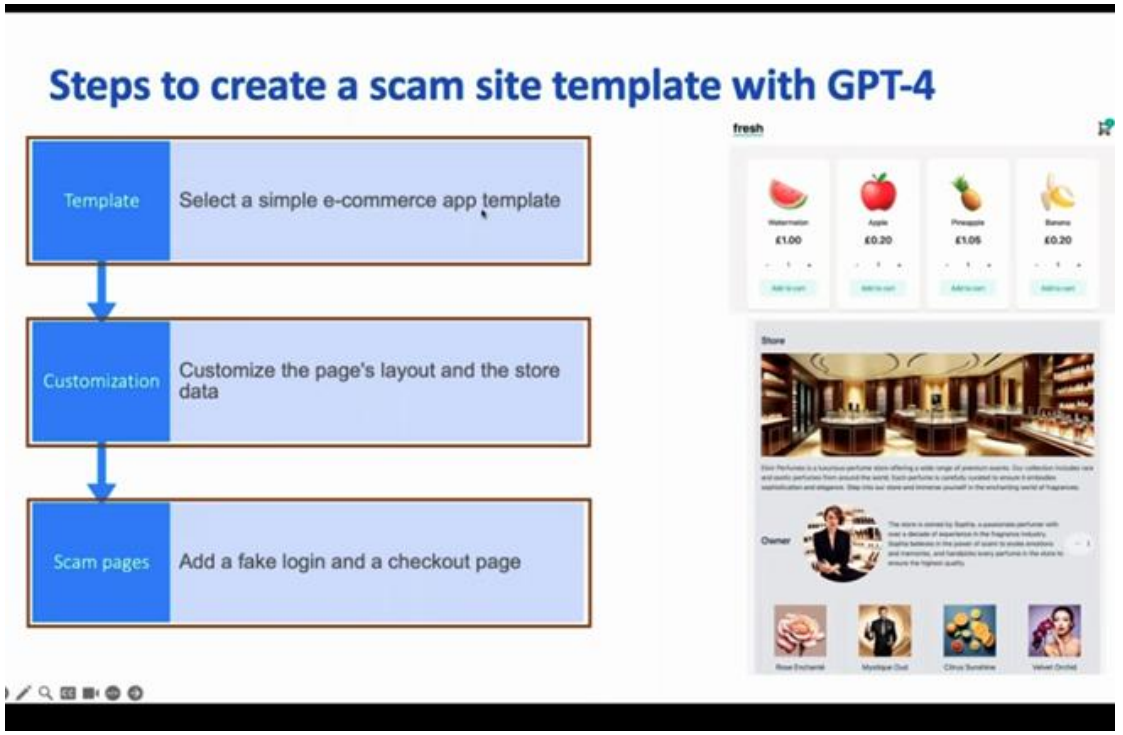
Deepfake Videos/Audios

AI-Generated Fake Websites and Apps

Fake websites and apps created by AI look very similar to real ones. They use AI to generate realistic interfaces and content to trick users into providing personal information.

These fake platforms often mimic popular services, such as online banking or e- commerce sites, to steal user credentials and financial data.

