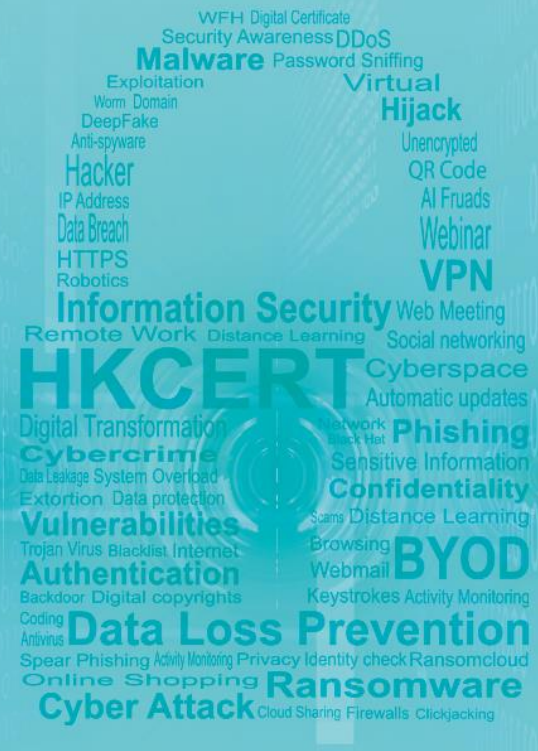
Hong Kong Computer
Emergency Response Team
Coordination Centre
HKCERT 香港電腦保安事故協調中心

香港保安觀察報告
2023 第一季度

發佈日期: 2023年5月



前言

提升資訊保安由認知做起

現今，有很多具備上網功能的數碼設備(例如個人電腦、智能手機、平板裝置等)，在用戶不知情下被入侵，令儲存在這些設備內的數據，每天要面對被盜取和洩漏，甚至可能被用於進行不同形式的犯罪活動的風險。

《香港保安觀察報告》旨在提高公眾對香港被入侵系統狀況的認知，從而作出更好的資訊保安選擇。這份季度報告提供的數據聚焦在被發現曾經遭受或參與各類型網絡攻擊活動（包括網頁塗改、釣魚網站、殭屍電腦等)的香港系統，其定義為處於香港網絡內，或其主機名稱的頂級域名是「.hk」或「. 香港」的系統。報告亦會回顧該季度所發生的重大保安事件及探討熱門保安議題，並提出易於執行的保安建議，提升公眾的資訊保安認知的水平，增強應對有關風險的能力。

善用全球保安資訊力量

本報告是香港電腦保安事故協調中心（HKCERT）和全球各地資訊保安研究人員共同合作的成果。很多資訊保安研究人員具有偵測針對他們或其客戶攻擊的能力，有些會把攻擊來源的可疑IP地址或惡意活動網絡連結的數據資料收集起來，並提供給其他資訊保安機構，以改善互聯網的整體保安。他們會遵守良好的作業守則，在分享數據前，先刪除個人身份資料。

HKCERT 建立Information Feed Analysis System (IFAS) 系統，收集和匯聚這些數據，對有關香港的資料進行分析。數據的來源廣泛和可靠，可以持平地反映香港資訊保安情況。

HKCERT會移除來自多個數據來源的重複報告，並以下面的統計指標來確保統計數據的質量。

網絡攻擊類型	統計指標
網頁塗改、釣魚網站	在本報告所述期間，錄得有關的單一網址的數量
殭屍電腦	在本報告所述期間，錄得各個殭屍網絡在季度內的同日單一IP 地址數量的最高值的總和

以下是IFAS資料的來源:

網絡攻擊類型	資料來源	開始使用
網頁塗改	Zone – H	2013-04
釣魚網站	CleanMX – Phishing	2013-04
釣魚網站	Phishtank	2013-04
殭屍電腦	Shadowserver - microso _sinkhole_events	2021-06
殭屍電腦	Shadowserver - microso _sinkhole_http_events	2021-06
殭屍電腦	Shadowserver - sinkhole_http_events	2021-06
殭屍電腦	Shadowserver - sinkhole_events	2021-06
殭屍電腦	Shadowserver - honeypot_darknet_events	2021-06

本中心採用以下方法去識別網絡的地理位置是否在香港。

方法名稱	開始使用	最後更新
Maxmind	2013-04	2023-04

更好的資訊帶來更好的服務

HKCERT將來會加入更多有價值的數據來源以進行更深入的分析，持續改善報告內容，亦會探討如何最有效利用這些數據提升 HKCERT 的服務。請發送電郵至*hkcert@hkcert.org* 反饋閣下的意見。

報告的局限

本報告的數據來自多個途徑，他們有不同的來源、收集週期和表達方式，各自亦存有局限，因此數據只宜作為參考，不宜用作直接比較或視為反映現實的全貌。

免責聲明

本中心可隨時更新或修正報告，恕不另行通知。對於本報告內容及數據中出現的任何錯誤、偏頗、疏漏或延誤，或據此而採取之任何行動，本中心概不負上任何責任。對於因使用本報告內容及數據而產生的任何特殊的、附帶或相應的損失，本中心概不負上任何責任。

