滙豐防詐騙指引

保護你的企業
免受詐騙和網
絡犯罪的威脅

滙豐
HSBC

保護你的企業免受詐騙威脅

對現今企業來說，詐騙是其中一種最常面臨的威脅。

稍一不慎，詐騙便可能招致重大的財務損失。不論企業規模大小，都會隨時面臨同等的威脅，因此，本指引旨在助你和員工能及早辨識詐騙危機，並作出有效的預防措施。如你不幸成為受害者時，亦可採取正確的應對措施。

高達430億美元

2016年6月至2021年12月全球商務電郵詐騙攻擊所造成的損失

資料來源：FBI互聯網犯罪投訴中心

本指引將助你進一步認識可能會威脅你業務的常見詐騙類型，並提供一些實用的防詐騙方法。如果你可在的機構中，對各成員進行相關的教育，將可讓企業獲得更全面保障。本指引提供了許多建議和檢查清單，可供管理階層和處理交易的支付團隊參考。

可能威脅你業務的詐騙類型

滙豐 HSBC

在付款時遭受詐騙的風險特別高

- **授權支付 (APP)** 詐騙是指騙徒冒充真正的收款人，欺騙企業將資金匯到騙徒手中。
- **網路釣魚**是APP 詐騙的常見方法，則是騙徒試圖欺騙用戶點擊一個連結，該連結將下載惡意軟體，或將用戶引導至虛假網站。
- 網路釣魚亦可能試圖偽裝成你信任的聯絡人，例如你的銀行，以獲取敏感資訊，如用戶名稱、密碼和賬戶詳細資訊。

滙豐 HSBC

商業電子郵件詐騙

騙徒常用偽冒電郵進行詐騙。

當付款期到時，騙徒會發送一封看起來像供應商發送的真正電郵，通知你收款銀行的詳細資訊已更改，並提供已更新的資訊及要求你付款。
此類詐騙往往難以被發現，因為：

- 騙徒通常使用供應商所常用的電郵地址，或看起來與該電郵地址非常相似的偽冒電郵地址。
- 騙徒所簽發的收據仿真度極高。
- 偽冒的供應商職員電郵簽名或溝通風格，均可能與真實的沒有明顯差異。
- 在某些情況下，騙徒可能已經獲得了登入郵箱的權限，因此該詐騙郵件將來自一個真實的電郵地址。騙徒將能夠存取郵件連結並以相似的語調和文字進行交流。
- 騙徒所要求的款項，往往是即將臨近付款期限。
- **跟真正供應商電郵的唯一的區別，通常是更改了收款銀行的詳細資料。**

電郵詐騙的成因

電郵賬戶被入侵

- 騙徒使用駭客技術或已竊取的賬戶資料，入侵企業的電郵賬戶。
- 電郵賬戶詳細資訊可能是因網路釣魚或資料外洩，而被騙徒獲取。
- 不法份子可能會蒐集有關使用者的聯絡人資料、郵件撰寫風格和個人資料，使他們的所杜撰的訊息看起來更可信。

偽冒電郵

- 不法份子開立一個與真實電郵地址非常相似的賬戶。
- 或者他們可能利用偽冒的電郵格式和標題，企圖令收件人不容易察覺，並將其當作為真實的郵件來回覆。

冒充高層主管詐騙

不法份子假冒公司的高層人員

- 他們將發送電郵給會計部門，要求緊急匯出一筆大額款項，原因可能是用於收購項目或其他重要交易。
- 他們通常會選擇高層人員不在公司時進行詐騙，讓對方難以查證核實。
- 再次強調，電郵賬戶可能是透過網路釣魚或資料外洩而被入侵，而入侵所需的相關資資料往往是透過公司網站或社交媒體收集得來。

其他常見的詐騙攻擊方式

語音釣魚和電話詐騙

電話詐騙，或稱語音釣魚，是指詐騙者假冒成你的銀行或其他可信任的機構來進行電話詐騙。他們甚至可能讓來電顯示成你認識且信任的號碼，此被稱為改號欺詐，其對話內容聽起來可能非常真實可信，詐騙者甚至可能已經掌握了一些有關你的個人資訊，如賬戶號碼或地址。如果你覺得有任何不妥，或察覺有異，請不要猶疑，立即掛斷電話。
你可以反過來致電你所知的機構電話號碼，例如你銀行卡背面的電話號碼，以核實來電的真偽。

