2024年國家網絡安全宣傳週澳門本地分論壇
個人資料保護專場活動

鍾麗玲女士
香港個人資料私隱專員

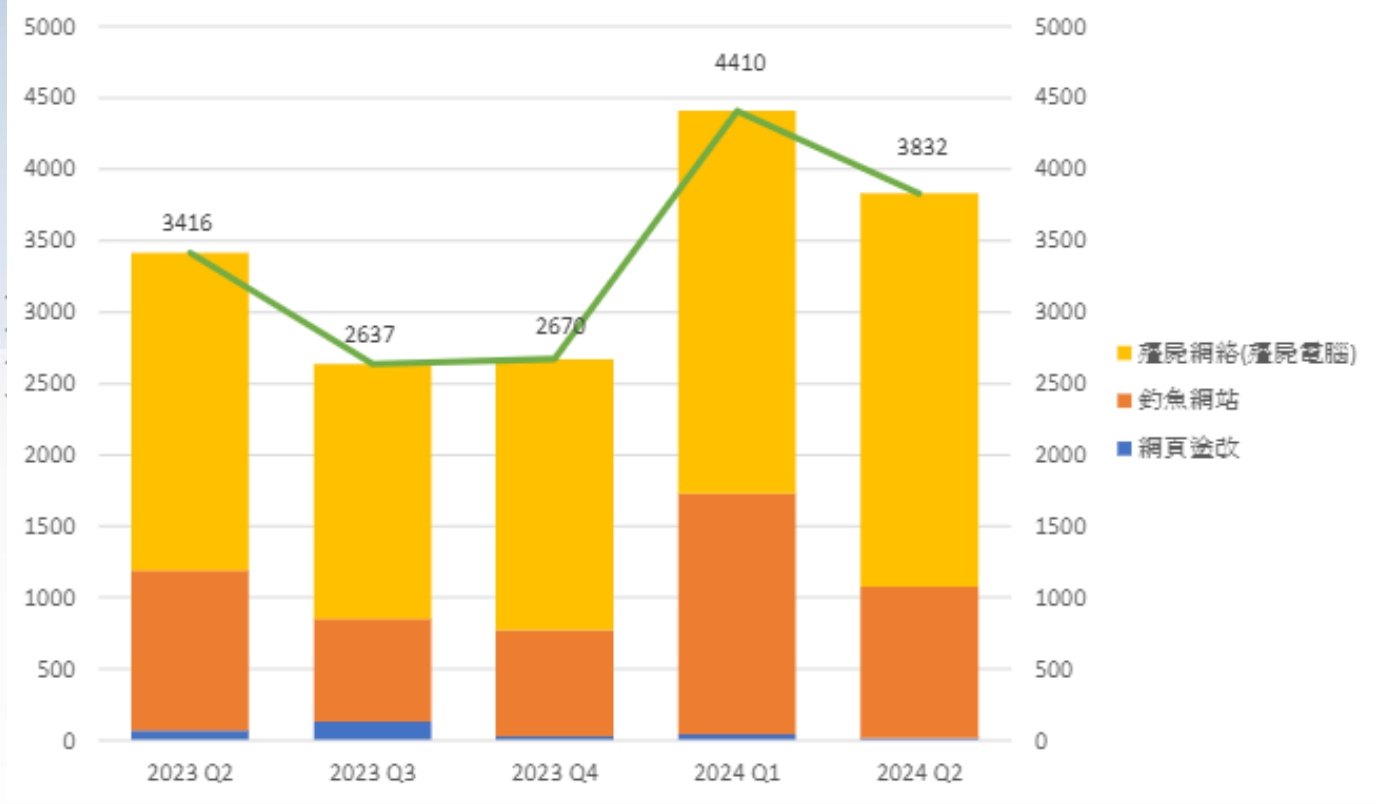
2024年9月12日

網絡安全風險與日俱增

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

全球趨勢

- 電訊公司Verizon的2023資料外洩調查報告顯示於**2013至2022年間**，資料外洩事故**大幅增加逾三倍**
- 市場調查公司Forrester 2023年的研究顯示**77%**的受訪機構表示於過去一年**曾遭受至少一次網絡攻擊**



本港趨勢

根據《香港保安觀察報告》，在2024上半年涉及香港的網絡保安事件宗數比2023下半年**上升55.3%**。

殭屍網絡（佔整體案例66%）是本地網絡保安事故的主要原因；其次為**釣魚網站**（佔整體案例33%）。

海外資料外洩事故的例子

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Medibank says hacker accessed data of 9.7 million customers, refuses to pay ransom