Appearance and Function



AI-Powered Phishing Emails and Messages

Persuasive Techniques

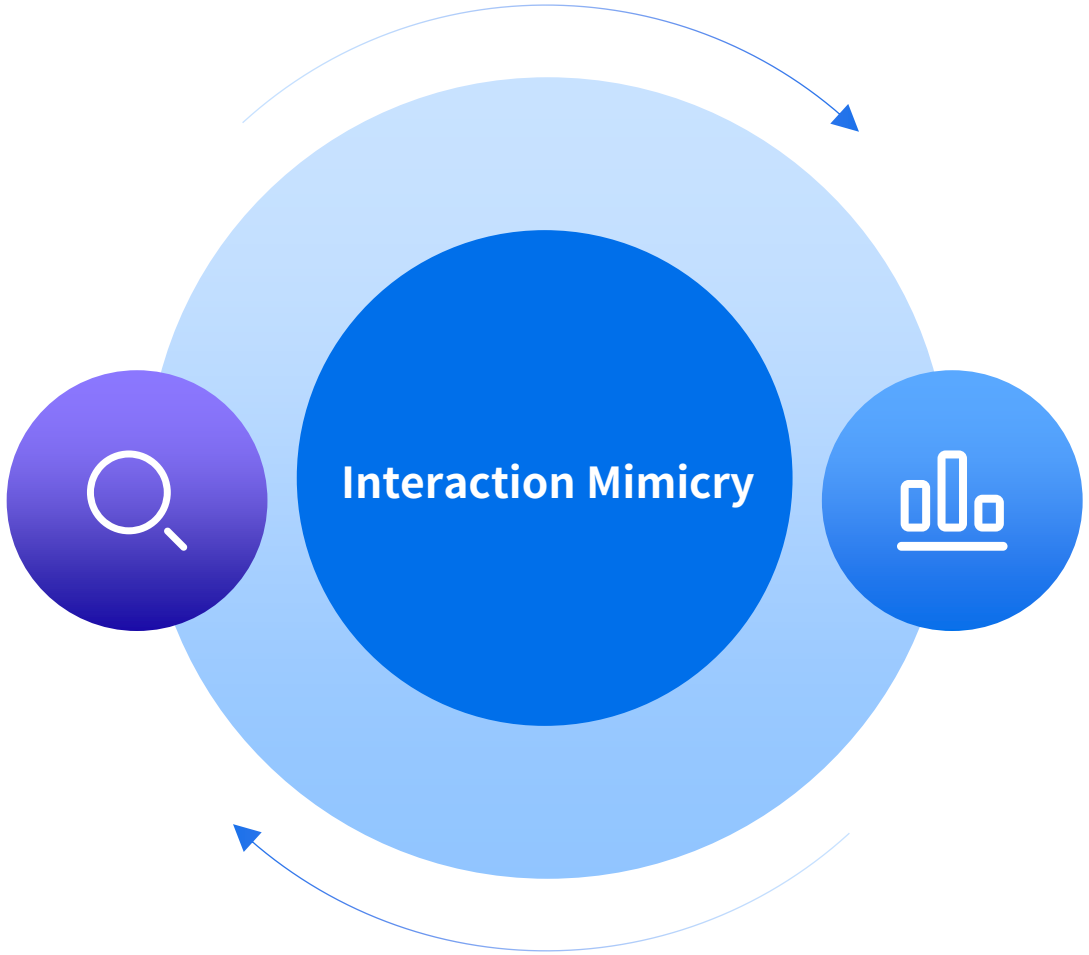
AI can generate phishing emails and messages that are highly convincing. They use natural language processing to create content that looks like it comes from a trusted source.

These emails often contain urgent requests for personal information or links to fake websites, exploiting people’ s trust and fear of missing out.

AI Chatbot Impersonations

01

AI chatbots can impersonate real people in online conversations. They use machine learning to respond in a way that seems human, making it difficult to detect the deception.