但請留意，騙徒可能繼續保持通話線路連通，甚至偽造撥號的音效，讓你誤以為真。因此，請使用另一部手機，或相隔至少30秒後才致電。
常見的例子包括：

- 「你的銀行」通知你的賬戶出現風險，需要將你的資金轉移到另一個賬戶，以確保安全。
- 「你的銀行」需要你的協助來調查詐欺事件。
- 你的網絡或電訊供應商致電給你，替你解決你從沒有報告過的問題。

銀行可以根據你的要求轉賬，但絕不會因此索取你的密碼、PIN碼、任何一次性密碼或安全代碼。

入侵賬戶欺詐

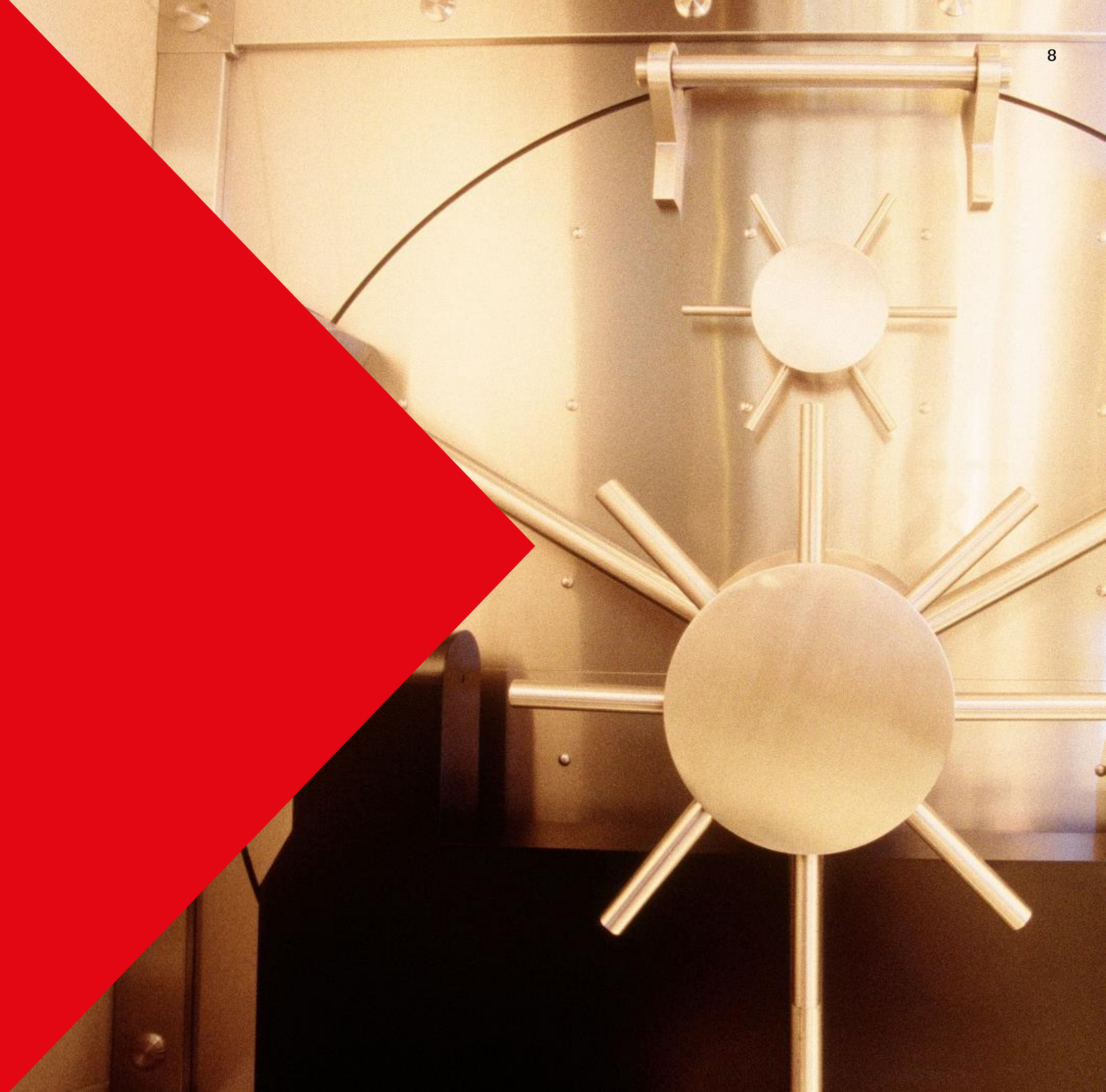
騙徒可能以偽冒的電話號碼致電給你，例如顯示為滙豐電話銀行或其所偽冒公司的電話號碼。騙徒往往對公司的運作相當熟悉，會引導你進行你所預期的流程，例如驗證程序，以搏取你的信任。

