恒生銀行
HANG SENG BANK

生成式人工智能(AI)和詐騙

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，為了保護您或您的企業免受詐騙威脅，本指引將助您進一步了解不同類型的詐騙手法，以及需要注意的事項。

如何運用生成式人工智能進行詐騙？

- 增強網絡釣魚電郵 - 雖然網絡釣魚電郵仍是常見的詐騙方法，騙徒透過人工智能，甚至可以模仿受信任者的語氣和態度製作出更巧妙的詐騙電郵。增加了釣魚電郵的辨認難度。

- 語音釣魚 - 語音釣魚利用生成式人工智能複製一個人的聲音，甚至能像聊天機器人一樣表達特定的語句。相較於其他詐騙手法，雖然語音詐騙情況並不常見，但這項技術仍然能夠協助騙徒成功詐騙。

- **深度偽造技術** – 深度偽造利用生成式人工智能來複製一個人的外貌和聲音。深度偽造影片能做到非常真實可信，通常會模仿被複製的人說出從未說過的話語。與語音釣魚類似，深度偽造詐騙案例並不常見，但仍然需要提高警覺。

什麼是人工智能?

- 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。

如何保障自己免受這些威脅？

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

- 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。
- 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。

流動保安編碼

流動保安編碼具有唯一性和有時效性，並只可給予授權人員的編碼。這些代碼可用於驗證通訊和交易，騙徒難以複製，從而加強了防禦。您可參照以下方式有效使用和保護流動保安編碼： ：

- 切勿向未經授權的人員透露您的任何身份驗證方法，包括發送到您註冊的行動或安全設備的密碼、一次性安全代碼和一次性密碼 (OTP)
- 保密傳送：透過加密電子郵件等安全管道，在必要時透過安全的內部平台將這些程式碼分發給授權人員。

監察及培訓

- 監察：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。
- 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。
- 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。
- 模擬攻擊：使用網路釣魚模擬攻擊來幫助員工識別和回應詐騙通訊。

如何分辨深度偽造技術 - 額外指引

隨著人工智能急速的發展，網絡詐騙層出不窮，亦意味著將來更難以分辨真假，因此更需要提高警覺。在辨識深度偽造時需要注意以下幾點:

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. 背景可能與聊天場景不符。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。