Reuters

November 8, 2022 5:05 AM GMT+8 · Updated a year ago

Casino giant MGM expects $100 million hit from hack that led to data breach

Reuters

2 minute read · Published 9:40 PM EDT, Thu October 5, 2023

An exterior view of MGM Grand hotel and casino, after MGM Resorts shut down some computer systems due to a cyber attack in Las Vegas, Nevada, U.S., September 13, 2023. Bridget Bennett/Reuters

Cybersecurity

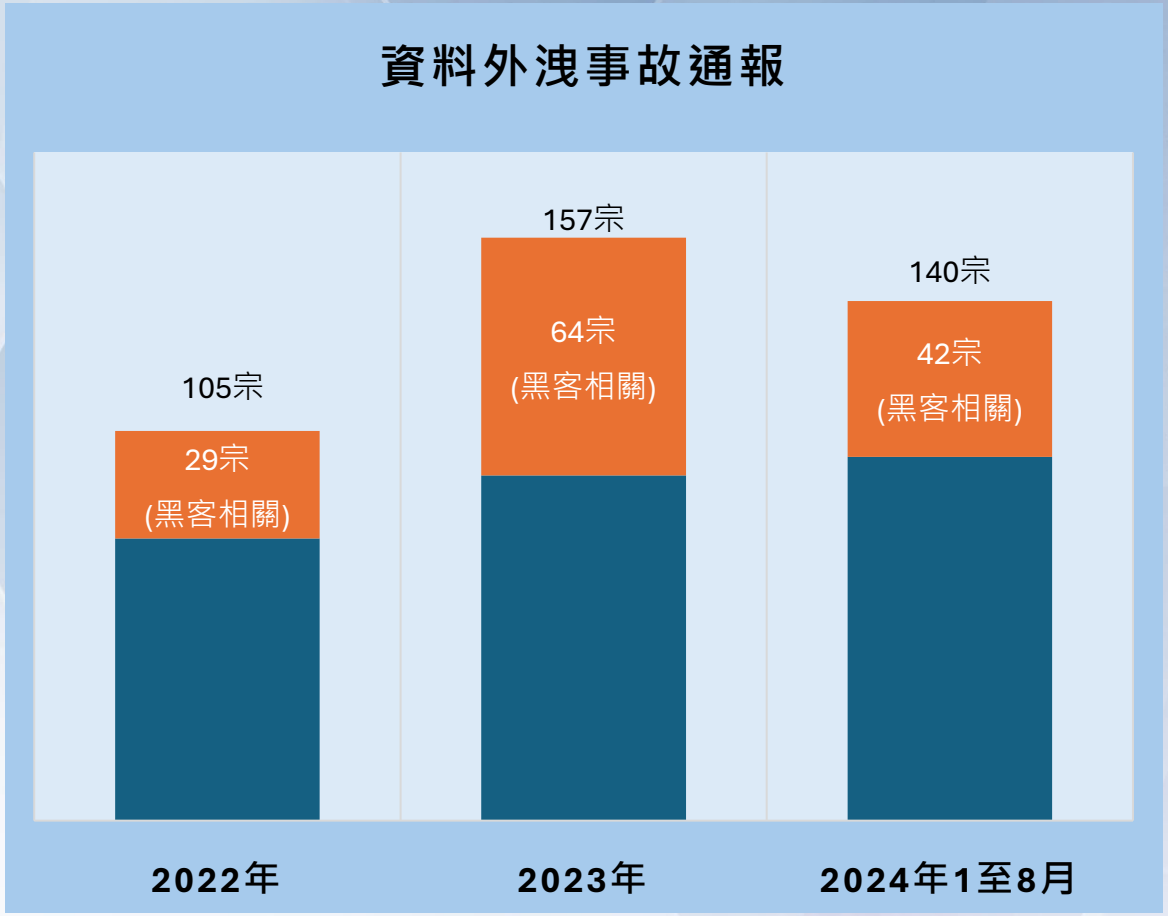
UnitedHealth hackers used stolen login credentials to break in, CEO says

By **Zeba Siddiqui**

May 1, 2024 5:09 AM GMT+8 · Updated 21 days ago

The corporate logo of the UnitedHealth Group appears on the side of one of their office buildings in Santa Ana, California, U.S., April 13, 2020. REUTERS/Mike Blake/File Photo *Purchase Licensing Rights*

