

# Generative Artificial Intelligence (AI) & Fraud

# Generative AI & Fraud

Fraudsters may use generative AI to scam people and businesses. To help protect yourself, it's important that you understand the different types of scams and what to look out for.

How could generative AI help fraudsters?

- **Enhanced email phishing** - While most scam emails are still basic, fraudsters could use generative AI to create more sophisticated emails that are perfectly written, and even copy the tone of voice of trusted people or businesses. This could make phishing emails harder to spot.
- **Voice spoofing** - Voice spoofing (or voice cloning) uses generative AI to copy a person's voice. The copied voice can then say certain phrases or act as a chatbot. Compared to other scams, voice spoofing is rare. However, this technology could help fraudsters to enhance the effectiveness of their scams.
- **Deepfakes** - A deepfake uses generative AI to copy the appearance and voice of a person. Deepfake videos can be convincing, usually showing the copied person saying things they've never said.

## What's AI?

- Artificial Intelligence (AI) is technology that allows computers to perform tasks and make decisions like a human. AI tools make these decisions by learning, they do this by analysing large amounts of data and looking for patterns.
- These decisions improve as the AI tool takes in more data. With enough data, an AI tool can make decisions similar to how a human would. This helps scammers try to impersonate people or businesses.

# How can you protect yourself against these threats?

Deepfakes enhance a fraudsters ability to social engineer their victims. That said, lots of existing controls remain effective for mitigating against this risk. Some key controls are noted below.

## Maintain usual fraud controls

- Always check and validate information you receive in emails and/or online, especially in forums or open-source websites. If you're unsure, check with a line manager or a genuine HSBC employee.
- Be mindful of emails, phone calls, and videos that want you to act quickly – this is often a sign of a scam.
- Caution against requests for personal information, account information, and financial information, HSBC will not request this information from you.
- Ensure that, wherever possible, you only take payment instructions from approved company communication channels. Fraudsters will often have to contact victims via open communication channels like WeChat, QQ, Dingding, WhatsApp and etc., as they are unable to access approved company channels.

## Security Codes

Security codes are unique, time-sensitive codes generated and distributed to authorized personnel. These codes can be used to authenticate communications and transactions, adding an additional layer of security that is difficult for fraudsters to replicate. Here's how they can be implemented effectively:

- **Unique Codes:** Generate a unique code to be used by employees.
- **Secure Distribution:** Distribute these codes via secure channels such as encrypted emails, or through internal secure platforms.
- **Verification Processes:** Require the code to be presented during sensitive transactions, high-value communications, or any situation where identity verification is critical.

## Human Oversight & Training

- **Human Oversight:** Maintain a level of human oversight for approving large or unusual transactions. Conducting business in person is not always possible but for significant transactions can act as a key control.
- **Deepfake Awareness:** Educate employees about the risks of deepfakes and how they can be used in fraud schemes. Training should cover how to recognize potential deepfake attempts and the importance of adhering to security protocols.
- **Phishing Awareness:** Provide ongoing training to help employees identify and respond appropriately to phishing attempts, which are often the precursor to more sophisticated attacks.

# Spotting A Deepfake - Additional Guidance



The rapid innovation in AI may mean that in the future deepfakes could become nearly indistinguishable from reality. Whilst these tips can help you to detect less sophisticated attacks, additional controls should be considered.



- 1 Glasses may appear odd, reflect differently or even disappear.
- 2 The persons features may be positioned incorrectly or move unnaturally.
- 3 The persons skin or hair may appear blurry or move.
- 4 The audio might not sync or match the video. Listen out for changes in tone and volume.
- 5 The background might not fit the context of the call. It may show strange reflections or anomalies.
- 6 The lighting may seem off. There may be strange shadows.

本文件由汇丰银行(中国)有限公司(“汇丰”)提供。

This document is issued by HSBC Bank (China) Company Limited (“HSBC”).

本文件仅用于阐述及说明之目的，不会产生由汇丰承担的任何合同承诺。本文件全部或部分并不构成要约、邀请或业务招徕。汇丰仅受其认可的正式书面协议下创设的合同承诺的约束。

This document is for reference and illustrative purposes only and shall not be capable of creating any contractual commitment on the part of HSBC. HSBC shall only become contractually bound on formal written agreement acknowledged by HSBC as creating such contractual commitment.

本文件所载信息可能来源于汇丰信任但未经验证的第三方。汇丰将尽力确认本文件所载信息于发布之日及时、完整且准确，但汇丰对本文件内容的准确性、完整性或与接受人意图的相关性不作保证，且汇丰不承诺亦无义务向接受人提供任何额外信息、更新本文件全部或部分内容、或更正任何可能显见的不准确处。本文件不构成汇丰向接受方提供的任何咨询、建议及/或顾问服务。汇丰不就接受人及/或任何其他人士因使用或依赖本文件中的任何建议而招致的任何直接或间接损失承担责任或义务。接受人应自行负责对本文件所涉产品、服务和其他内容做出独立评估。汇丰建议接受人向法律、监管、税务、财务和会计顾问进行咨询。

The information contained in this document may include information from third parties who HSBC believes to be reliable but such information will not have been independently verified by HSBC. HSBC will try to ensure such information is current, accurate and complete at the date of publication, HSBC does not warrant that the contents of this document are accurate, sufficient or relevant for the recipient’s purposes and HSBC gives no undertaking and is under no obligation to provide the recipient with access to any additional information or to update all or any part of the contents of this document or to correct any inaccuracies in it which may become apparent. HSBC will not accept liability for any direct, indirect or consequential losses arising from the use of or the reliance on the information contained in this document by any person. You are responsible for making your own evaluation about the products referred to in this document. You are recommended to consult with suitably qualified professional advisers to obtain the appropriate financial, legal, accounting, tax or other advice before making any decision or take any action that might affect you or your business.

© 版权所有。汇丰银行（中国）有限公司2024。未事先征得汇丰银行（中国）有限公司之书面许可，不得通过电子、机械、影印、录制或其它任何形式或方式复制、于检索系统中保存或转载文中之任何内容。

Copyright: HSBC Bank (China) Company Limited 2024. ALL RIGHTS RESERVED. This document should not be photocopied, reproduced, distributed or disclosed in whole or in part to any other person without the prior written consent of HSBC.