接著，他們將以各種方法來騙取你的安全資訊，例如使用者名稱、密碼、安全代碼。騙徒隨後可以使用這些資訊，成功入侵你的賬戶，並將你的資金轉走。

請謹記：

- 滙豐不會要求你提供卡片PIN碼、密碼或安全代碼。
- 不要向任何人透露安全代碼。
- 滙豐絕不會要求你將資金轉移到任何安全賬戶。

防止詐騙

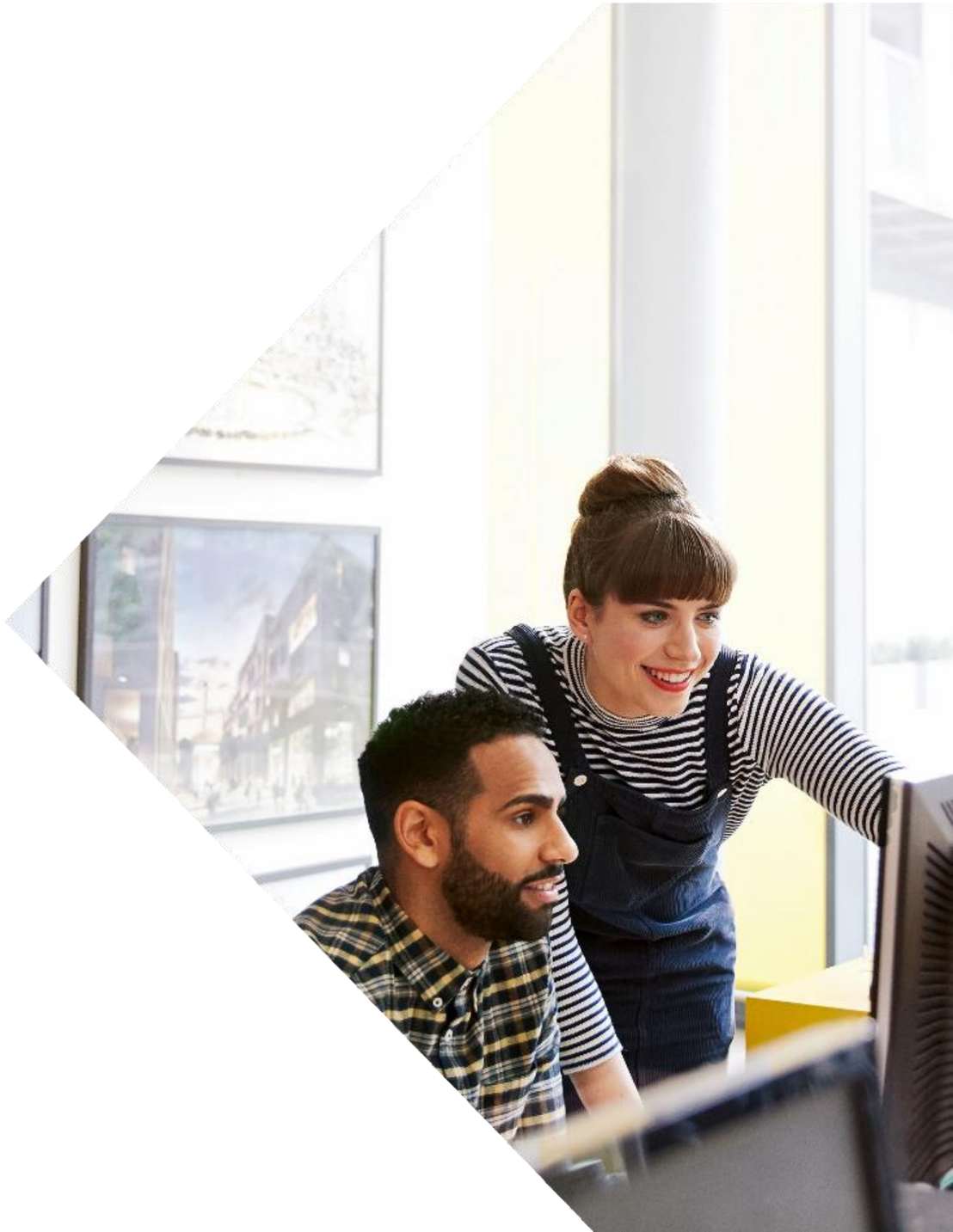


滙豐 HSBC

降低詐騙風險

每家企業都可以採取一些措施以降低詐騙風險。這些措施既不複雜，亦無需花耗大量成本。

- 評估你的業務，在最易受詐騙威脅的部份提高警覺。
- 教育員工如何辨識和避免詐騙，並確保他們了解公司的安全政策和措施。
- 最重要的是，**任何新的受款人或賬戶的詳細資料都需要經過核實。**
- 對任何異常或不合理的請求，必須作出進一步的查詢。
- 接下來的部分，將為負責付款的人員提供更詳細的指引。



確認電郵地址

騙徒會偽冒為可信賴的人士。

- 如果發件人的名字相當熟悉（你認識或經常通信來往的人），請**確認電郵地址是否相符。**
- 如果發送人為同事，其電郵地址應列在公司的電郵件目錄上（如有）。
- 確認網域名稱的拼寫是否正確。詐騙者經常會創建與真實域名非常相似的假域名，並更改一個或兩個字母，務求令收件人不容易察覺。例如：J@rnbusiness.com 及 J@mbusiness.com。
- 請注意，電郵顯示的名稱可能與實際發件人的電郵地址不符。