公署接獲的資料外洩事故通報



- 公署於2023年共接獲**157宗**資料外洩事故通報，比2022年的105宗**上升近五成**。
- 而公署於**2024年首8個月**已接獲**140宗**通報，達2023年全年總宗數約**九成**。
- 於2023年涉及**黑客入侵**的資料外洩事故**共64宗**（佔全年事故的41%），比2022年的29宗（佔全年事故的28%），**大幅增加逾一倍**。
- 於2024年首8個月，涉及**黑客入侵**的資料外洩事故共**42宗**，達2023年全年有關宗數**約65%**。

香港《私隱條例》的相關規定

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

資料外洩事故可構成違反《私隱條例》 附表1的保障資料第4原則

保障資料第4(1)原則

資料使用者須**採取所有切實可行的步驟**，確保由資料使用者持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響

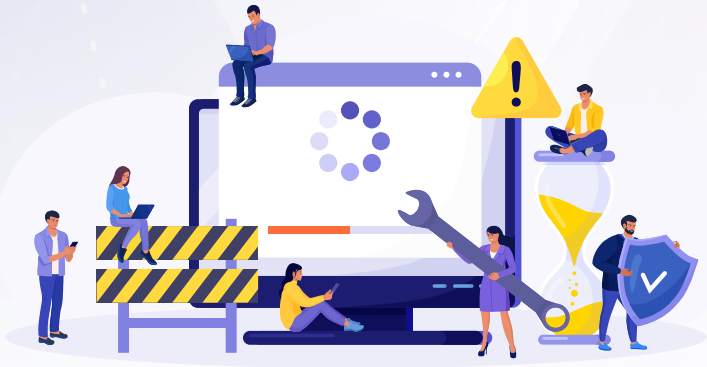
保障資料第4(2)原則

如資料使用者聘用（不論是在香港或香港以外聘用）**資料處理者**，以代該資料使用者處理個人資料，該資料使用者須採取**合約規範方法**或其他方法，以防止轉移予該資料處理者作處理的個人資料被未獲准許或意外地被查閱、處理、刪除、喪失或使用

資料外洩的常見原因

主要技術風險

- 網絡釣魚
- 未修補保安漏洞
- 低強度密碼
- 過時的操作系統和應用程式
- 植入惡意軟件



資料外洩個案分享（1）– 電郵系統遭入侵

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

- 2021年，公司A向私隱專員公署作出資料外洩通報，表示**其六個員工的電郵帳戶曾遭黑客入侵，導致客戶發送至該些電郵帳戶的電郵被轉發至兩個不明的電郵地址。**

涉及**超過1,600名**客戶的個人資料，當中包括姓名、職稱、電郵地址、公司名稱、電話號碼及信用卡資料。

資料外洩個案分享（1）– 電郵系統遭入侵

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

調查結果發現四項缺失：

1. 薄弱的密碼管理

2. 保留已過時的電郵帳戶

3. 電郵系統欠缺針對遠端存取的保安措施

4. 欠缺針對資訊系統的保安措施

資料外洩個案分享（1）– 電郵系統遭入侵

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

執行通知

- **修訂資訊保安政策**，加入並詳細說明強密碼管理政策、定期刪除已過期或不再使用的電郵帳戶機制，及訂立系統以定時監察及審核（包括內部審核）電郵帳戶的使用情況
- 制訂有效措施以**確保員工依循**已修訂的資訊保安政策
- **聘請獨立的資料保安專家**對公司的系統保安，包括電郵系統進行定期檢視及審核
- 為員工**制定最新的資訊保安培訓**，並妥善記錄培訓進度，以及對培訓的參與及有效程度作出評估

資料外洩個案分享（2）– 勒索軟件攻擊

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

- 2023年，資訊科技公司B向私隱專員公署作出資料外洩通報，表示**其電腦系統及檔案伺服器遭受到勒索軟件攻擊及惡意加密。自稱Trigona的黑客組織要求公司支付贖金，為已被加密的檔案解鎖。**

涉及**超過13,000名**受影響人士，當中約四成受影響人士為求職者及已離職僱員。受影響的個人資料包括姓名、身份證號碼及／或副本、護照號碼及／或聯絡資料，以及部分人士的財務資料、健康資料、照片、出生日期、僱傭資料、社交媒體帳戶資料及／或學歷資料及屬數名人士的信用卡資料等。