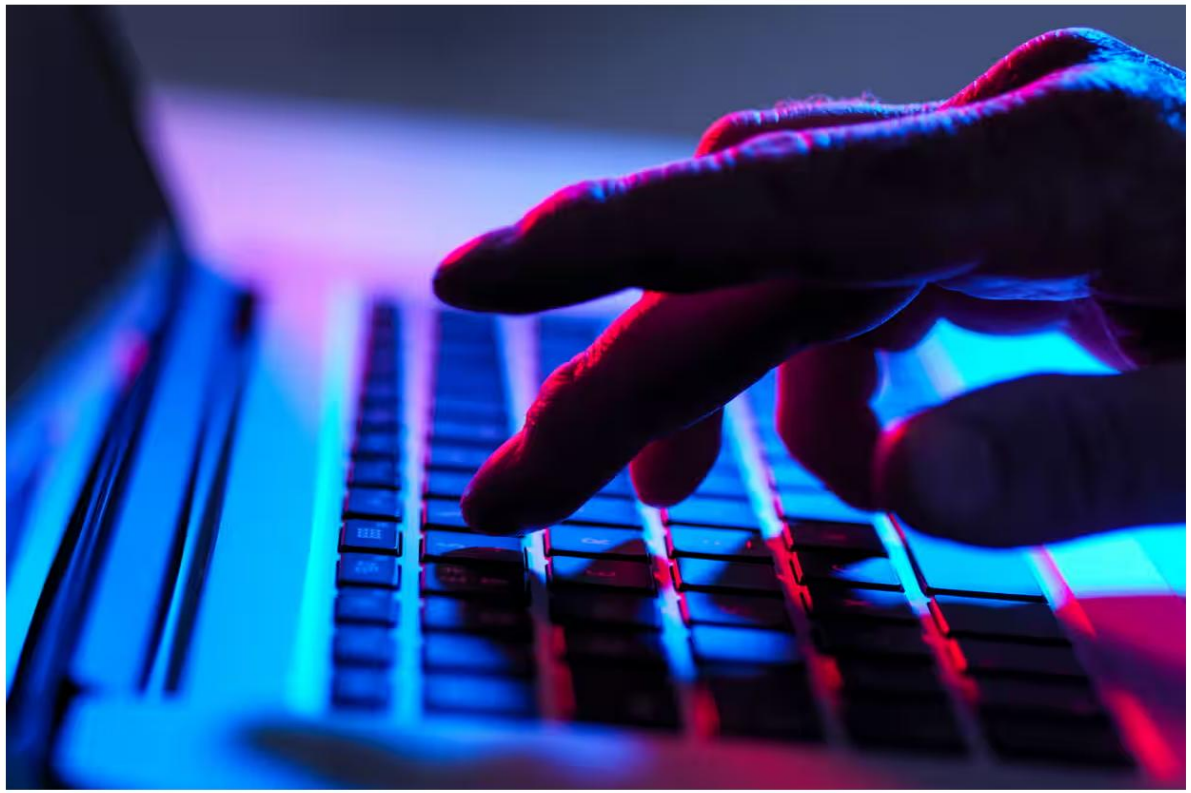
02

These chatbots can be used to gather personal information or persuade people to take actions that benefit the scammers, such as clicking on malicious links.

AI Chatbot Impersonations

A man stalked a professor for six years. Then he used AI chatbots to lure strangers to her home

James Florence, 36, agreed to plead guilty after using victim's information to guide chatbots in impersonation



Photograph: Andrew Brookes/Getty Images/Image Source

03

How Deepfake Technology Works

Data Collection

Deepfake technology requires a large amount of data to train the AI model. This includes images, videos, and audio recordings of the person to be imitated.

Scammers collect this data from various sources, such as social media, public records, and leaked databases, to create realistic deepfakes.

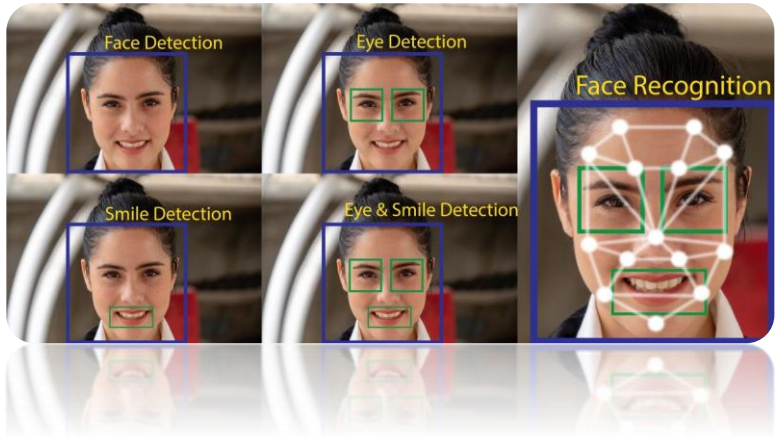
Training the AI Model

Machine Learning Process

The AI model is trained using the collected data. Machine learning algorithms analyze the data to learn the patterns and characteristics of the person’ s appearance and behavior.