仔細審查電郵

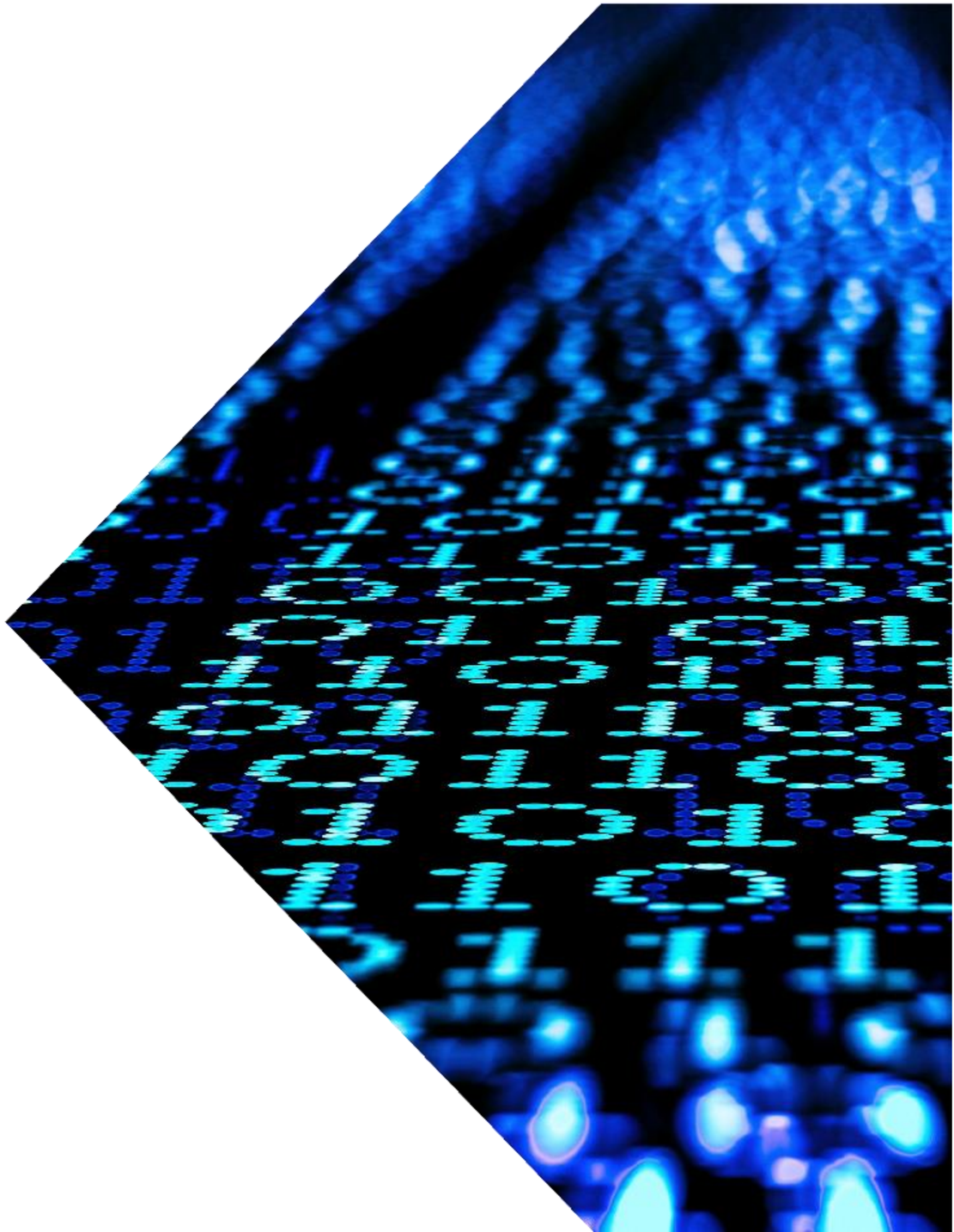
聲稱緊急情況更要警惕。

- 如果任何與付款事宜相關的電郵，使用了緊急的語氣，或以沒有回電選項為理由，則應視為可疑電郵。
- 一些釣魚郵件寫得相當糟糕，即使拼寫正確，也可能出現文法錯誤。對從外部發送過來的電郵應加倍警惕，特別是那些載有連結或附件的電郵。請注意，生成式人工智能使騙徒更容易杜撰出更真實可信的惡意電郵。
- 如果你收到不尋常的電郵，且/或不認識寄件人，**請勿點擊電郵內的連結或打開附件。**

核實新收款人或賬戶的資料變更

請使用可靠的聯絡方式向對方查證。

- 在可行的情況下，請嘗試與你相識的人聯絡。例如，如果公司內部人員要求資料變更，請直接致電該人員以作確認。如果變更要求來自供應商，請致電與你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，你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，你應致電該寄件人，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。



防止詐騙

任何類型的企業均有機會遭受不同形式的欺詐幸而，你可以採取一些措施來讓你的企業免受詐騙和網路犯罪的威脅。以下是一些可以幫助你降低企業內部詐騙風險的建議清單。

建議

制定及落實有關匯款的保安機制

防範欺詐的關鍵在於確保所有款項都經過充份的驗證才付出。因此，企業應定立機制防止匯款團隊在未經充份驗證的情況下，授權新的或被要求變更的付款。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。

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，你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。

