香港華人會計師公會
會計師持續專業進修嘉年華

資料外洩事故趨勢及分享

鍾麗玲女士
香港個人資料私隱專員

2024年11月16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

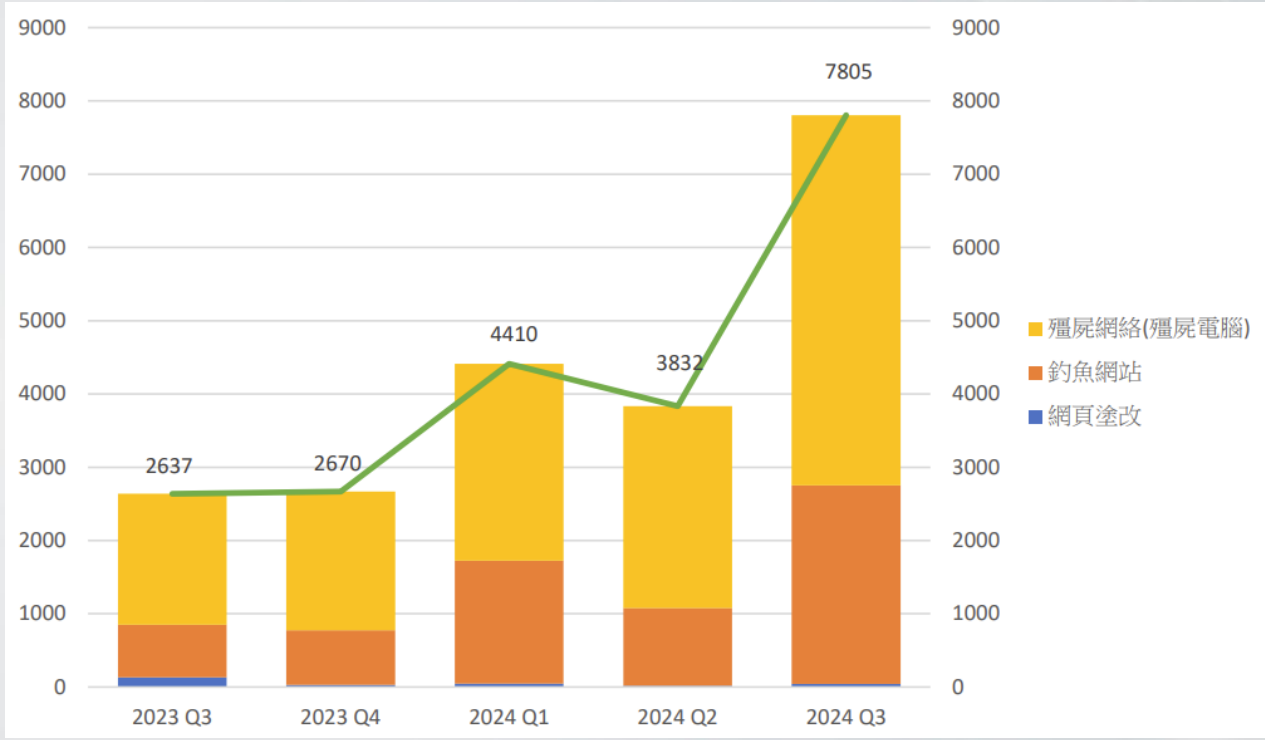
全球趨勢

- 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》[1]，2024年第三季度涉及香港的網絡保安事件宗數比上季**上升103.6%**，比去年同季更**上升196.0%**

- **殭屍網絡**（佔整體案例64.7%）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34.7%）



[1] 香港保安觀察報告 (2024年第三季度)：
https://www.hkcert.org/f/report/912892/916161/2024Q3%20HK%20SecurityWatchReport%20(Chinese).pdf

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

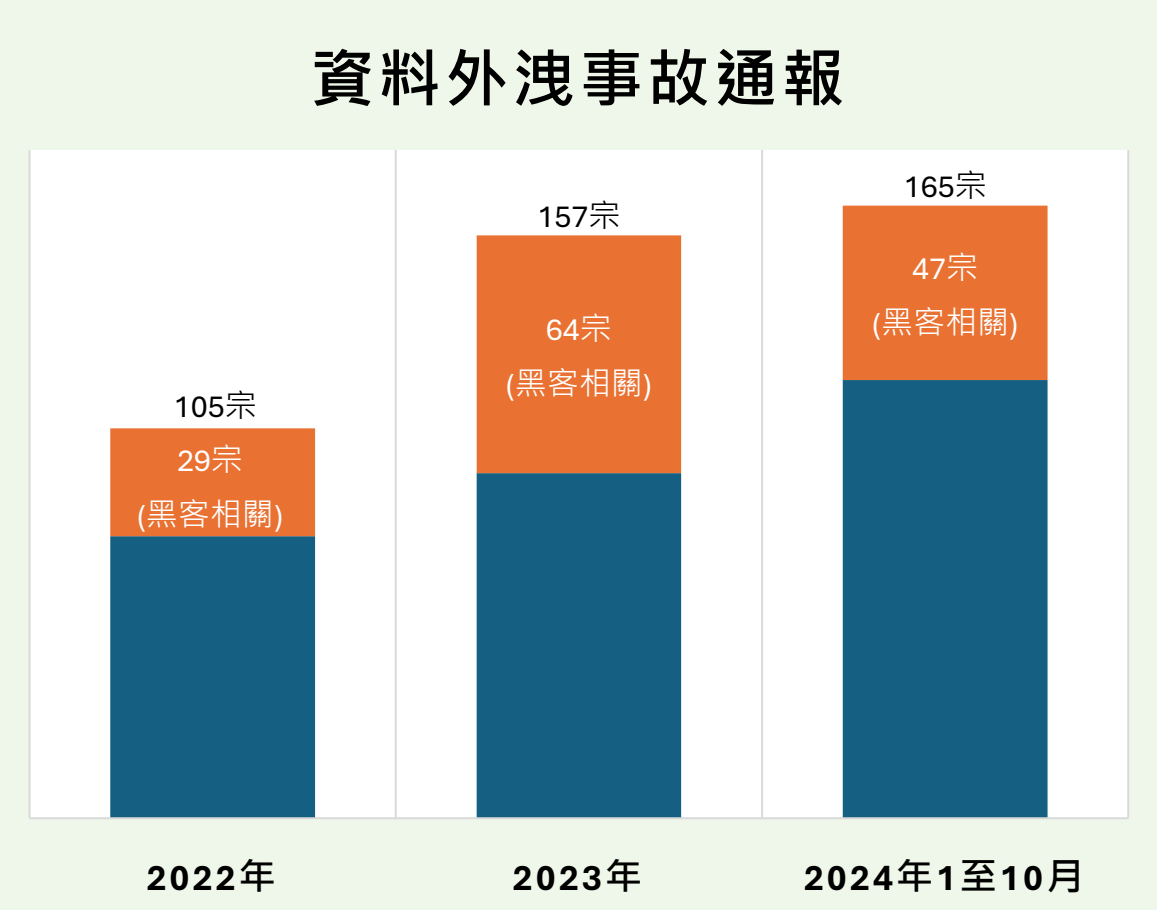
UnitedHealth hackers used stolen login credentials to break in, CEO says