授權條款

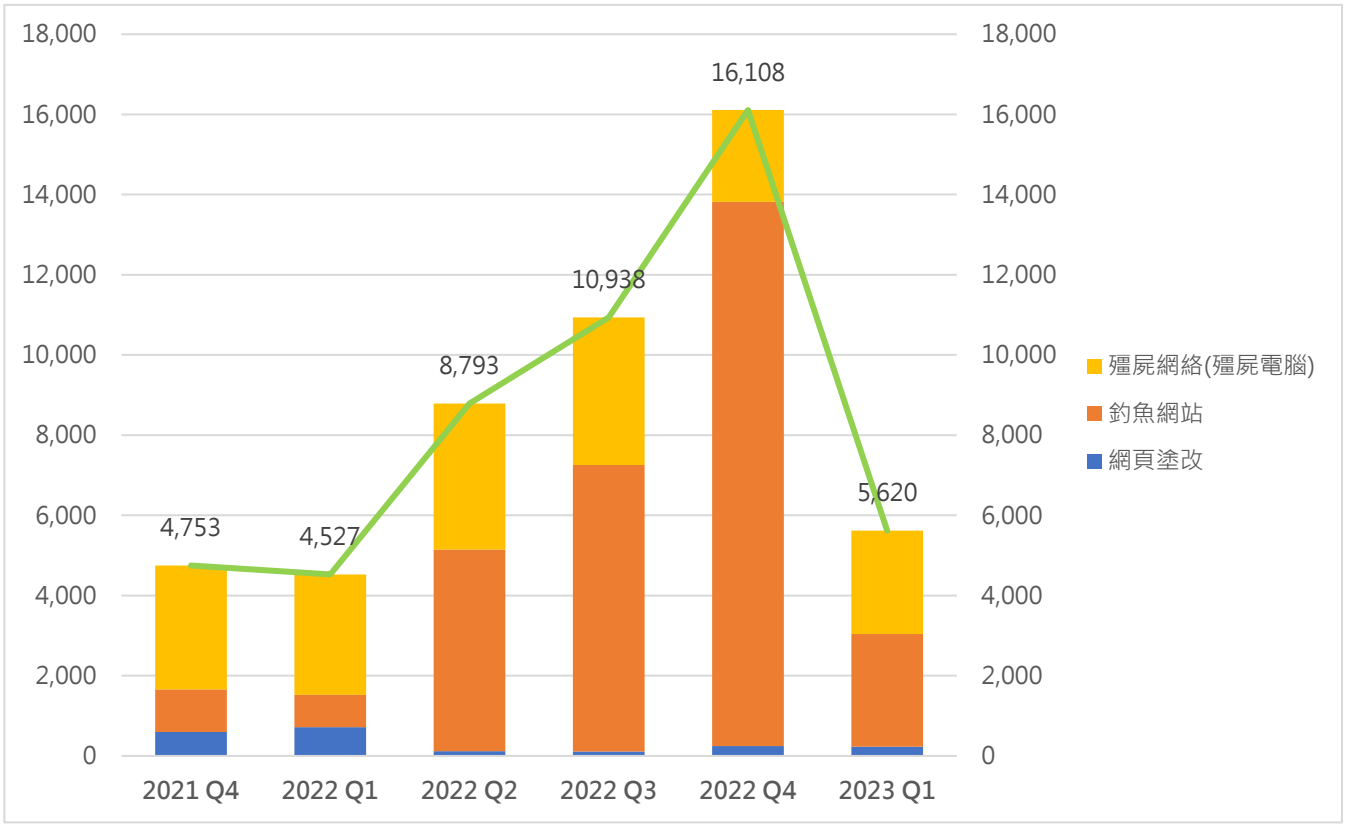
2023 第一季度報告概要

涉及香港的單一網絡保安事件宗數

5,102

按季下跌

65%↓



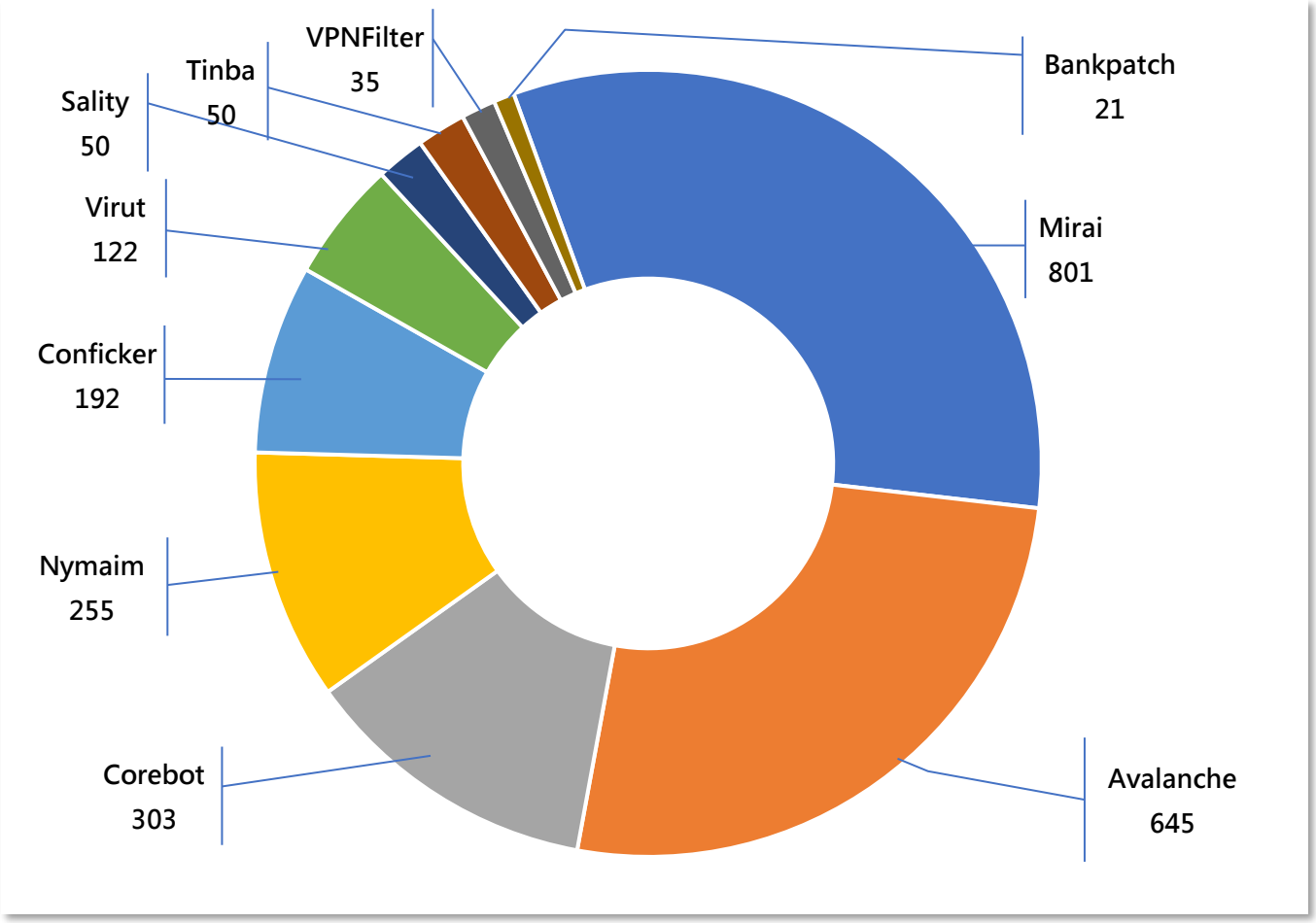
事件類別	2022 Q1	2022 Q2	2022 Q3	2022 Q4	2023 Q1	按季
網頁塗改	718	118	113	249	233	-6%
釣魚網站	806	5,033	7,141	13,574	2,804	-79%
殭屍網絡(殭屍電腦)	3,003	3,642	3,684	2,285	2,583	+13%
總數	4,527	8,793	10,938	16,108	5,620	-65%

香港網絡內的主要殭屍網絡

Mirai
801
↓ 20.0%

Avalanche
645
↑ 51.1%

Corebot	303	+152.5%
Nymaim	255	+54.5%
Conficker	192	-7%
Virut	122	+1425%
Sality	50	+127.3%
Tinba	50	-56.9%
VPNFilter	35	-5.4%
Bankpatch	21	-80%



** 主要殭屍網絡指在報告時間內，透過資訊來源有可觀及持續穩定的數據。殭屍網絡的規模是計算在報告時間內，每天嘗試連接到殭屍網絡的單一IP地址總數的最大值。換言之，由於不是所有殭屍電腦都會在同一天開機，因此殭屍網絡的實際規模應該比以上的數字更大。*