加強你的密碼可靠性

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

如果你或你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。請盡快與你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。

檢查清單：高層管理人員

最有效抵禦詐騙的方法，就是防範於未然。以下檢查清單可為你提供一些實用建議，助你保護企業的網絡安全。

- [ ] 對於全新或經過修訂的付款指示，貴公司有否訂立驗證機制？員工是否知道如何取得已知聯絡人的資料？

- [ ] 貴公司有否訂立付款指示的保安機制？包括如何提出付款指示、由誰審核、以哪種方式支付，以及在遇上疑惑時該如何驗證付款指示？

- [ ] 密碼的安全強度是否足夠（例如：最小字符長度及使用字母、數字和符號的組合）。貴公司是否正在考慮使用密碼管理器或規定使用密碼短語？

- [ ] 貴公司有考慮應用雙重驗證機制及其可行性？

- [ ] 假如發生欺詐付款時，你的員工知道如何應對和處理嗎？

- [ ] 對於欺詐攻擊，例如電郵地址遭到入侵，貴公司有否制訂應對措施？

- [ ] 你有定期與提交付款指示的相關人員討論詐騙的潛在風險？

檢查清單之二：處理付款要求

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。

確認電郵地址的真偽

如果電郵發件人的名字相當熟悉（你認識或經常通信來往的人），請**確認電郵地址是否相符。**

如果發送人為同事，其電郵地址應列在公司電子郵件目錄上（如有）。此外，請確認網域名稱的拼寫是否正確，亦應留意詐騙者經常會創建與真實域名非常相似的假域名，但會修改一個或兩個字母，務求令收件人不容易察覺。例如：J@rnbusiness.com 及 J@mbusiness.com。最後，請仔細檢查電郵顯示的名稱，可能與實際發件人的電郵地址不符。