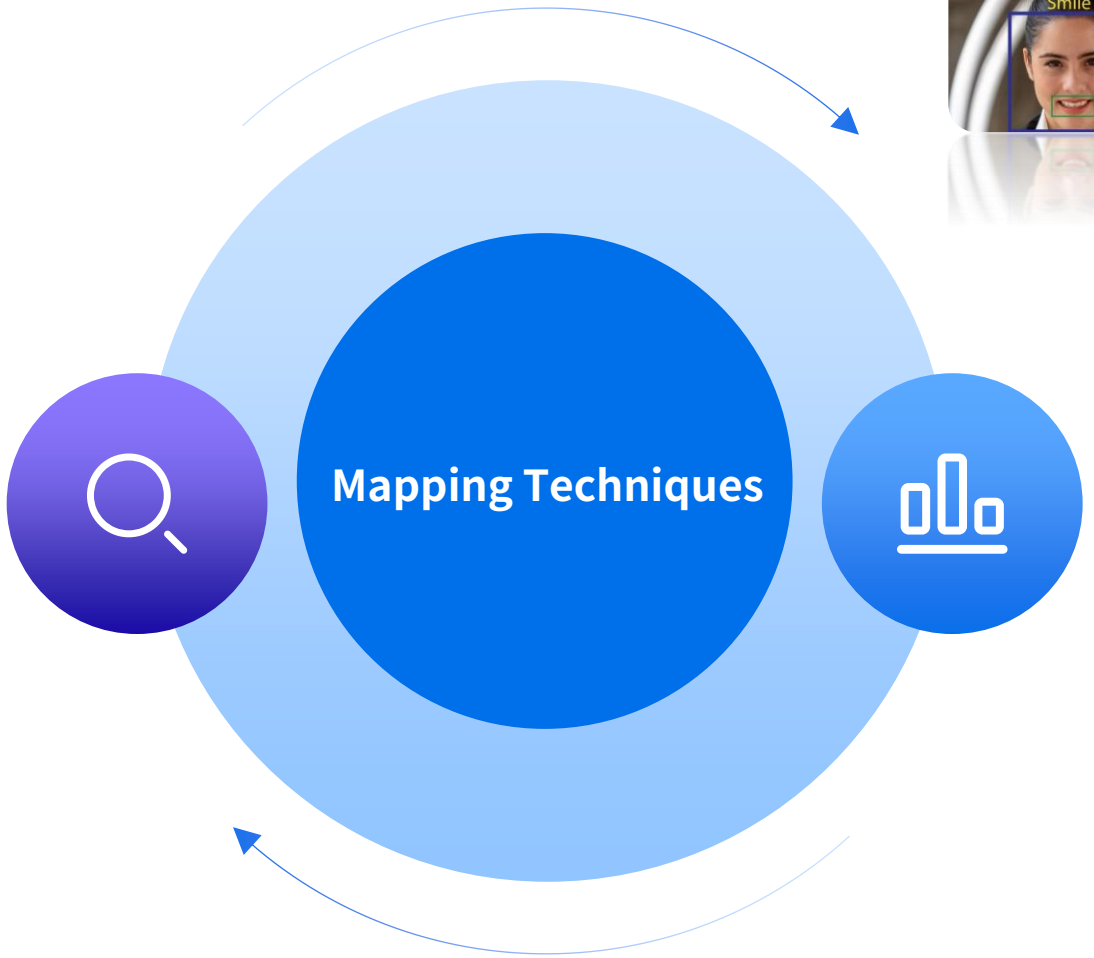
This process involves complex computations and adjustments to the model, making it more accurate and convincing over time.

Face/Expression Mapping



01

Face and expression mapping is a crucial step in creating deepfakes. The AI model maps the facial features and expressions of the person to be imitated onto a different face.