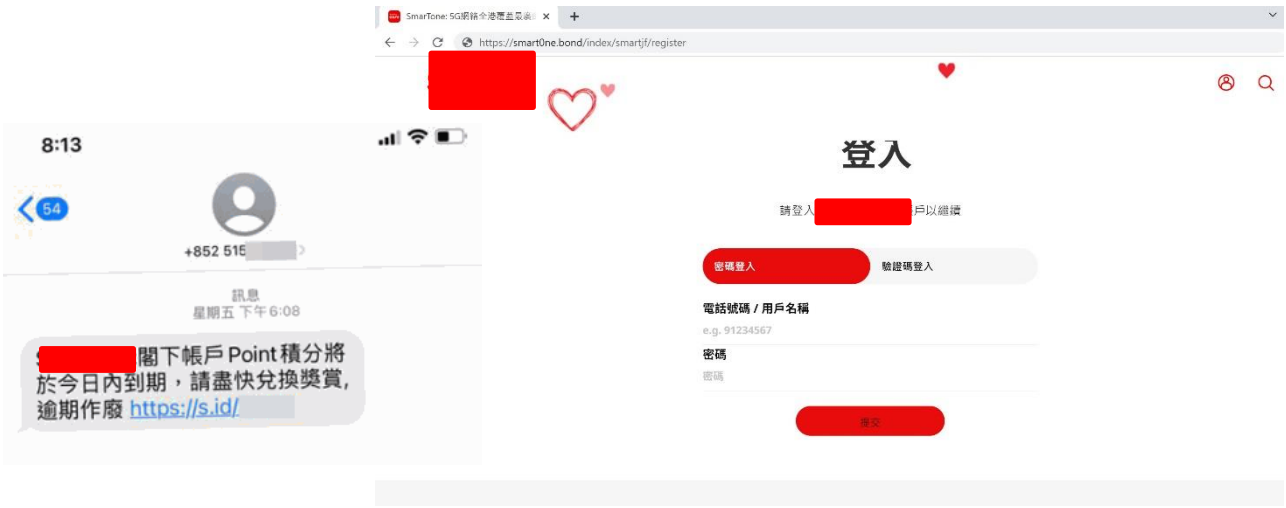
市民求助誤中本地購物獎賞計劃和電訊商網絡釣魚訊息

本季因涉及信用咭公司釣魚網站減少，所以釣魚網站數字明顯下跌79%，但值得注意的是，有關數字只反映寄存於香港系統內的網站情況，並不包括海外。換句話說，黑客可以將釣魚網站寄存海外伺服器，但攻擊香港用戶。例如本季本港就曾發生多宗有關釣魚攻擊引致香港用戶重大損失的例子(下文會探討有關攻擊)，當中涉及的釣魚網站亦是寄存於海外。由此可見，公眾絕不能掉以輕心，對任何可疑的訊息都要保持警惕。

近期本港發生的網絡釣魚個案例子

最近，包括購物獎賞計劃和本地電訊商等在內多個高知名度的網絡釣魚案件在新聞中曝光。HKCERT亦收到求助個案。

在本地電訊商案例中，網絡罪犯通過發送假郵件，冒充電訊商向客戶發送SMS。SMS包含一個連結，指向一個假網站，該網站看起來與電訊商的官方網站完全相同，但是旨在竊取使用者的登入資料。攻擊者還使用了一種稱為「品牌劫持」的技術，他們使用了一個域名，看起來與電訊商的正式域名相似。這很容易被不知情的使用者忽視。一旦用戶在假網站上輸入了他們的登入資料，攻擊者就能夠竊取他們的個人數據，並用於欺詐活動。這種攻擊可能會帶來嚴重的後果，包括身份盜用、財務損失和對受害者聲譽的損害。



在香港，一個受歡迎的獎賞計劃也被針對了類似的釣魚攻擊。攻擊者發送假SMS訊息，聲稱用戶內的積分將會到期，需要點擊連結領取獎賞。該連結指向一個假網站，看起來與該公司的官方網站完全相同，但目的是盜取用戶的個人資料，如聯絡電話。

為了保護公眾免受釣魚攻擊，HKCERT也為公眾提供一些安全建議：

1. 謹慎處理不知名的電子郵件，特別是那些要求點擊連結或提供個人信息的電子郵件。
2. 仔細檢查發件人的電子郵件地址及電話號碼，確保它是正確。
3. 在點擊連結之前，應先查看URL，確保它不是假網站。
4. 在可能的情況下使用多重或雙因素身分驗證，減少被入侵風險。
5. 保持您的電腦和流動裝置最新的安全更新和防病毒軟件。

「智慧城市」創未來 「智破釣魚」防騙局

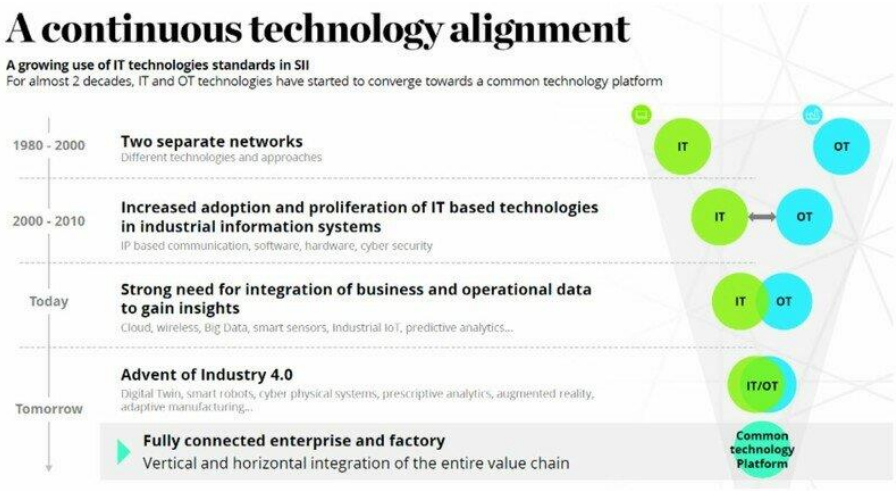
OGCIO（政府資訊科技總監辦公室）今年三月在各區舉辦了一系列智慧城市活動，旨在推動香港市民對智慧城市的認識和參與，並探討如何透過科技和網絡創建更安全、更方便、更宜居的城市。而保障用戶的網絡安全是創建智慧城市的重要任務，所以HKCERT 亦有參與活動，透過小遊戲及展板作介紹，提高市民慎防網絡釣魚攻擊的相關意識。

網絡焦點：如何減低工業系統聯網化所帶來的新網絡保安風險

近年，越來越多工商企業和公用事業機構會運用5G或物聯網（Internet of Things，簡稱IoT）技術高速度、高容量和低時延的特點，把工業營運技術（Operational Technology，簡稱OT）系統連接至資訊科技（Information Technology，簡稱IT）系統或互聯網，讓工廠機器及重要基礎設施設備的運作數據可即時回傳至IT系統，方便實時監察和分析機器和設備的運作情況，甚至自行調節運作參數，大幅提升生產效率及產能，進一步優化管理。

