反詐騙聯盟（教育）啟動禮

日期：2024 年 10 月 12 日

地點：香港科技大學花旗集團演講廳（LT-A）

私隱專員鍾麗玲主題演講
提升數據安全 防範詐騙之本

前言

1. 梁副主席（全國政協副主席及香港特別行政區前行政長官梁振英先生）、沈教授（香港科技大學校董會主席沈向洋教授）、蕭處長（香港警務處處長蕭澤頤先生）、劉主席（香港專業聯盟主席劉炳章先生）、高博士（大灣區香港中心及「一帶一路」國際合作香港中心董事高靜芝博士）、各位嘉賓，大家好。

2. 今日我十分榮幸出席反詐騙聯盟（教育）啟動禮，讓我可以親身見證反詐騙聯盟（教育）一連串推廣及教育工作正式展開，相信在警務處及教育界的同心協力下，定必可以提高學校、家長及學生對詐騙手法的認識和防範意識，更好地保護自己和身邊的人。

騙案的演變及趨勢

3. 隨着資訊科技不斷進步及發展，加上 2019 冠狀病毒病疫情進一步加快數碼科技應用的步伐，更多個人和機構的活動都轉移到網

絡上進行，例如透過網絡遙距工作、進行網上視像會議、透過社交媒體聯系、進行網購及使用各式各樣的網上服務。

4. 網絡活動越趨普遍，亦改變了騙案的模式和規模。現時更多騙徒透過電話短訊、通訊應用程式、電子郵件、社交媒體平台及網站尋找獵物，以往的街頭祈福黨、保藥黨，已演變至今時今日的網絡釣魚、網上情緣、網上投資騙案等等。國際刑警組織於前年發表《全球罪案趨勢報告》[1]， 便將網絡釣魚及網上騙案，與洗黑錢和勒索軟件列為三大罪行威脅，並預測有關趨勢將會持續。

5. 近年人工智能的發展一日千里，亦出現越來越多利用 AI 技術行騙的個案。在 2024 年初，有騙徒自稱是一間跨國公司的英國總部首席財務官，要求香港分部的員工出席網上視像會議，聲稱要進行秘密交易。視像會議上，騙徒假冒英國首席財務官及其他看似是英國財務部門的職員，於過程中指示該名香港員工進行轉帳交易，前後轉帳 15 次至本地 5 個銀行帳戶、涉及合共 2 億港元。涉事的香港公司在約一星期後與總公司確認後，才發現被騙。在 2024 年 5 月，亦再有跨國公司受騙，同樣收到由騙徒假冒的首席財務官的短訊，其後與對方進行視像會議，最終損失約 400 萬港元[2]。所以在 AI 時代，有片都未必有真相。

[1] Financial and Cybercrimes Top Global Police Concerns, Says New INTERPOL Report
[2] 再有跨國公司墮 Deepfake 騙案　港員工與「CFO」視像會議失$400 萬

防範詐騙與保障個人資料私隱密不可分

6. 騙徒看來如此高明，我們豈不是束手就擒？答案當然「不是」。其實，騙徒手法雖然層出不窮，但萬變不離其宗，目的都是想盜取我們的個人資料圖利或行騙。在 2024 年首九個月，私隱專員公署分別收到 864 宗及 38 宗有關套取市民個人資料作詐騙用途的查詢及投訴，當中查詢數字較去年同期上升 67%，而投訴數字則與去年同期相同。

7. 在五花百門的行騙手法之下，我們要時刻提高警覺，在提供個人資料前應「停一停、諗一諗」，既不隨便向他人披露個人資料，亦不隨意點擊或掃瞄可疑的超連結及二維碼。此外，我們要不時留意帳戶及簽帳紀錄，並好好保護帳戶密碼及啟用帳戶登入雙重認證功能。

8. 科技進步，現時「有圖、有片亦未必有真相」，騙徒會透過人工智能深度偽造技術製作詐騙影片，所以我們要盡量減少在社交媒體平台及即時通訊軟件分享生物辨識資料，包括個人的正面照片及影片，並檢視相關的預設保安及私隱設定。

9. 為了提升市民的防騙意識，私隱專員公署早前便推出了一系列向公眾宣傳防騙訊息的活動，包括以「個人資料咪亂俾　踢走騙徒靠晒你」為主題製作宣傳海報於社區派發及展示；並以有關主題製作了一系列防騙宣傳短片，分階段在公署的官方 YouTube 頻道、

電視台及車廂電視播放。此外，公署亦不時舉辦及參與防騙專題講座，並設立「防騙貼士」專頁，向公眾提供防騙資訊。我們亦設立「個人資料防騙熱線」，處理懷疑誘騙個人資料的查詢或投訴。

