恒生銀行
HANG SENG BANK

生成式人工智慧(AI)和诈骗

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，为了保护您或您的企业免受诈骗威胁，本指引将助您进一步了解不同类型的诈骗手法，以及需要注意的事项。

如何运用生成式人工智能进行诈骗?

- 增强网络钓鱼电邮 – 虽然网络钓鱼电邮仍是常见的诈骗方法，但骗徒透过人工智能，甚至可以模仿受信任者的语气和态度制作出更巧妙的诈骗电邮。增加了钓鱼电邮的辨认难度。

- 语音钓鱼 – 语音钓鱼利用生成式人工智能复制一个人的声音，甚至能像聊天机器人一样表达特定的语句。相较于其他诈骗手法，虽然语音诈骗情况并不常见，但这项技术仍然能够协助骗徒成功诈骗。

- 深度伪造技术 – 深度伪造利用生成式人工智能来复制一个人的外貌和声音。深度伪造影片能做到非常真实可信，通常会模仿被复制的人说出从未说过的话语。与语音钓鱼类似，深度伪造诈骗案例并不常见，但仍然需要提高警觉。

什么是人工智能?

- 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。

如何保障自己免受这些威胁?

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

- 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。

- 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。骗徒通常通过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通讯渠道。

流动保安编码

流动保安编码是具有唯一性和时效性，并只可给予授权人员的编码。这些编码可用于验证通讯和交易，骗徒难以复制，从而加强了防御。您可参照以下方式有效使用和保护流动保安编码：

- 切勿向未经授权的人员透露您的任何身份验证方法，包括发送到您注册的行动或安全设备的密码、一次性安全代码和一次性密码 (OTP)

- 保密传送：通过加密电子邮件等安全渠道，在必要时通过安全的内部平台将这些程式码分发给授权人员。

监察及培训

- 监察：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。

- 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。

- 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。

- 模拟攻击：使用网路钓鱼模拟攻击来帮助员工识别和回应欺诈性通讯。

如何分辨深伪伪造技术- 额外指引

随着人工智能急速的发展，网络诈骗层出不穷，亦意味着将来更难以分辨真假，因此更需要提高警觉。在辨识深度伪造时需要注意以下几点:

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. 背景可能与聊天场景不符。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