OT與IT的關係

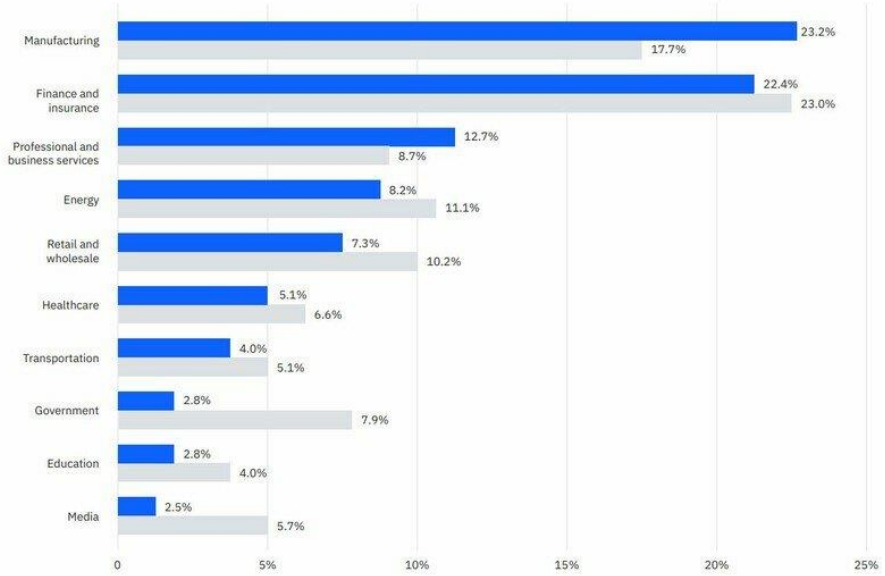
以往，OT系統及IT系統屬兩個完全獨立的網絡，前者有自己的通訊技術如Modbus等，與後者的TCP/IP協定不同，大家不能連接。現在兩者已漸採用統一的標準化協定或物聯網設備（IoT）將兩個系統連接及分享數據。未來OT系統及IT系統將會融為一體，促進工業自動及智能化。

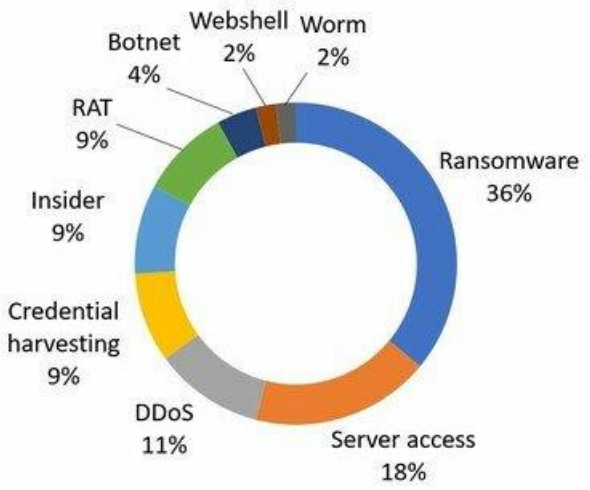


OT系統及IT系統融合帶來機遇，亦帶來新的網絡保安風險，其中一個例子是若將兩者互聯後，以往只影響IT系統的惡意軟件風險亦會延伸至OT系統。

事實上，此類風險已經成為現實。根據國際商業機器IBM的最新報告，製造業於2021年已經成為遭受最多網絡攻擊的行業，而勒索軟件攻擊是OT系統最為常見的網絡攻擊之一，原因是工廠主要倚靠OT系統持續運作來帶來收益，而黑客利用勒索軟件可癱瘓機器運作，直接令機構蒙受損失，更易傾向支付贖金解決問題；更甚的是如受影響機構是提供基礎關鍵設施，如電力，公用事業、交通等，受影響的更會是普羅大眾，黑客便可以此脅迫機構支付更大額的贖金。例如2021年3月，有黑客透過遠程軟件TeamViewer入侵美國佛羅里達州奧德馬爾市的電腦系統，更一度嘗試更改當地供水設施的化學品濃度，濃度足以令人體嚴重受傷。

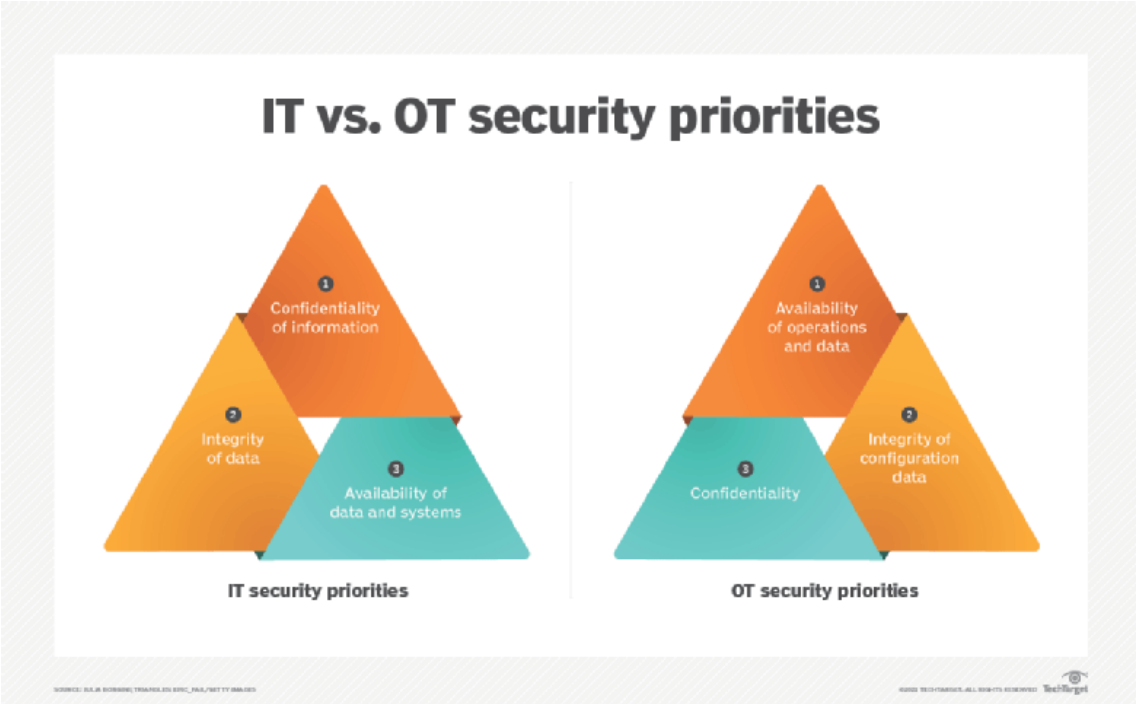
這篇保安網誌將會探討IT/OT融合帶來的挑戰，以及在融合前後的準備功夫，並會介紹減低風險的措施。





IT/OT融合帶來的挑戰

「工業4.0」現時最大的困難是如何穩妥地把OT系統及IT系統連接起來（IT/OT Convergence），因兩者對保安的考量優次不同：IT系統保安著重保護用戶數據，會經常引用CIA三要素概念【即機密性（Confidentiality）、完整性（Integrity）、可用性（Availability）】來制定保安措施，以數據保密及保護數據不被篡改為主要目的；而OT系統較少處理用戶數據，所以更著重確保機器可持續地、可靠地和安全地運作，以及保護運作參數。



