生成式人工智能(AI)與詐騙

人工智能詐騙

騙徒可能利用生成式人工智能來欺騙個人和企業

為保障自身及企業安全，了解騙徒如何運用此技術至為重要。

生成式人工智能已成為騙徒所使用詐騙手法的工具之一，使詐騙手法更逼真。由於此技術能模仿語言風格，甚至複製影像及聲音，騙徒更容易冒充您熟悉及信任的人士或企業。

常見手法包括：

- **語音冒充**–騙徒致電企業員工，冒充公司行政總裁，指示員工將一筆「機密」款項匯入一個暫記賬戶。由於員工誤以為正在與行政總裁通話，便批准了該筆付款。
- **深度偽造技術 (deepfake)** –騙徒可能會複製供應商公司某位成員的完整外貌與聲音，以冒充其身份。騙徒假扮成已知的供應商公司代表，安排與付款方公司通話，並要求更改銀行賬戶資料。由於負責付款的同事誤以為自己「親眼見到」熟悉的供應商代表，便批准更改銀行賬戶資料。

甚麼是生成式人工智能？

- 人工智能（AI）是一種允許電腦模仿人類思維和決策的技術。人工智能通過分析大量數據並不斷學習，從而使所作出的決策更貼近人類思維模式。
- 隨著人工智能接收及分析更多數據，人工智能的決策將不斷改進，並能夠做出 與人類相似的決策，這使得騙徒更容易冒充人或企業。
- 生成式人工智能則運用相同技術來創造內容，包括文字、圖像、影片及 / 或音訊。

請勿假設電話或視像通話必定真實可信。如對方要求提供敏感資料、指示向新受款人付款，或施加壓力要求即時行動，請格外警惕。企業應設有清晰明確的增加新受款人的付款程序。無論員工對受款人有多大信任，該程序亦不應被繞過。

如何保護自己免受這些威脅？

深度偽造提高了騙徒誘騙受害者的能力。雖然如此，很多現行的措施仍能有效降低這些風險。以下介紹了一些關鍵的防騙措施。

謹記常用的防詐騙措施

- 特別留心那些要求您迅速採取行動的短訊/電郵/電話/影片——這些通常是詐騙的跡象。
- 請注意，恒生絕不會通過電郵或短訊要求你提供任何個人或公司帳戶資料及財務資料。
- 確保盡量只接受來自已批准的公司通訊渠道傳送的付款指示。騙徒通常透過 WhatsApp 等公開通訊渠道聯絡受害者，因為他們無法使用經批准的公司渠道。
- 務必檢查和驗證從短訊/電子郵件/ 網上收到的資訊，尤其是在任何人都可以發佈帖文的論壇或網站。如果不確定信息真僞， 請與客戶經理確認。

每日安全代碼

每日安全代碼是每日產生的獨特且具時效性的代碼，僅分發予獲授權人員。這些代碼可用作驗證通訊及交易，為防騙加設一重難以被騙徒複製的安全保障。以下是有效實施方式：

- **每日獨立代碼**：每日產生一組獨特代碼，供員工使用。
- **安全分發**：透過加密電郵或公司內部安全平台分發代碼。切勿與組織外部人士分享代碼。
- **核實程序**：在敏感交易、高價值通訊或任何需要身份驗證的情況下，要求提供當日代碼。

監察及培訓

- **人工審核**：針對大額交易或異常交易的審核，制定合適的內部控制機制，包括設定交易限額，日終跟蹤異常交易，並設定多於一人作交易批核。在執行重要交易時，建議當面進行交易，避免損失。
- **網絡釣魚防範意識**：為員工提供持續的培訓，幫助員工辨識並懂得應對網路釣魚攻擊。網絡釣魚攻擊通常是接連其他更精密的攻擊。
- **深度僞造防範意識**: 教導員工瞭解深度僞造技術的風險 以及騙徒如何將其用於欺詐。培訓應涵蓋如何辨識深 偽詐騙、遵守保密協定的重要性，以及如何舉報可疑活動。

如何分辨深度偽造技術 - 額外指引

人工智能技術迅速發展，意味著深度偽造 (deepfake) 內容將愈來愈難與真實影像分辨。雖然以下建議有助識別較低階的偽造手法，但仍應考慮額外的控制措施以加強防範。

請記住：即使對方的外貌與聲音看似來自您公司內部人士，若其要求異常，仍應保持懷疑態度。對於大型或不尋常的交易，維持一定程度的人工審批始終是良好做法。

1. 眼鏡會產生反光，無法正常呈現光照的自然物理特性
2. 面部表情不自然或五官位置異常，或身體移動方式不自然
3. 頭髮或皮膚可能呈現模糊或異常移動
4. 口型無法對上。注意聆聽音調和音量的變化
5. 背景可能與通話場景不符。可能會顯示奇怪的反射或異常現象
6. 似乎沒有開燈或有奇怪的陰影。