提升數據安全

10. 在處理市民求助時，經常聽到他們問「騙徒最初如何獲得我的資料呢？」有些情況當然是受害人誤中圈套，例如在虛假網站輸入資料，但有些則可能源自一些機構的資料外洩事故。

11. 相信大家都會留意到無論是在香港還是其他地區，不同類型的網絡攻擊和個人資料外洩事故都時有發生，更有上升趨勢。而教育機構持有大量教職員、學生及家長的個人資料，當然成為黑客的目標之一。根據一份有關教育機構遭勒索軟件攻擊的全球調查報告[3]，於 2023 年分別有 63%的受訪初中教育機構，以及 66%的受訪高等教育機構，表示曾遭受網絡攻擊，較其他行業的平均值 59%為高。而在今年 1 月至 9 月期間，公署亦接獲共 26 宗有關教育機構的資料外洩事故通報，當中 10 宗涉及黑客攻擊。

12. 例如公署早前接獲一宗教育機構通報，有黑客利用暴力攻擊入侵其資訊管理系統，獲取了管理員密碼，並建立了具有管理權限的

[3] The State of Ransomware in Education 2024

新帳戶，可以查閱資料庫中的個人資料。事件影響超過 24,000 名家長及學生用戶的個人資料。公署調查後發現事故源於相關機構的密碼管理欠佳，未有採取適當措施保護管理員帳戶。事故發生後涉事機構在登入資訊管理系統時採用雙重認證功能、並設定高強度密碼及定期清理不必要的帳戶，以加強系統的保安及管理。

13. 除了網絡安全漏洞之外，員工對個人資料的處理不善及意識不足亦會讓不法之徒有機可乘。公署曾接獲一宗學校的求助，有家長收到由學校的即時通訊軟件發出要求轉賬的訊息，因而揭發該帳戶已遭騙徒騎劫。事件涉及約 370 名人士的個人資料，包括學生姓名及家長的電話號碼，以及教職員的姓名和電話號碼。經公署介入後，學校為所有即時通訊軟件帳戶啟動雙重認證功能，並制訂相關使用指引，包括要求教職員定期檢視及適時刪除即時通訊軟件內的通訊資料。

14. 根據《私隱條例》保障資料第 4 原則，持有個人資料的機構必須採取所有切實可行的步驟，確保所持有的個人資料受到保障。假如發生資料外洩，涉事機構有機會違反《私隱條例》的規定。

15. 正因如此，公署建議所有機構應未雨綢繆，提升網絡保安和數據安全，並採取合適的機構性及技術性措施以保障載有個人資料的資訊系統，當中包括：定期進行資訊保安系統風險評估；使用防火牆等軟件保護電腦網絡，並定期更新軟件；定期對資訊系統進

行保安漏洞評估及滲透測試；實施修補程式的管理；加密傳輸中和存儲中的資料；以及分隔開內部資料伺服器與網絡伺服器等等。

16. 為員工提供適當培訓、提高員工的資料保安意識也必不可少。機構應考慮將演習納入資訊保安培訓，例如在提供有關釣魚詐騙的培訓後，安排模擬釣魚郵件攻擊，以實戰幫助教職員提高警覺、建立一道「人力防火牆」。若可在風險可控的環境從錯誤中學習，對員工、對機構皆有裨益。

17. 隨着公眾對個人資料私隱保障的期望與日俱增，機構亦應建立一妥善的個人資料私隱管理系統，以幫助機構循規地收集、持有、處理和使用個人資料，確保數據安全。

18. 國家安全二十個重點領域之中，明確列出數據安全和網絡安全為兩個關鍵領域，可見兩者在數碼年代的重要性。為協助機構做好網絡及數據安全的工作，公署分別發布了《資訊及通訊科技的保安措施指引》及《資料外洩事故的處理及通報指引》，為機構提供適切的建議措施。公署亦於 2023 年 11 月推出了數據安全三大法寶，當中包括免費的「數據安全快測」評估專頁，以協助機構就其數據安全措施是否充足進行自我評估，公署會因應評估結果提供建議及相關參考資料。數據安全三大法寶亦包括為機構提供最新數據安全資訊的「數據安全」專題網頁，及「數據安全」熱線。

結語

19. 打擊騙徒是一場持久戰，正如公署的宣傳口號「個人資料咪亂俾踢走騙徒靠晒你」，只要所有人都提高保障個人資料意識，所有機構都做好保護數據安全的工作，不法之徒便無法得逞。私隱專員公署將會繼續做好我們執法、促進、推廣及教育的工作，同時加强與業界和不同持份者的聯繫及交流，與大家攜手保障個人資料私隱，踢走騙徒！

20. 最後，我祝願反詐騙聯盟（教育）工作順利，成果豐碩，祝大家身體健康，謝謝大家！