除了這兩大分別外，OT系統及IT系統還有以下分別：

- 生命周期

  IT系統一般的生命周期較短，大約是3至5年。相反，OT系統的生命周期可以長達20多年。在工廠內不難看見不少舊OT系統仍然運作，公司及人力市場也缺乏了解這些系統的技術專才，在系統融合時容易造成技術斷層。

- 網絡安全標準和作業系統

  IT系統很早已經連接到互聯網，因此面對著黑客無時無刻的攻擊，已經具備一套成熟的資訊保安技術如數據加密等。至於OT系統，它們一般處於一個與世隔絕的網絡環境，在設計上數據會用低強度的加密方法來傳送，甚至是沒有加密。另外，OT系統多採用客制化的作業系統，任何重大改動都有機會影響不同機器間的協調運作，所以系統較難進行更新修復保安漏洞。再者，OT系統在設計時沒有考慮黑客攻擊，所以防護措施及相關的網絡保安發展，例如偵測非法入侵的措施、員工於事故後的回復和應變能力等，亦相對乏善足陳和落後。

- 維護要求

  IT系統在設計時一般會考慮「主副」機制，即使在主系統維護時需要重新啟動，副系統也能持續服務。OT系統在營運上難以實施「主副」機制，因成本上升意味生產效益下降。若要在維護時需要停運OT系統，會為生產力造成打擊。即使維修完成後，也需要進行保安測試，才能重新投入生產。對比IT系統，OT系統在維護時需要考慮更多因素，造成OT系統維護頻率相對較少，容易留下保安隱患。

兩者在系統設計上差異會造成不同的風險。

IT/OT融合前後的準備

在融合OT系統及IT系統前，需要充分的準備，以減低融合後帶來的風險。融合後，亦需要更新企業內部保安政策及營運守則。香港電腦保安事故協調中心（HKCERT）對此有以下建議：

- 進行網絡及保安評估

  對整個OT系統及IT系統進行深入的評估，包括網絡及安全兩方面評估。網絡評估是指對企業內所有系統資產、網絡結構及數據流向進步審查。安全評估則是對企業內的登入賬號、遠端接入方法、系統存在的漏洞及網絡服務進行分析；

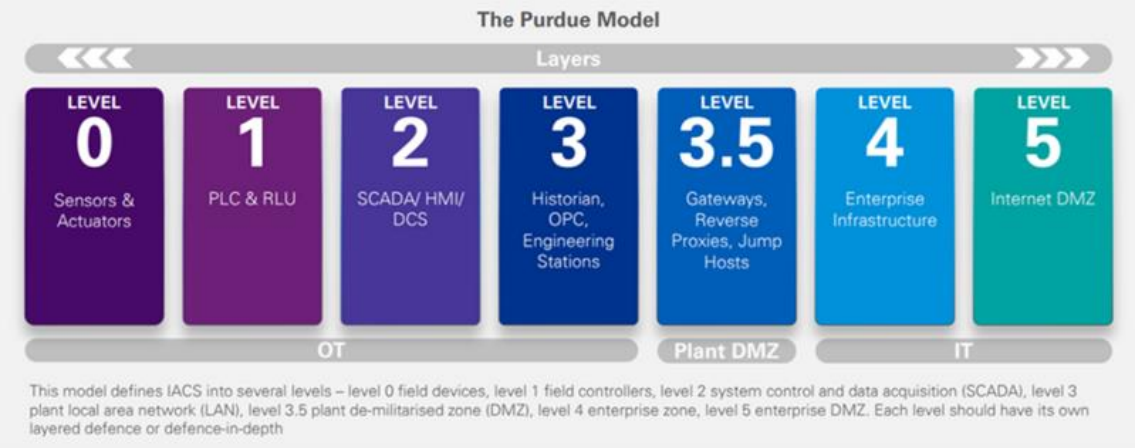
- **撰寫風險評估報告**

  從營運及資安角度，把營運、流程、系統等風險進行確認及分類。對所有風險制定建議及解決方法，並撰寫一份全面的評估報告。

- **制定實施計劃及嚴格執行**

  制定實施計劃前，釐清各方持份者的職責。在OT系統及IT系統融合前，把評估報告提及的風險先清理。制定詳細及清晰的融合計劃，並定立合適的時間表。操作人員需要嚴格執行實施計劃，在操作完成後進行評估測試。在制定融合計劃時，其中一個常見的挑戰是如何設計一個安全的架構，當中牽涉如何將不同設備分層及區間。業界有不同的標準模型可供參考，而普渡參考模型 (Purdue Reference Model) 便是其中之一個。

  這個電腦整合製造模型於1990年代由美國印第安納州普渡大學的學者提出，共分為七個分層，每個分層都有各自功能及相關系統，亦是一個網絡分段，可藉由不同的網絡保安措施控制存取，防止攻擊者由其中一個網絡 (例如: IT 網絡)入侵至另一個網絡(例如: OT 網絡)。以下圖為例，3.5層是防止 IT 和 OT 之間的橫向威脅移動，一般是放置防火牆和代理等安全系統。使用者可根據機構的實際情況來設計合適的架構。



