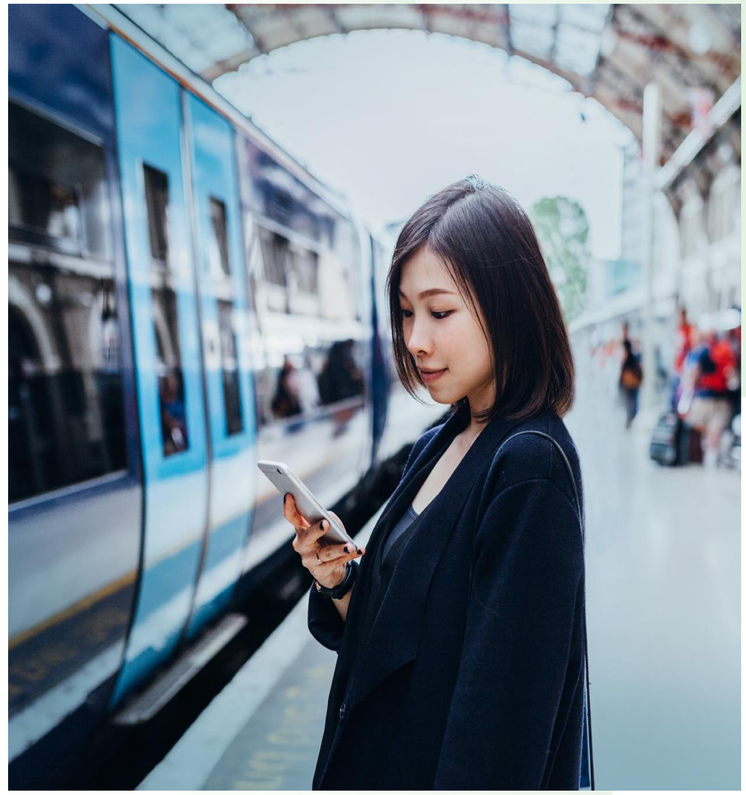
# 如何減少付款詐騙風險

# 減少付款詐騙風險

每間企業均可採取一系列簡單且成本不高的措施，以減少付款詐騙及騙局的風險。防範工作人人有責。

- 在您的業務中可能存在弱點的部分培養警覺意識
- 教育員工如何識別和避免詐騙，並確保他們了解公司的安全政策和程序。
- 對任何不尋常或與業務背景不符的付款要求，應主動提出查詢。
- 最重要的是，任何新增的受款人或銀行賬戶資料，務必透過已預先建立的可靠渠道（例如已知聯絡人及電話號碼）核實。
- 接下來的數頁投影片將提供更詳盡的指引，為負責付款的同事提供支援。



# 檢查電郵地址

## 騙徒會冒充可信人士。

- 即使電郵署名為您熟悉的人士（如您認識或經常聯絡的人士），亦應核對電郵地址是否正確。
- 如發送人屬公司同事，其電郵地址應可在公司通訊錄中查核（如有提供）。
- 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。

# 仔細檢查電郵

## 「緊急要求」是常見的警號。

- 如電郵涉及付款事宜，且語氣緊急或聲稱無法回電，應視為可疑訊息。
- 部分網絡釣魚電郵語句粗疏，即使拼字正確，語法亦可能錯誤。對外來電郵務必保持高度警覺，尤其是含有連結或附件者。請注意：生成式人工智能令騙徒更容易製作自然語氣、內容逼真的惡意電郵。
- 如您並未預期收到該訊息，或不認識發件人，切勿點擊連結或開啟附件。

# 新受款人或變更賬戶資料均需核實

## 請務必透過已知聯絡方式與指示方核實其要求。

- 在可行的情況下，應致電您熟悉的聯絡人進行確認。例如：如變更付款資料要求來自公司內部人員，請直接致電該同事確認；如變更要求來自供應商，請致電您經常聯絡的負責人，並同時核對銀行代碼及賬戶號碼。
- 切勿直接回覆該電郵或使用電郵內所提供的聯絡方式。
- 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相關人士發送釣魚郵件。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。

# 減低付款詐騙風險

## 任何類型的企業均可能面對詐騙風險，手法亦多不勝數。

### 制定及落實有關匯款的保安機制

確保所有付款均經妥善核實，是防止詐騙最關鍵的一步。建立既定的程序，防止匯款團隊在未經核實的情況下授權新增或更改的付款指示。按照所訂立的保安機制，就可確保匯款團隊不會僅根據，看起來真實的付款指示，未經驗證的電郵或電話指示轉移資金。此外，也應鼓勵員工直接聯絡收款人以確認新的或變更的付款要求。

### 提高員工警惕性

企業應為員工提供充足的培訓，教導員工防詐騙是公司任何一員的責任，並建立一套能讓員工向管理層安心反映疑慮的企業文化。

### 審慎管理您的數碼足跡

在社交媒體平台上過度分享個人資訊，可能令騙徒掌握您、您的朋友、家人及聯絡人的資料，並用作冒充身份。減少公開個人資訊，有助降低成為攻擊目標的風險。

### 鼓勵員工三思而後點擊

點擊可信任的網站上的連結雖然無妨，但點擊未經驗證電郵和即時訊息中的連結，則應可免則免。將鼠標懸停在連結上，您便可看到隱藏的網址並驗證其真實性。在點擊任何電郵內的連結或下載任何附件之前，請再三查證，尤其應注意是否出現拼寫和文法錯誤。

### 加強您的密碼可靠性

請考慮使用密碼管理器或密碼短語。密碼短語通常比傳統密碼更長，但更容易記住且難以破解。鼓勵員工隨機選擇三個單詞，並選擇字母、數字和符號組合，以加強密碼的可靠性。

### 在遇上詐騙/網路攻擊時應採取的措施

如果您或您的公司不幸成為詐騙/網路攻擊的受害者，請迅速採取應對措施。及時舉報已發現或疑似的事件有助於保障公司免受進一步的攻擊，減低損失。請盡快與您的銀行或相關的的財務機構聯絡，以確保及時得到所需的支援。

.