02

This involves detailed analysis of facial landmarks and movements, ensuring that the deepfake looks natural and realistic.

Neural Network Generation

Creating the Deepfake

The neural network generates the deepfake by combining the mapped facial features with the trained model. It creates a video or audio that closely resembles the original person.

The generated deepfake can be further refined to improve its quality and realism, making it harder to detect.

Refinement and Post-Processing

Enhancing Realism

Refinement and post- processing are used to enhance the realism of the deepfake. This includes adjusting lighting, color, and other visual elements to make it look more authentic.

01

The goal is to create a deepfake that is indistinguishable from the real person, making it a powerful tool for deception.

02

Limitations of Old vs. New Deepfake Technology

1

Old deepfake technology had many limitations, such as noticeable flaws in facial expressions and movements. However, new technology has significantly improved, making deepfakes more realistic.

2

Modern deepfakes can now be created with higher resolution and more accurate movements, making it harder to detect them without specialized tools.

Technological Evolution

04

Case Study 1 - AI Deepfake Scam in Finance Industry

Case Study:1 - Finance Industry Deepfake

Initial Contact

Finance employee received email from "CEO" requesting urgent video call.

Deepfake Conference

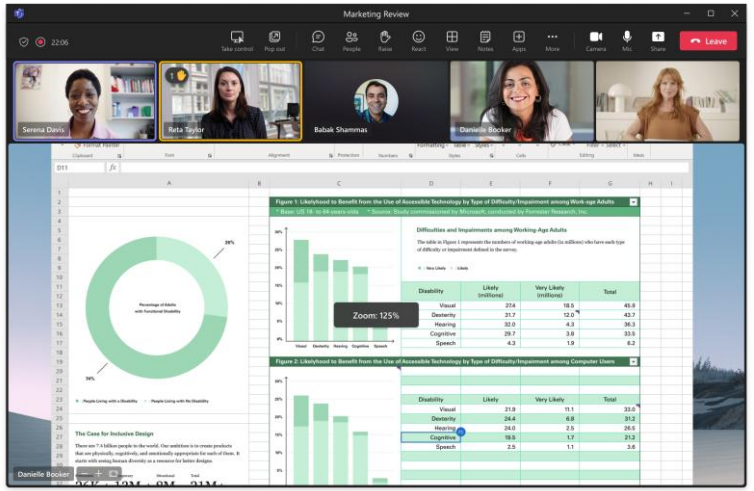
Scammers used pre-recorded video with AI-generated responses.

Fund Transfer Request

Fake executive requested immediate transfer of HK$3.8 million.

Scripted Evasion

Scammers avoided real-time interaction using prepared responses.



Hong Kong / Law and Crime

‘Everyone looked real’: multinational firm’s Hong Kong office loses HK$200 million after scammers stage deepfake video meeting

- Employee fooled after seeing digitally recreated versions of company’s chief financial officer and others in video call
- Deepfake technology has been in the spotlight after fake explicit images of pop superstar Taylor Swift spread on social media sites

Case Study:1 - Finance Industry Deepfake

Avoiding Real-Time Interaction

Scammers used scripted segments to avoid real- time interaction. They carefully planned the video content to minimize the need for live responses, making it harder to detect the deception.

The deepfake video was designed to look seamless, with the fake executive appearing to give instructions and provide information as if it were a real meeting.

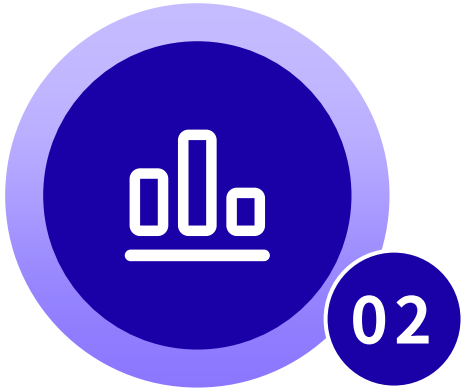
05

Detecting Deepfakes

Unnatural Movements

Eyes and Mouth

One way to detect deepfakes is to look for unnatural movements in the eyes and mouth. Deepfakes often struggle to accurately replicate these complex movements, leading to noticeable flaws.