仔細審查電郵

如果任何與付款事宜相關的電郵，使用了緊急的語氣，或以沒有回電選項為理由，則應視為可疑電郵。一些釣魚郵件寫得相當糟糕，即使拼寫正確，也可能含有文法錯誤。對從外部發送過來的電郵應加位倍警惕，特別是那些包含連結或附件的電郵。請注意，生成式人工智能使得騙徒更容易杜撰更真實可信的惡意電郵。如果你收到不尋常的電郵，且/或不認識寄件人，**請勿點擊電郵內的連結或打開附件。**

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，並請嘗試與你相識的人確認。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，請致電與你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，你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，你應致電該寄件人，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。

我們應評估所收到的請求是否合理？有沒有異常的地方？

假如遭受詐騙應如何應對

滙豐 HSBC

如果你不幸成為詐騙受害人

立即採取適當措施，可把詐騙所造成的損失減至最低，同時亦提高追回資金的可能性。

- **停止與騙徒的一切聯絡。**
- **盡快通知所有相關人士和組織**（員工、客戶和財務機構），並須立即聯絡銀行，發出退款指示。因為資金轉移速度非常快，一旦被轉移，退款程序便會更困難。
- 向有關當局**舉報詐騙個案**。
- **查看你的財務記錄**，以辨別任何未經授權的交易或可疑活動。
- **保留所有與詐騙相關的證據**，包括電郵、收據和任何其他通訊，以便日後取證之用。
- **檢討並改善公司的保安政策和措施。**

向滙豐舉報詐騙

如你懷疑有未經授權的詐騙性轉賬或賬單付款，或懷疑企業的網絡安全受到威脅，請立即致電滙豐24小時工商金融服務熱線 +852 2748 8288或致電你的客戶經理。

我們同時建議你透過香港警務處「電子報案中心」https://www.police.gov.hk/ppp_tc/contact_us.html 舉報個案。

如果你是滙豐財資網客戶，請立即將相關詐騙性交易資料發送給你的客戶經理，包括：

- 滙豐財資網客戶編號
- 公司名稱
- 滙豐財資網使用名稱
- 指示參考號碼

你可致電你的客戶經理或者通過以下電話聯繫反欺詐組去確認事件的跟進。

- 國際長途 + 1 778 452 2774
- 免費電話（僅限於美國和加拿大）1 866 979 4722
- 免費電話 （僅限於英國） 0800 169 9903

如果你遭受網絡攻擊，請採取以下措施：

- **關閉所有受影響設備的網絡連線**，以防止惡意軟件散佈或未經授權的入侵。
- **更改所有受影響賬戶的密碼**，包括電郵、網絡和其他可能洩露了資料的賬戶。
- 聘用信譽良好的網絡保安公司，對你的系統進行**全面檢查**，以發掘其他漏洞或入侵活動。
- **盡快通知所有相關人士和組織**，例如員工、客戶和監管機構，並為他們提供所有相關資料。
- **確定攻擊來源**，並採取措施，防止未來再次遭受類似的攻擊。

