生成式人工智能(AI)与诈骗

人工智能诈骗

骗徒可能利用生成式人工智能来欺骗个人和企业

为保障自身及企业安全，了解骗徒如何运用此技术至为重要。

生成式人工智能已成为骗徒所使用诈骗手法的工具之一，使诈骗手法更逼真。由于此技术能模仿语言风格，甚至复制影像及声音，骗徒更容易冒充您熟悉及信任的人士或企业。

常见手法包括：

- **语音冒充**–骗徒致电企业员工，冒充公司行政总裁，指示员工将一笔「机密」款项汇入一个暂记账户。由于员工误以为正在与行政总裁通话，便批准了该笔付款。
- **深度伪造技术 (deepfake)** –骗徒可能会复制供应商公司某位成员的完整外貌与声音，以冒充其身份。骗徒假扮成已知的供应商公司代表，安排与付款方公司通话，并要求更改银行账户资料。由于负责付款的同事误以为自己「亲眼见到」熟悉的供应商代表，便批准更改银行账户资料。

什么是生成式人工智能？

- 人工智能（AI）是一种允许电脑模仿人类思维和决策的技术。人工智能通过分析大量数据并不断学习，从而使所作出的决策更贴近人类思维模式。
- 随着人工智能接收及分析更多数据，人工智能的决策将不断改进，并能够做出 与人类相似的决策，这使得骗徒更容易冒充人或企业。
- 生成式人工智能则运用相同技术来创造内容，包括文字、图像、影片及 / 或音讯。

请勿假设电话或视像通话必定真实可信。如对方要求提供敏感资料、指示向新受款人付款，或施加压力要求即时行动，请格外警惕。企业应设有清晰明确的增加新受款人的付款程序。无论员工对受款人有多大信任，该程序亦不应被绕过。

如何保护自己免受这些威胁？

深度伪造提高了骗徒诱骗受害者的能力。虽然如此，很多现行的措施仍能有效降低这些风险。以下介绍了一些关键的防骗措施。

谨记常用的防诈骗措施

- 特别留心那些要求您迅速采取行动的短讯/电邮/电话/影片——这些通常是诈骗的迹象。
- 请注意，恒生绝不会通过电邮或短讯要求你提供任何个人或公司帐户资料及财务资料。
- 确保尽量只接受来自已批准的公司通讯渠道传送的付款指示。骗徒通常透过 WhatsApp 等公开通讯渠道联络受害者，因为他们无法使用经批准的公司渠道。
- 务必检查和验证从短讯/电子邮件/ 网上收到的资讯，尤其是在任何人都可以发布帖文的论坛或网站。如果不确定信息真伪， 请与客户经理确认。

每日安全代码

每日安全代码是每日产生的独特且具时效性的代码，仅分发予获授权人员。这些代码可用作验证通讯及交易，为防骗加设一重难以被骗徒复制的安全保障。以下是有效实施方式：

- **每日独立代码**：每日产生一组独特代码，供员工使用。
- **安全分发**：透过加密电邮或公司内部安全平台分发代码。切勿与组织外部人士分享代码。
- **核实程序**：在敏感交易、高价值通讯或任何需要身份验证的情况下，要求提供当日代码。

监察及培训

- **人工审核**：针对大额交易或异常交易的审核，制定合适的内部控制机制，包括设定交易限额，日终跟踪异常交易，并设定多于一人作交易批核。在执行重要交易时，建议当面进行交易，避免损失。
- **网络钓鱼防范意识**：为员工提供持续的培训，帮助员工辨识并懂得应对网路钓鱼攻击。网络钓鱼攻击通常是接连其他更精密的攻击。
- **深度伪造防范意识:** 教导员工了解深度伪造技术的风险 以及骗徒如何将其用于欺诈。培训应涵盖如何辨识深 伪诈骗、遵守保密协定的重要性，以及如何举报可疑活动。

如何分辨深度伪造技术 - 额外指引

人工智能技术迅速发展，意味着深度伪造 (deepfake) 内容将愈来愈难与真实影像分辨。虽然以下建议有助识别较低阶的伪造手法，但仍应考虑额外的控制措施以加强防范。

请记住：即使对方的外貌与声音看似来自您公司内部人士，若其要求异常，仍应保持怀疑态度。对于大型或不寻常的交易，维持一定程度的人工审批始终是良好做法。

1. 眼镜会产生反光，无法正常呈现光照的自然物理特性
2. 面部表情不自然或五官位置异常，或身体移动方式不自然
3. 头发或皮肤可能呈现模糊或异常移动
4. 口型无法对上。注意聆听音调和音量的变化
5. 背景可能与通话场景不符。可能会显示奇怪的反射或异常现象
6. 似乎没有开灯或有奇怪的阴影。