除普渡參考模型外，「零信任」架構是另一個值得參考的保安架構，當中提倡微分段原則、數據加密、存取任何數據和系統服務皆要經過認證及以最小授權原則來進行。

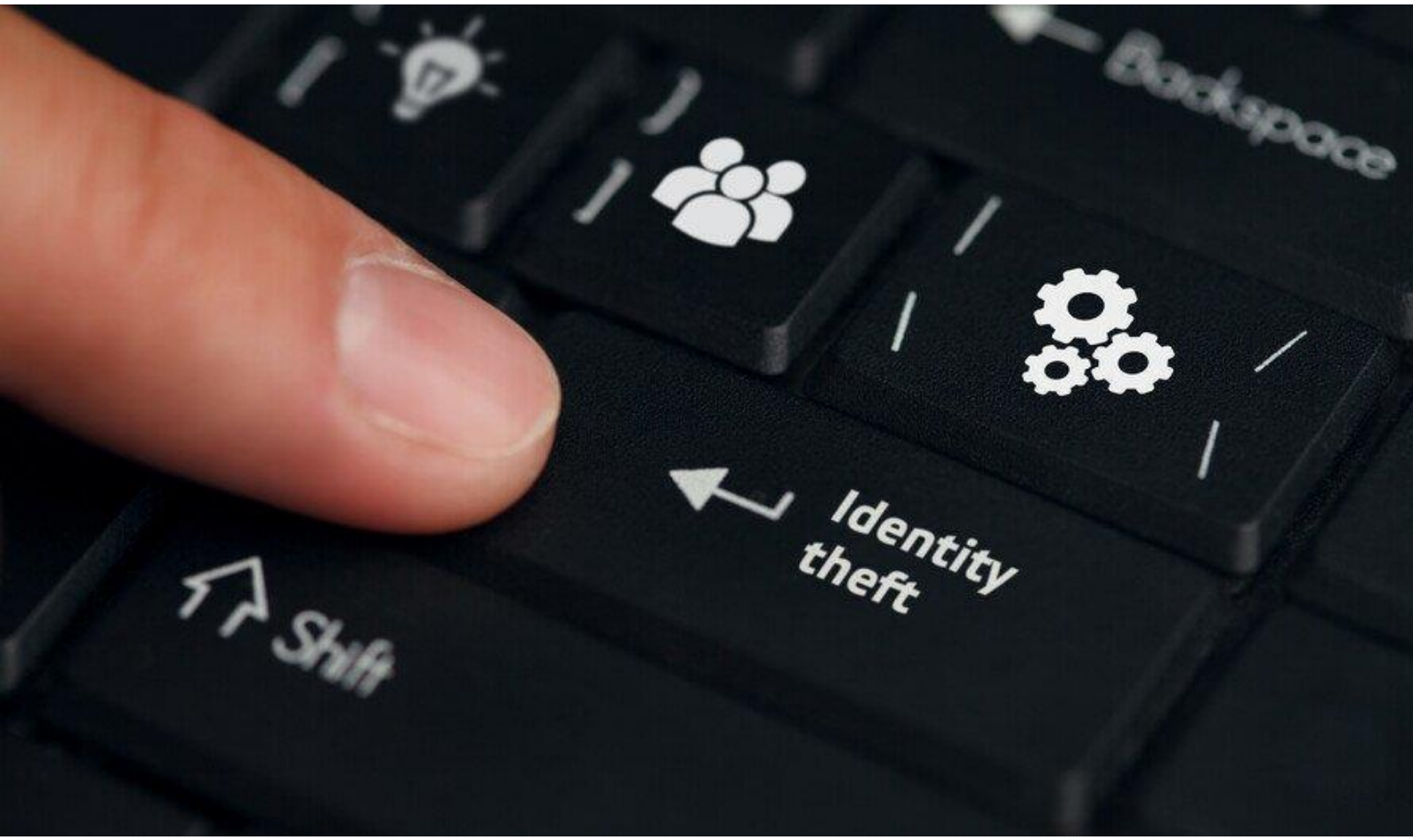
- **更新營運政策**

  融合後，IT團隊及OT團隊會增加工作接觸機會。企業可以考慮重組這兩個團隊，甚至增聘IT及OT技術兼備的專家來協助營運。在維護方面，由於OT系統連接到IT系統，雙方團隊需要同步及統一資訊安全標準。另外，對過往未能監管的系統立即進行修正，以免黑客隱藏在企業系統進行攻擊。

另外，將IT/OT系統融合通常是透過建立IoT網絡及使用不同的IoT設備作為傳感器或收集數據，所以IoT設備的保安措施也能應用得上。就此，HKCERT在 2020發佈了《物聯網保安最佳實踐指引》，內容涵蓋應用**IoT設備時要注意的網絡保安事項。大家可以此作為參考。**

詳細資料可參閱HKCERT保安博錄
https://www.hkcert.org/tc/blog/how-to-mitigate-new-cyber-security-risks-arising-from-the-growing-use-of-technology-in-industrial-operations

網絡分析：你知道什麼是身份 / 憑證盜用嗎？



身份和憑證的網上盜用並不是一個新事物。然而，2019冠狀病毒病疫情加速了大家在工作和生活上對網上服務的日益依賴，從而為網絡犯罪分子創造更多竊取個人資料以謀取私利的機會。因此，HKCERT 將身份/憑證盜用列為 2023 年五大資訊保安風險之一。

什麼是身份認證及身份攻擊

身份認證是指驗證瀏覽資訊或服務權限的授權的過程，用作驗證並確保用戶有權瀏覽這些內容或服務。身份認證最常見的例子是使用用戶名和密碼登錄，而有關技術最近更已經發展到可以利用指紋或面部來識別用戶身份。儘管大多數身份認證技術都是值得信賴的，但都可能存在缺陷。而這些缺陷往往會遭網絡犯罪分子利用來發動攻擊。

顧名思義，身份攻擊是針對身份認證進行的攻擊，以帳戶或憑證作為攻擊途徑（attack vectors），偷取密碼、密鑰（ key）、會話令牌(Session Token)、用戶帳戶信息和其他詳細信息以假冒用戶身份。如果組織中較高權限的身份認證被偷取，更可以被利用作不同的惡意行

為，例如分發勒索軟件或入侵系統偷取機密文件等等，最終招致重大損失。

近年攻擊趨勢

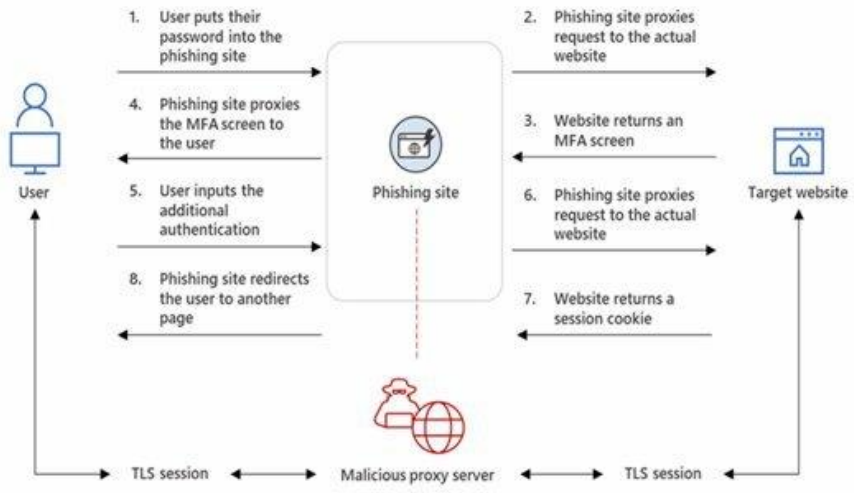
網絡釣魚是近年日趨頻密的最常見的身份攻擊方法之一。HKCERT 最新發布的《香港保安觀察報告》季度報告顯示，本地釣魚網站事件在 2022 年第四季首次錄得過萬宗，達 13,574 宗，按季激升 90%，較去年同期更上升逾 11 倍。此類攻擊的激增可歸因於開源網絡釣魚軟件包的氾濫，例如可以避開多重要素驗證 (multi-factor authentication, MFA)進行「連線劫持」的 Evilginx2。由此可見，針對身份的攻擊十分猖獗，並預計在可見的將來會繼續是一個主要的網絡安全威脅。