術語概覽

詐騙和網路安全術語須知

- **防毒軟體** - 用於預防、偵測，甚至移除惡意軟體的電腦程式。
- **自帶設備政策（BYOD）** - 由企業實施的政策，允許員工將自己的個人電子設備作公務用途。
- **常見漏洞與揭露（CVE）** - 羅列已發現資安弱點及漏洞的清單，並提供獨有的ID編號、描述和參考資料以便供公眾查閱。
- **加密貨幣** - 可像商品一樣交易的端對端去中心化電子貨幣。
- **網絡攻擊** - 對電腦系統、網絡、基礎設施或設備的惡意攻擊。
- **網絡事件** - 國家網絡安全中心（NCSC）定義為「違反系統安全政策以影響其完整性或可用性和/或未經授權訪問或試圖訪問系統的行為；符合《濫用電腦法》（1990年）」。
- **暗網** - 網路的其中一部分，但無法在搜尋器搜索出來，僅能透過特殊權限或軟體訪問。
- **數碼足跡** - 使用網路後留下的數據蹤跡，可能包括被動信息，如存儲的Cookie，或者被主動在網絡上發表的資訊，如社交媒體帖子。
- **加密** - 使用數學算法將數據打亂的過程。這些數據可以是靜態加密，例如儲存在硬碟中的數據，亦可以是傳輸中的數據，例如透過 HTTPS 從你的網頁瀏覽器傳送到銀行伺服器的資料。加密了的資料並不能代表網絡上的不法份子無法截取，只是已被轉換為無用的和無法理解的亂碼，讓不法份子得物無所用。
- **防火牆** - 根據特定規則，監控網路進出流量的網路安全系統。
- **駭客** — 專門從事電腦網路攻擊的人士。黑帽駭客進行惡意攻擊，而白帽駭客則進行有助於網路防禦的行動。
- **惡意軟體** — 以達成不法或惡意目標的程式，涵蓋多個方面，例如提供遠端存取、載入或植入其他惡意程式、竊取銀行資訊、加密並拒絕存取資料，或盜用設備的運算能力。
- **安裝補丁** — 安裝修補程式以更新現有軟體或硬體，修復已發現錯誤和漏洞的過程。
- **滲透測試（pen testing）** - 機構利用駭客的攻擊手段來檢測自身網絡的安全性，通常由「紅隊」或專業的白帽駭客團隊負責。

- **釣魚 -** 通常透過電子郵件欺騙收件人洩露敏感資料、點擊惡意連結和/或打開惡意附件。不法份子常用釣魚以取得設備或網絡上初始入侵管道。
- **勒索軟體 -** 封鎖或限制使用者存取資料的惡意軟體，並要求受害者支付贖金才能解除限制。
- **短訊釣魚** — 透過短訊/簡訊傳送的釣魚訊息。
- **社交工程** — 操控他人的心理而作出某種行為，通常用於騙取個人資料。
- **魚叉式網路釣魚** — 針對特定人士或群體所發出的釣魚訊息。
- **特洛伊木馬** — 偽裝成看似無害的檔案或程式，讓受害者以為可安心開啟。特洛伊木馬十分常見，通常透過釣魚郵件傳送，或者由其他稱為「載體」的惡意軟體傳送。
- **雙重要素驗證（2FA）** — 一種要求用戶提供兩種身分識別要素的驗證過程，例如已知密碼和一次性密碼（OTP）。一般來說，這些要素可分為：「認知要素」（密碼）、「生物特徵」（指紋）或「持有物件」（密匙卡）。
- **虛擬私人網路（VPN）** — 允許在公共基礎設施上建立安全私人的連線，最初由機構開發，以對訪問內部網絡資源，例如電郵伺服器或共享文件夾等的員工進行身份驗證。現在，越來越多的人使用消費者VPN來作為建立及選取VPN伺服器的加密連線，並使用該伺服器連接到其他互聯網資源。
- **語音釣魚** — 透過電話進行並大量利用社交工程的釣魚攻擊。
- **零日漏洞** — 在補丁或更新發佈之前所發現到的漏洞。利用此類漏洞的惡意軟體通常被稱為零日漏洞攻擊。

免責聲明

資料包中的某些資訊是由香港上海滙豐銀行有限公司（「本行」）根據可靠但未經獨立核實的資訊來源而準備。 編製資料包所載的內容及資訊時，本行已嚴謹處理，但不對其準確性或完整性做出任何擔保、陳述或保證，也不承擔任何責任或義務。 除特別説明外，所表達的意見僅代表本行的意見，如有更改，恕不另行通知。

本資料包是為你的查閱和資訊而準備的。 未經香港上海滙豐銀行有限公司事先書面許可，不得以任何形式或任何方式（電子、機械、影印記錄或其他方式）複製或傳播本資料包的任何部分。

免責聲明中英文本如有任何歧義或不一致，概以英文本為準。