For example, the eyes may not blink naturally, or the mouth movements may not sync perfectly with the spoken words.

Simple Actions Test

Finger Across Face

Asking the person to perform a simple action, such as crossing their face with a finger, can help detect deepfakes. Computers struggle with sudden changes and can give themselves away.

If the person in the video cannot perform the action or it looks unnatural, it may be a deepfake.

Computer Struggles

Sudden Changes

Computers have difficulty handling sudden changes in movements or expressions. These struggles can be detected by closely observing the video for any inconsistencies or unnatural behavior.

For example, a sudden change in lighting or a quick head movement may reveal flaws in the deepfake.

Detecting Deepfakes

06

Case Study 2 - Loan Fraud Involving AI Deception

Case Study 2
- Loan Fraud Involving AI Deception

Identity Theft

Scammers collected personal data from social media profiles.

Document Forgery

AI generated realistic financial statements and identification papers.

Fraudulent Loans

Multiple loans approved using victim's identity, funds immediately transferred overseas.

Virtual Impersonation

AI voice cloning used in verification calls with financial institutions.

07

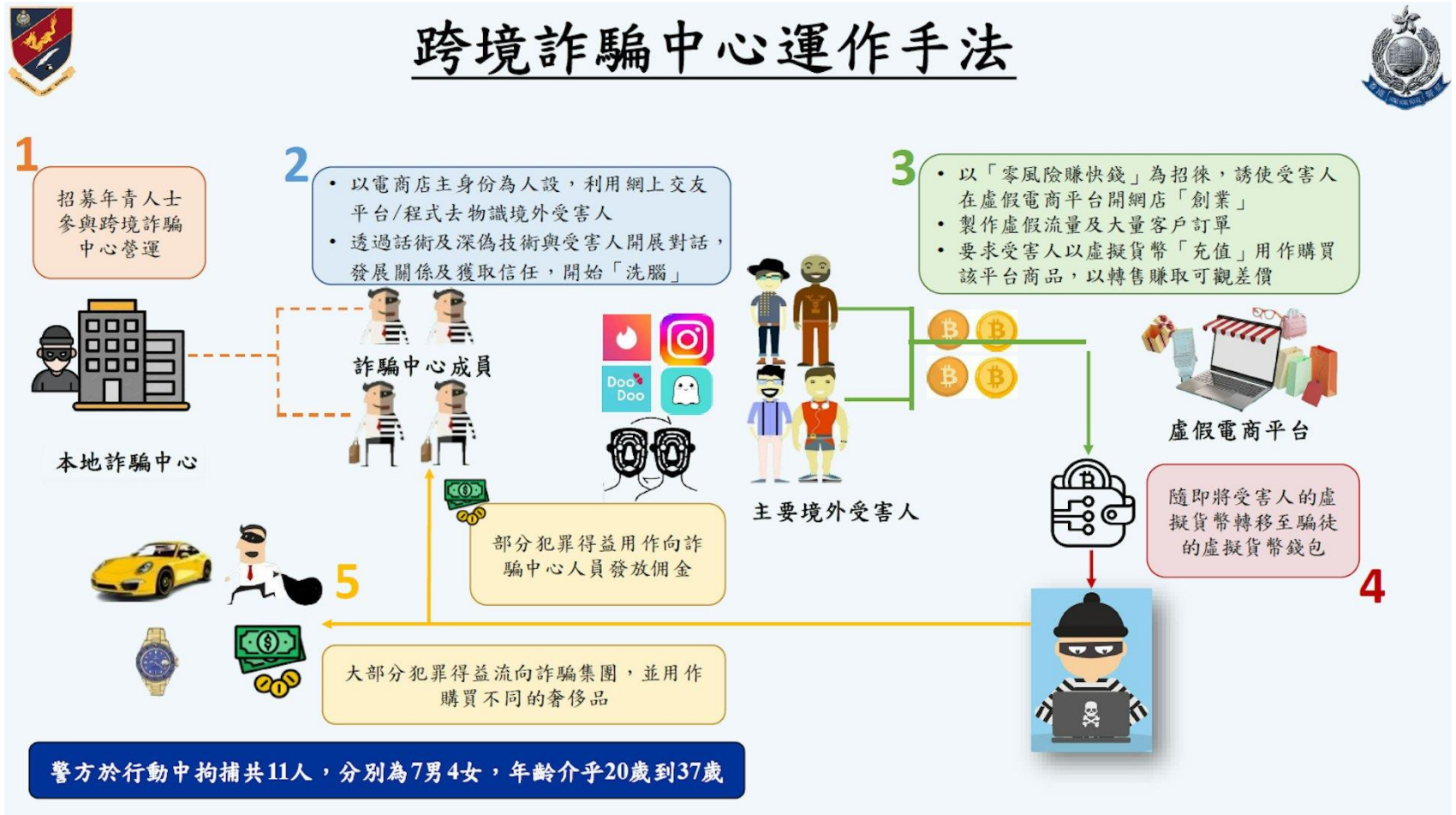
Case Study 3 - Scam Centre of AI Face-Swapping Fraud