資料外洩個案分享（2）– 勒索軟件攻擊

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

調查結果發現五項缺失：

1. 資訊系統欠缺有效的偵測措施
2. 沒有為遠端存取資料啟用多重認證功能
3. 對資訊系統進行的保安審計不足
4. 資訊保安政策有欠具體
5. 個人資料被不必要地保留

資料外洩個案分享（2）– 勒索軟件攻擊

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

執行通知

- **徹底檢視載有個人資料的資訊系統**的安全及其保安措施，確保該些系統沒有已知的惡意軟件及保安漏洞，以及具備有效的偵測措施
- 為所有會存取載有個人資料的資訊系統的遙距使用者**實施多重身分認證**，並**定期檢視遙距存取的權限**
- 聘請**獨立的資訊保安專家**對資訊系統進行**最少每年一次的風險評估及保安審計**
- 制訂清晰及全面的資料系統保安政策及程序，涵蓋**防範、偵測及應對網絡攻擊的各種管控措施**，及**進行風險評估及保安審計的要求**
- 從資訊系統**銷毀所有逾期保留的個人資料**
- 制訂清晰的資料保留政策，**訂明每個系統內個人資料的保留期限**，及**制訂刪除已屆保留期限的個人資料的執行細節**
- 制訂並實施有效措施以**確保員工遵循上述資訊系統保安政策及程序**

資訊及通訊科技的資料保安建議措施

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

資料保安建議措施 *七大建議措施一覽*

1. 資料管治和機構性措施
2. 風險評估
3. 技術上及操作上的保安措施
4. 資料處理者的管理
5. 資料保安事故發生後的補救措施
6. 監察、評估及改善
7. 其他考慮

