

# 生成式人工智能(AI) 与诈骗

# 生成式AI与诈骗

犯罪分子可能利用生成式AI对个人和企业实施诈骗。为保障自身利益，了解诈骗的不同类型和注意事项尤为重要。

诈骗分子如何利用生成式AI犯罪？

- **增强钓鱼电邮的攻击能力**——尽管大多数诈骗电邮仍采用基础模式，但犯罪分子已能够利用生成式AI编写出更为复杂的邮件，内容堪称完美，甚至模仿值得信赖的个人或企业的语气，因而令钓鱼电邮更难识别。
- **语音欺诈**——语音欺诈或语音克隆是利用生成式AI复制个人的声音。复制的声音可以说出特定的短语或充当聊天机器人。与其他诈骗方式相比，语音欺诈更少见，但这项技术能够帮助诈骗分子提高其诈骗的有效性。
- **深伪技术**——深伪技术利用生成式AI复制别人的外貌和声音。深伪视频非常逼真，通常是出现被复制人说一些他们从来没说过的话。

## AI是什么？

- 人工智能(AI)是一种令电脑像人类一样执行任务和决策的技术。AI工具通过学习做出这些决策，并通过分析大量数据和发掘当中的模式来实现。
- AI工具获得的数据越多，其决策越准确。有了足够的数据，AI工具就能够做出与人类相似的决策。这就可以帮助诈骗分子试图冒充个人或企业。

# 如何保障自己免受这些威胁？

深伪技术提高诈骗分子对受害人实施社交工程攻击的能力。话虽如此，但现有的许多控制措施仍能有效缓减这些风险。下面列出部分关键控制措施。

## 维持一般防范诈骗控制措施

- 务必检查和验证你通过电邮和/或在线上收到的信息，尤其是来自论坛或开源网站。如你不确定，请与你的直属经理或真实的汇丰员工核对。
- 那些要求你迅速行动的电邮、电话及视频电话尤其要注意——这些通常是诈骗的迹象。
- 要小心那些向你索取个人信息、账户信息和财务信息的请求，汇丰不会向你索取这些信息。
- 请确保尽可能只接收来自已获审核的公司通讯渠道的支付指示。由于诈骗分子无法访问获审核的公司通讯渠道，他们通常会通过微信、QQ、钉钉、WhatsApp等公开通讯渠道联系受害人。

## 安全密码

安全密码是生成并分发给授权人员的唯一且具有时效敏感性的密码。这些密码可用于验证通讯和交易，额外增加一层安全保障，令诈骗分子难以复制。以下是其如何有效实施的方式：

- **唯一密码：**生成唯一密码供员工使用。
- **安全分发：**通过加密电邮或内部安全平台等安全渠道分发这些密码。
- **验证流程：**要求在敏感交易、重要通讯或任何身份验证至关重要的情况下提供密码。

## 人工监控及培训

- **人工监控：**对审批大额或不寻常交易保留一定程度的人工监控。在经营业务时，我们不可能做到事事亲力亲为，但在执行重要交易，亲力亲为就可发挥关键控制作用。
- **防范深伪诈骗意识：**训练员工认识深伪技术的风险及如何用其来实施诈骗计划。培训应涵盖如何识别潜在深伪诈骗企图及遵守安全协议的重要性。
- **防范网络钓鱼意识：**持续提供培训，帮助员工识别网络钓鱼企图并作出适当的应对，因为网络钓鱼企图通常是更复杂攻击的前兆。

# 发现深伪诈骗——补充指引



AI快速创新迭代，这可能意味着未来的深伪骗术可以做到近乎以假乱真。虽然这些小贴士可以帮助你发现不太复杂的攻击，但仍需考虑采取额外的控制措施。



- 1 眼镜看上去可能有点奇怪，反射的影像不同，甚至消失。
- 2 人物特征可能位置不对或动作不自然。
- 3 人物的皮肤或头发可能看起来很模糊或者在动。
- 4 音频可能与视频不同步或不匹配。细心留意音调和音量的变化。
- 5 背景可能与通话的内容不符，并可能出现奇怪的反射或异常现象。
- 6 光线可能看起来不对，并可能出现奇怪的影子。

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.