不同手法的身份攻擊

身份攻擊的手法層出不窮，了解不同的攻擊手法，可避免跌入陷阱。

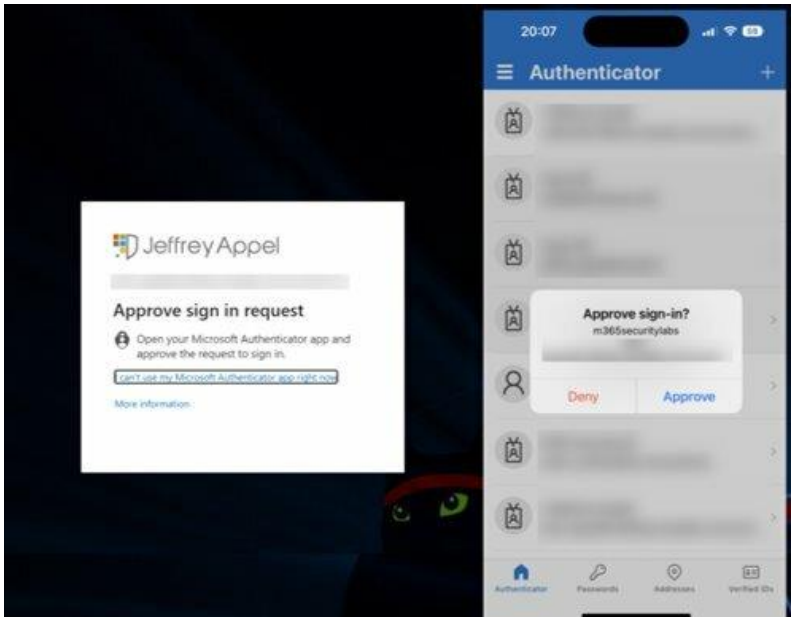
- 中間人攻擊(AiTM)釣魚

  網絡犯罪分子會利用電郵、SMS 簡訊等方法把與官方網站十分相似的釣魚網站連結發出，誘騙用戶登入。再以釣魚網站作為一個跳板，在受害人與官方網站中間代理登入請求，從而成功繞過 MFA 多重要素驗證。成功驗證後，把受害人載入官方網站繼續使用服務，而網絡犯罪分子在後台已成功偷取帳號資料及 Session Cookies，以用作不法行為。



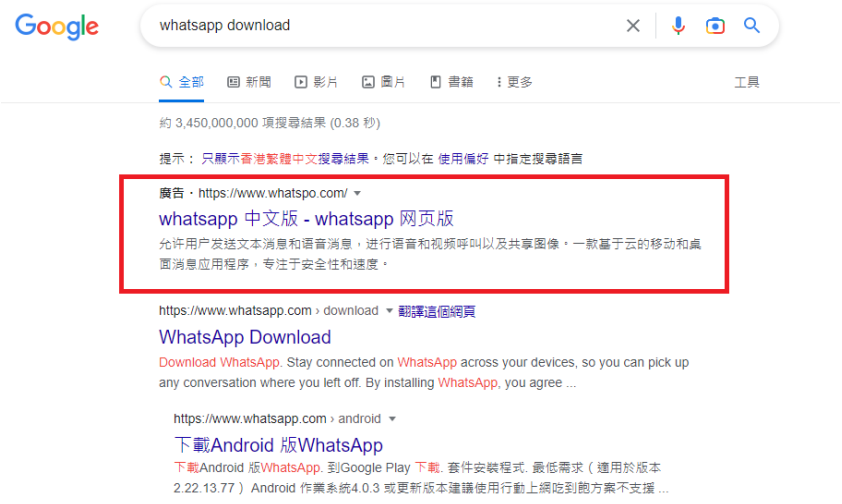
- **多重要素驗證 (MFA)疲勞攻擊**

  網絡犯罪分子通過不同渠道，例如利用外洩的資料或進行「暴力破解法」，不斷測試可能的密碼組合來找出帳號密碼。隨後不斷發出身份驗證確認訊息，疲勞轟炸受害人，直至受害人屈服或錯手按下同意。



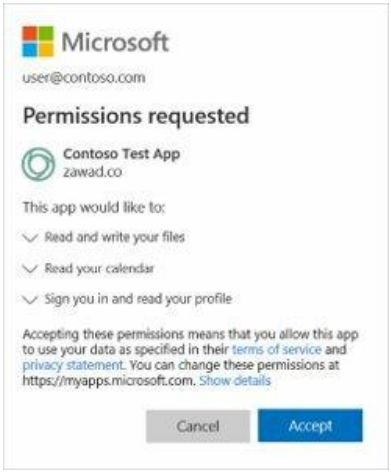
- **偽裝廣告**

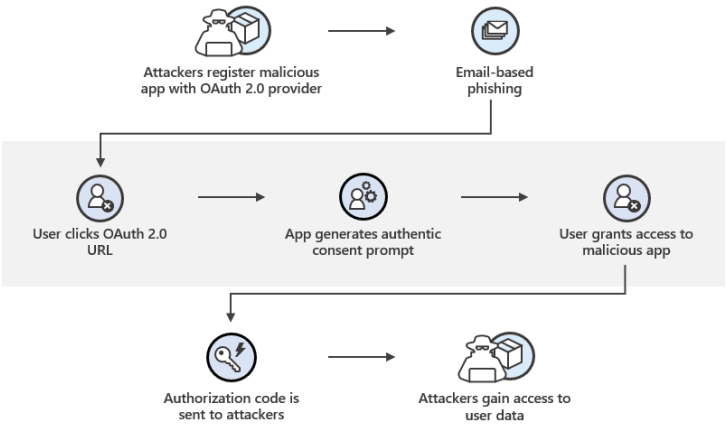
  網絡犯罪分子利用 Google 平台廣告功能，把惡意網站置頂，令用戶誤信惡意網站為正常網站。而惡意網站可能會誘使用戶下載安裝惡意程式或作中間人攻擊(AiTM)釣魚。



- **OAuth 釣魚攻擊**

  網絡犯罪分子誘騙受害者授予權限給惡意程式，允許程式利用 OAuth 2.0 協議訪問帳戶詳細信息並執行操作。當惡意程式取得相關權限之後，可隨時訪問用戶數據。Microsoft 亦曾發出警告，呼籲 O365 用戶小心這類型的授權。



