檢查清單：處理付款–第 1 / 2 部分

在最容易受詐騙威脅的業務範疇，應時刻保持警覺及採取合適的行動，請參考下列建議，有助相關的人員以更嚴謹的方法處理付款指示，並培養對詐騙有警覺性的企業文化。

- **想一想：該要求是否不尋常或與業務背景不符？是否合乎邏輯？**任何涉及匯款或賬戶資料的電郵，如語氣緊急或聲稱無法回電，均應視為可疑。如您並未預期收到該訊息，或不認識發件人，**切勿點擊任何連結或開啟附件**。
- **請核實電郵地址是否屬真實及可信**。即使電郵署名為您熟悉的人士（如您經常聯絡的人士），亦**應核對電郵地址是否正確**。騙徒會冒充可信人士。如屬公司同事，其電郵地址應可在公司通訊錄中查核（如有提供）。

  另外，請特別留意網域名稱的拼寫是否正確。騙徒常會建立與真實網域極為相似的偽冒地址，只改動一兩個字母，企圖混淆收件人，例如 J@rnbusiness.com 與 J@mbusiness.com 。顯示名稱可能隱藏真實的發件人電郵地址，切勿只憑表面判斷。
- **即使匯款指示來自高級管理層，也應保持警覺，提出質疑**。騙徒深知員工更傾向聽從高層指示，因此常會冒充高級主管或業務夥伴發出付款要求。切勿單憑電郵內容信任付款指示，即使發件人身份看似可信。騙徒亦可能透過常用的即時通訊平台進行詐騙。

請注意，騙徒有可能已入侵並取得您正在通訊的電郵賬戶的存取權限

© Hang Seng Bank

RESTRICTED

檢查清單：處理付款–第 2 / 2 部分

核實新增或更改的付款資料，有助減低付款詐騙的風險。除了回撥電話加以確認，還有多項重要措施可進一步減低風險。

- **核實新收款人或賬戶的資料變更**
  在可行的情況下，請使用可靠的聯絡方式向對方查證，並請嘗試與您相識的人確認。例如，如果變更請求來自公司內部人員，請直接致電該人員以作確認。如果來自供應商，請致電與您經常聯絡的人員以作確認。請勿回覆電郵或使用電郵中的聯絡方式。一般情況下，網絡不法分子在獲得登入賬戶權限後，會向賬戶聯絡清單上的人士發送釣魚郵件。這代表著即使電郵的內容相當可疑，您仍可能會因為電郵地址正確無誤，而認為真的是由該寄件人發出。此時，您應致電該寄件人，既可以確認電郵中的要求，亦可提醒他們的電郵賬戶或已遭入侵。
- 切勿直接回覆該電郵或使用電郵內所提供的聯絡方式。如騙徒已入侵他人賬戶，他們極有可能更改聯絡資料，令您最終與騙徒通話。
- 請主動致電付款指示方確認，切勿依賴對方來電。騙徒深知回撥核實是常見程序，可能會先行聯絡您，以避開此步驟

請注意，騙徒有可能已入侵並取得您正在通訊的電郵賬戶的存取權限

© Hang Seng Bank

RESTRICTED