下載指引

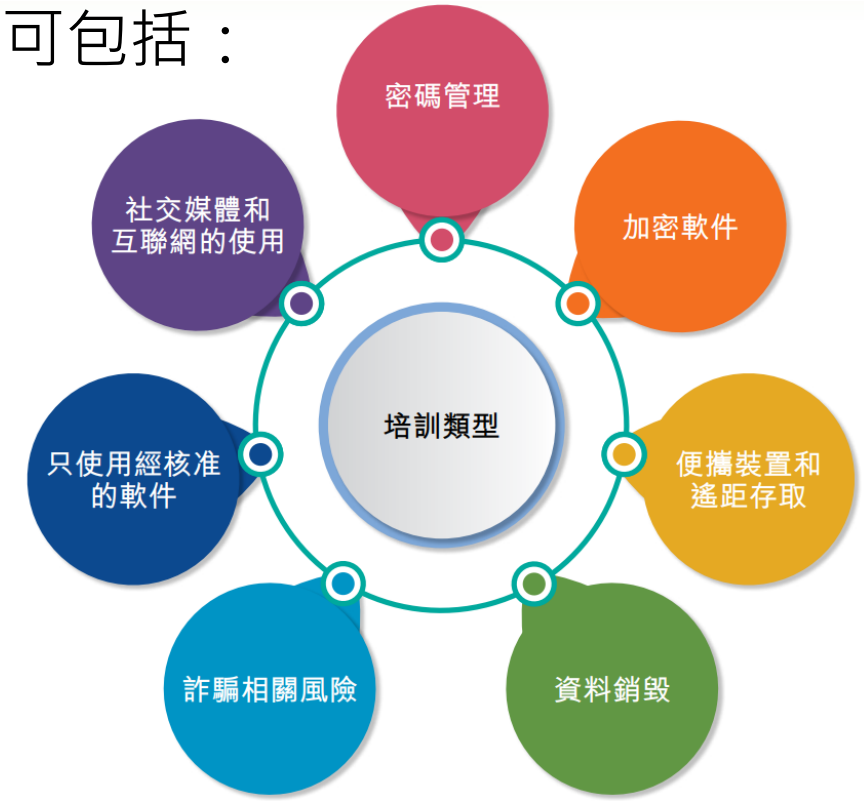
下載小冊子

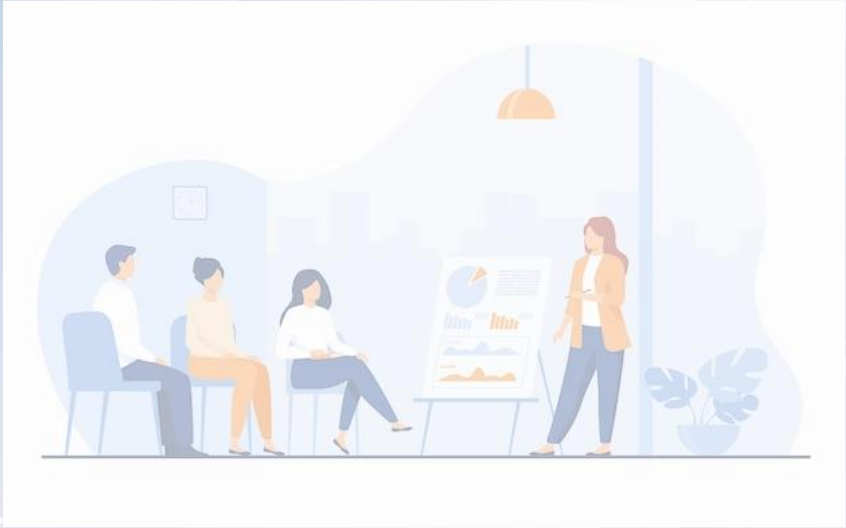
資訊及通訊科技的資料保安建議措施

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

資料管治和機構性措施 — *培訓*

工作人員應在入職時及往後**定期接受足夠培訓**，培訓類型可包括：





NOTE

企業可考慮將「演習」納入資料保安培訓（例如**模擬網絡釣魚攻擊**），以提高員工的警覺程度

資訊及通訊科技的資料保安建議措施

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

技術上及操作上的保安措施

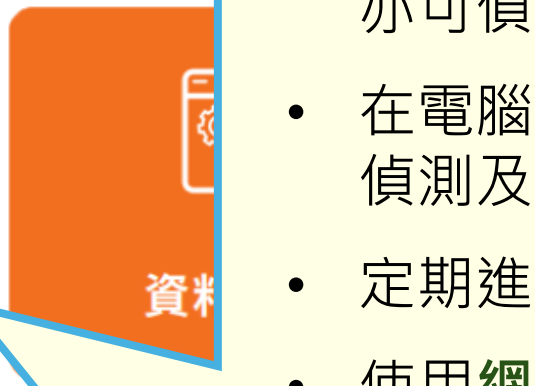
資料使用者應採取**足夠及有效的保安措施**，以保護其控制或所持有的個人資料和資訊及通訊系統：

- 保護電腦網絡
- 資料庫管理
- 存取管控
- 防火牆和反惡意軟件
- 保護網絡應用程式
- 加密
- 電郵及檔案傳送
- 資料備份、銷毀及匿名化

資訊及通訊科技的資料保安建議措施

技術上及操作上的保安措施

資料使用者應採取**足夠及有**
和資訊及通訊系統：



- 在網絡安裝**防火牆**，以防止未經許可的網絡連接，亦可偵測網絡攻擊
- 在電腦及伺服器安裝**防毒軟件**（反惡意軟件），以偵測及防止病毒及威脅
- 定期進行**保安漏洞評估**及**滲透測試**
- 使用**網站安全掃描服務**，定期掃描以偵測最新的已知或潛在的網絡安全風險
- 及時更新正在使用的系統及軟件，可以**修補保安漏洞**，減少被攻擊的機會

資訊及通訊科技的資料保安建議措施

資料保安事故發生後的補救措施

資料使用者在資料保安事故發生時可採取的補救措施：

- 停止並中斷連接受影響的系統
- 更改密碼或中止權限
- 更改系統配置
- 通知受影響人士並提供建議
- 通知私隱公署及其他執法或監管機構
- 修補保安漏洞
- 在可行情況下掃瞄系統
- 汲取經驗及教訓

NOTE

資料使用者亦應從資料保安事故中汲取經驗及教訓，覆檢和加強其整體資料管治和資料保安措施

資訊科技相關指引及報告

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

- 資料外洩事故的處理及通報指引
- 人工智能 (AI): 個人資料保障模範框架
- 《人工智能 (AI): 個人資料保障模範框架》單張
- 《電子點餐的私隱關注》報告
- 《數碼時代的私隱保障：比較十大網購平台的私隱設定》報告
- 社交媒體私隱設定大檢閱
- 開發及使用人工智能道德標準指引
- 保障個人資料私隱 – 使用社交媒體及即時通訊軟件的指引
- 資訊及通訊科技系統的貫徹數據保障設計指引

www.pcpd.org.hk

謝謝！Thank you!