Case study - Scam Centre of AI Face-Swapping Fraud

港聞 / 突發

警破工廈詐騙中心　揭AI換臉扮「美女」氹開電商平台　一周騙百萬

撰文：凌逸德
出版：2025-04-19 13:25　更新：2025-04-19 17:40



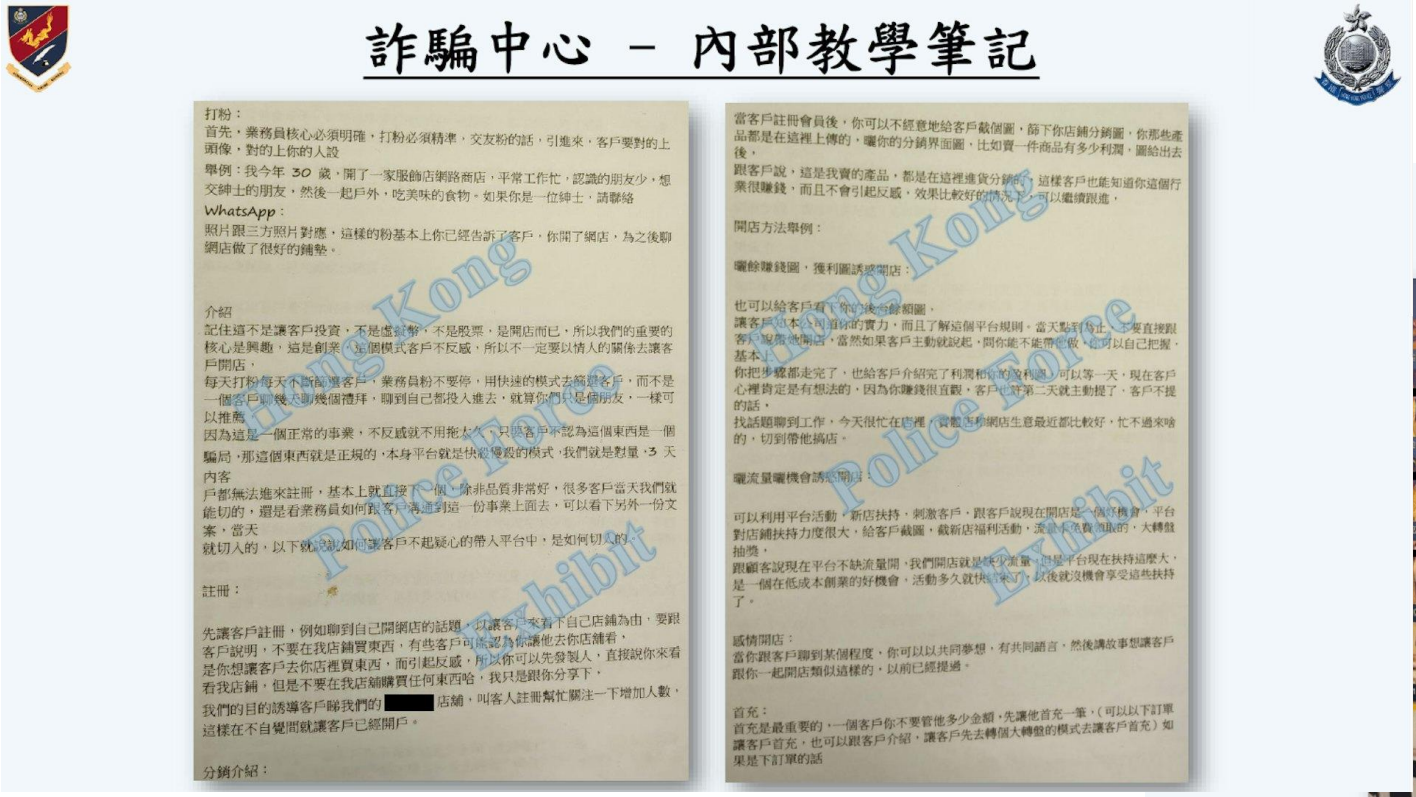
Case study - Scam Centre of AI Face-Swapping Fraud