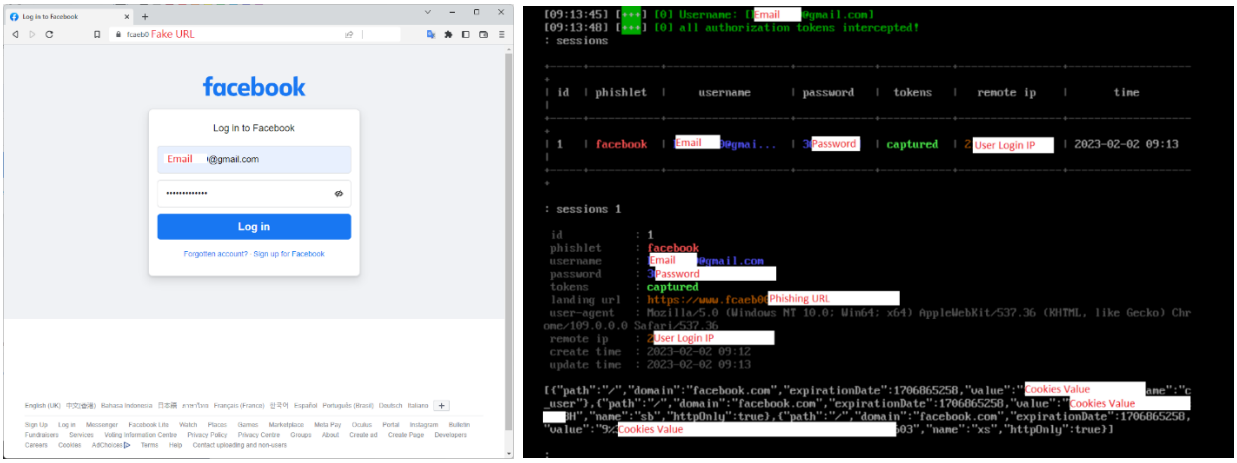


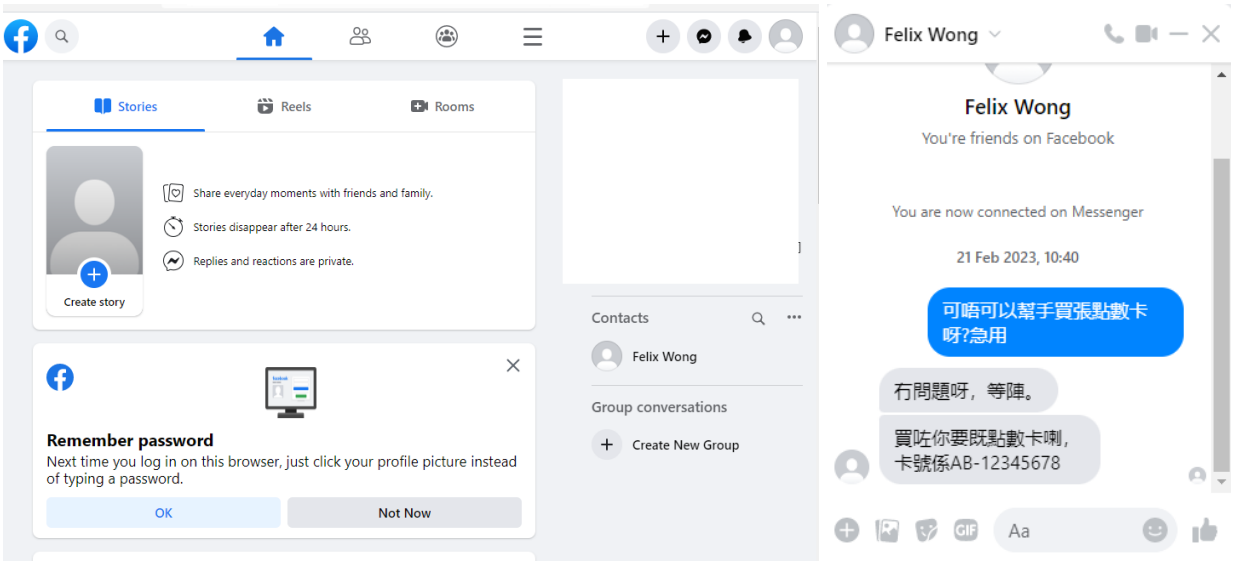
- **社交工程攻擊**

  網絡犯罪分子利用人的心理弱點來進行欺詐，例如會查看受害者社交媒體的內容，了解受害者的背景，冒充受害者的朋友或熟人，騙取受害人的個人資料，進行不法行為。

例子：中間人攻擊 (AiTM) 捕獲Facebook帳戶

以下是一個中間人攻擊的例子，網絡犯罪分子利用開源工具仿製了一個假 Facebook 登入專頁用以偷取帳戶資料。假登入專頁使用開源網絡釣魚軟件包來仿製及利用「誤植域名」令假登入專頁更像真。受害人在假 Facebook 登入專頁輸入帳戶資料及進行多重要素驗證 ，網絡犯罪分子在後台竊取帳戶資料及 Session Cookies，並利用所竊取的資料登入受害人帳戶及聯絡受害人朋友，進行詐騙。





總結及建議

以上提到了幾種不同的攻擊手法及攻擊例子。而隨著技術進一步發展，攻擊手法只會愈來愈多樣化。為防止個人資料或帳號被盜用，大家使用網上服務時需多加小心。就此，HKCERT 提供以下保安建議：

1. 切勿假設使用 HTTPS 協定的網站是絕對真實可信的
2. 切勿假設搜索引擎搜尋結果顯示的全為合法網站
3. 應小心檢查網址串法，核實網站真偽
4. 收到可疑電子郵件或 SMS 簡訊時，切勿打開任何連結或附件；可利用「CyberDefender 守網者」的「防騙視伏器」，通過檢查電郵地址、網址和 IP 地址等，來辨識詐騙及網絡陷阱
5. 向任何人或機構提供個人資料前要小心考慮清楚
6. 使用更高規格的認證技術，例如硬件 FIDO (Fast IDentity Online) 免密碼登入認證

7. **避免在不同平台或服務使用相同的**賬號和密碼
8. **使用網上服務後謹記登出及關閉瀏覽器**

詳細資料可參閱HKCERT保安博錄
https://www.hkcert.org/tc/blog/do-you-know-what-is-identity-credential-theft

資安小貼士：提防假冒ChatGPT應用程式及釣魚網頁

人工智能聊天機器人ChatGPT在2022年11月推出後短短兩個月便獲得1億用戶垂青，最近更推出一項名為ChatGPT Plus的付費訂閱服務。不幸的是，黑客亦借此機會，通過提供虛假的應用程式或免費使用高級服務作招徠，誘使用戶下載惡意軟件或分享敏感資訊。

根據網絡安全情報公司 Cyble 的報告，黑客建立了類似官方網站、社交媒體頁面和流動應用程式的假網站，誘騙使用者下載惡意軟件。至今 Cyble 已經發現逾 50 個假冒和惡意的應用程式，它們會使用 ChatGPT 商標來進行詐騙活動，包括 SMS 欺詐、間諜軟件和帳單欺詐。

針對這情況，香港電腦保安事故協調中心（HKCERT）提醒用戶：

- 一旦 ChatGPT 服務正式開放予香港用戶使用，應只通過 ChatGPT 的官方渠道（https://chat.openai.com/）訪問該服務；
- 只從官方應用商店和有信譽的出版商下載安裝應用程式；
- 通過使用社交媒體驗證徽章功能（如 Facebook 和 Instagram 的藍色徽章）來驗證社交媒體頁面；
- 切勿打開來歷不明的檔案、網頁或電子郵件；可利用「CyberDefender 守網者」的「防騙視伏器」來辨識詐騙及網絡陷阱，此搜尋器支援檢查電郵地址、網址和 IP 地址等；和

- 保持系統、軟件和防病毒軟件更新。

詳細資料可參閱HKCERT保安博錄
https://www.hkcert.org/tc/blog/hkcert-security-tips-beware-of-fake-chatgpt-apps-and-phishing-websites

-完-

香港電腦保安事故協調中心
電話：8105 6060
電郵：hkcert@hkcert.org