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10個月**已接獲**165宗**通報，達2023年全年總宗數約**105%**
- 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10個月**，涉及**黑客入侵**的資料外洩事故共**47宗**

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

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

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

勒索軟件攻擊個案（1）– 資訊科技公司

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A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。

勒索軟件攻擊個案（1）– 資訊科技公司

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

勒索軟件攻擊個案（2）– 非牟利機構

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

- 2024年，非牟利機構B向私隱專員公署作出資料外洩通報，表示其伺服器遭**勒索軟件攻擊及惡意加密**。有關的勒索軟件屬**Trigona的變種**，合共八台伺服器、一台數據儲存器及18台電腦遭受勒索軟件攻擊及加密。黑客曾要求機構支付贖金，為已被加密的檔案解鎖。

涉及**超過72,300名**會員的個人資料，當中包括姓名、香港身份證號碼、護照號碼、相片、出生日期、地址、電郵地址、電話號碼及緊急聯絡人的姓名及電話號碼。

勒索軟件攻擊個案（2）– 非牟利機構

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

調查結果發現六項缺失：

1. 伺服器被意外地**曝露於互聯網**
2. 資訊系統**欠缺**有效的**偵測措施**
3. **沒有**為管理員帳戶啟用**多重認證**功能
4. **欠缺**資訊**保安政策**及指引
5. **沒有**定期進行**風險評估**及**保安審計**
6. **欠缺**離線**數據備份**方案

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

技術上及操作上的保安措施

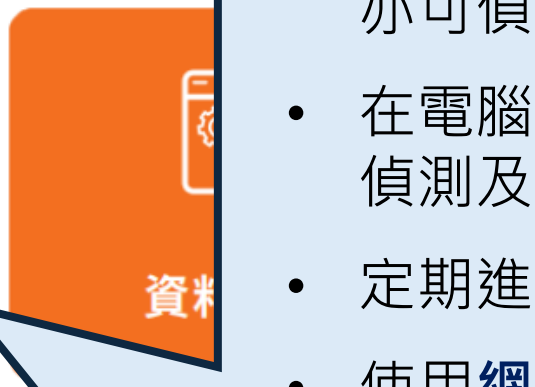
資料使用者應採取**足夠及有效的保安措施**，以保護其控制或所持有的個人資料和資訊及通訊系統：

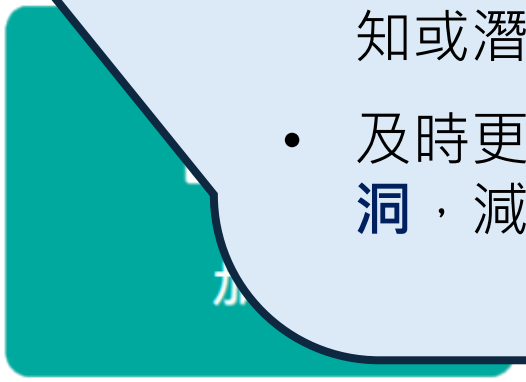
- 保護電腦網絡
- 資料庫管理
- 存取管控
- 防火牆和反惡意軟件
- 保護網絡應用程式
- 加密
- 電郵及檔案傳送
- 資料備份、銷毀及匿名化

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

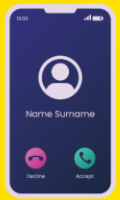
資訊科技相關指引及報告

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

- 人工智能 (AI)：個人資料保障模範框架
- 資料外洩事故的處理及通報指引
- 《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

「數據安全」套餐 “Data Security” Package



數據安全熱線
Data Security Hotline
2110 1155

數據安全快測
Data Security Scanner
https://www.pcpd.org.hk/Toolkit/tc/

數據安全專題網頁
Data Security Webpage
https://www.pcpd.org.hk/tc_chi/data_security/index.html

免費名額參加研習班及講座
Free quotas to join professional workshop and seminars

PCPD HK

PCPD.org.hk

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

謝謝！Thank you!