港聞 / 突發

警破工廈詐騙中心　揭AI換臉扮「美女」冚開電商平台　一周騙百萬

撰文：凌逸德
出版：2025-04-19 13:25　更新：2025-04-19 17:40

74



08

Prevention Strategies for Individuals

Prevention Strategies for Individuals

Question Unexpected Communications

Be wary of urgent requests. Verify through separate, established channels.

Verify Identity

Call official numbers directly. Never use contact details provided in suspicious messages.

Use Multi-Factor Authentication

Enable MFA on all accounts. Biometric verification adds an extra security layer.

Stay Informed

Learn about latest scam techniques. Knowledge is your best defence.

09

Prevention Strategies for Organizations

Implementing MFA for Remote Access

Secure Remote Connections

Implement MFA for remote access to your organization’ s systems. This ensures that only authorized personnel can access sensitive information and reduces the risk of unauthorized access.

MFA helps prevent AI- generated scams from compromising your organization’ s security.

Conducting IT Account Audits

Removing Unnecessary Accounts

Conduct regular IT account audits and remove unnecessary accounts. This helps minimize the risk of unauthorized access and ensures that only active employees have access to your systems.

Regular audits also help detect any suspicious activity or unauthorized accounts.

Enabling Log Monitoring

Alert Notifications

Enable log monitoring and set up alert notifications. This allows you to detect any unusual activity or potential security breaches in real- time.

01

You can configure alerts for suspicious login attempts, unauthorized access, or other unusual behavior.

02

Keeping Systems and Software Up-to-Date

Security Patches

Keep all operating systems and software up- to- date. Regular updates and security patches help protect your systems from known vulnerabilities and reduce the risk of AI- generated scams.

Ensure that your IT team regularly checks for updates and applies them promptly.

Training Employees

Train employees to recognize AI- generated scams. Provide regular training sessions and resources to help employees identify suspicious communications and avoid falling victim to scams.

This helps create a security- aware culture within your organization and reduces the risk of successful AI scams.

Recognizing AI Scams

10

Available Resources and Support

CyberDefender.hk

Cyber Knowledge Platform

CyberDefender.hk is a one- stop cyber knowledge platform that provides valuable information and resources on cybersecurity. It offers articles, videos, and tools to help individuals and businesses stay safe online.

Scameter / Scameter+

Checking Suspicious Contacts

Scameter and Scameter+ are tools designed to check suspicious contacts and transactions. They provide real- time alerts and information to help you identify potential scams.

These tools can be used by both individuals and businesses to stay vigilant and avoid falling victim to AI- generated scams.

Support for Organizations

Awareness Programme

Vulnerability Disclosure Program