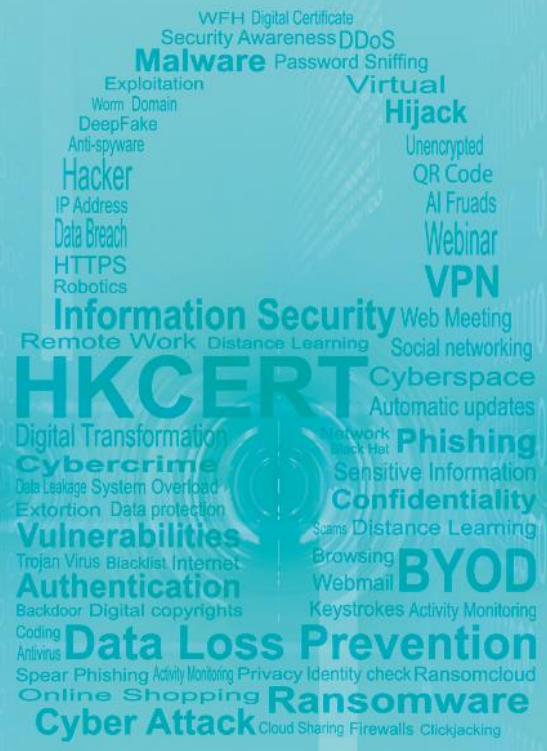
Hong Kong Computer
Emergency Response Team
Coordination Centre
HKCERT 香港電腦保安事故協調中心

香港保安觀察報告
2024 第一季度

發佈日期: 2024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	2024-04

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

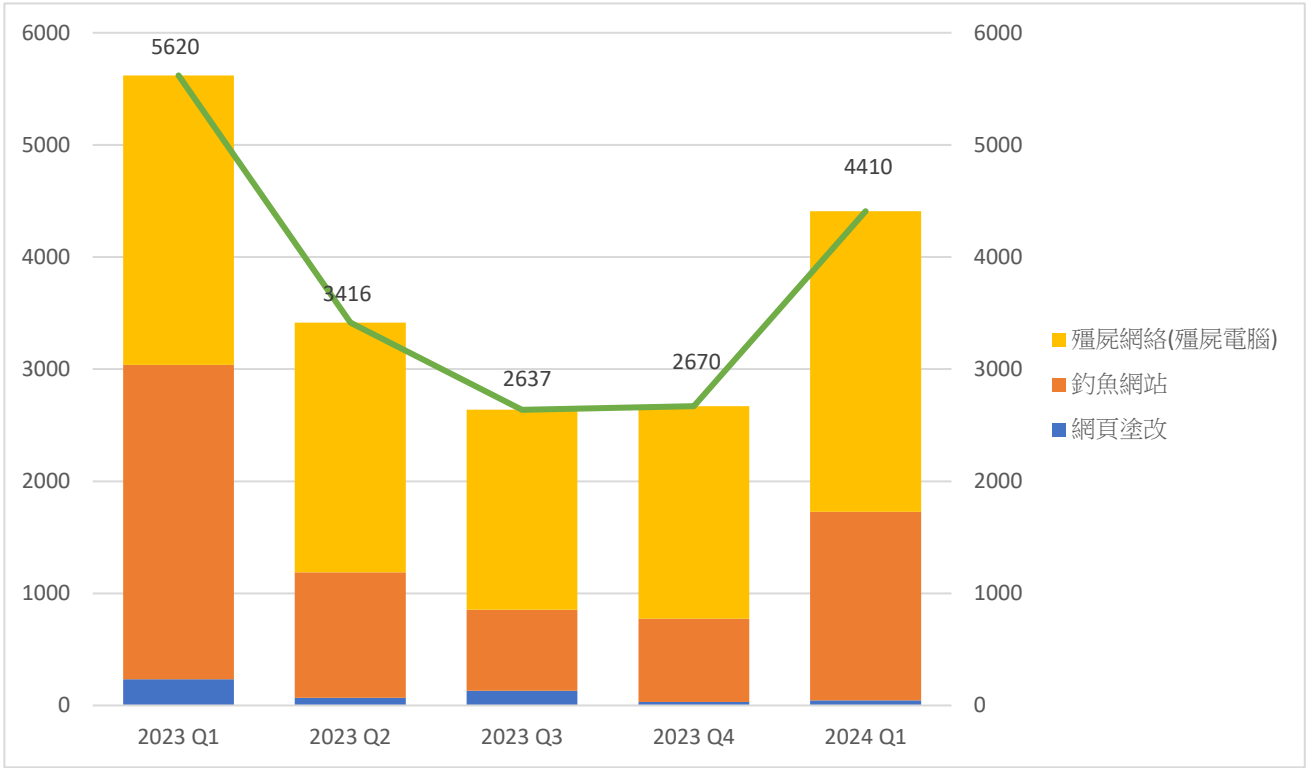
2024 第一季度報告概要

涉及香港的單一網絡保安事件宗數

4,410

按季上升

65.2%↑



事件類別	2023 Q1	2023 Q2	2023 Q3	2023 Q4	2024 Q1	按季
網頁塗改	233	69	132	31	46	+32.6%
釣魚網站	2,804	1,120	722	742	1,682	+126.7%
殭屍網絡(殭屍電腦)	2,583	2,227	1,783	1,897	2,682	+41.4%
總數	5,620	3,416	2,637	2,670	4,410	+65.2%

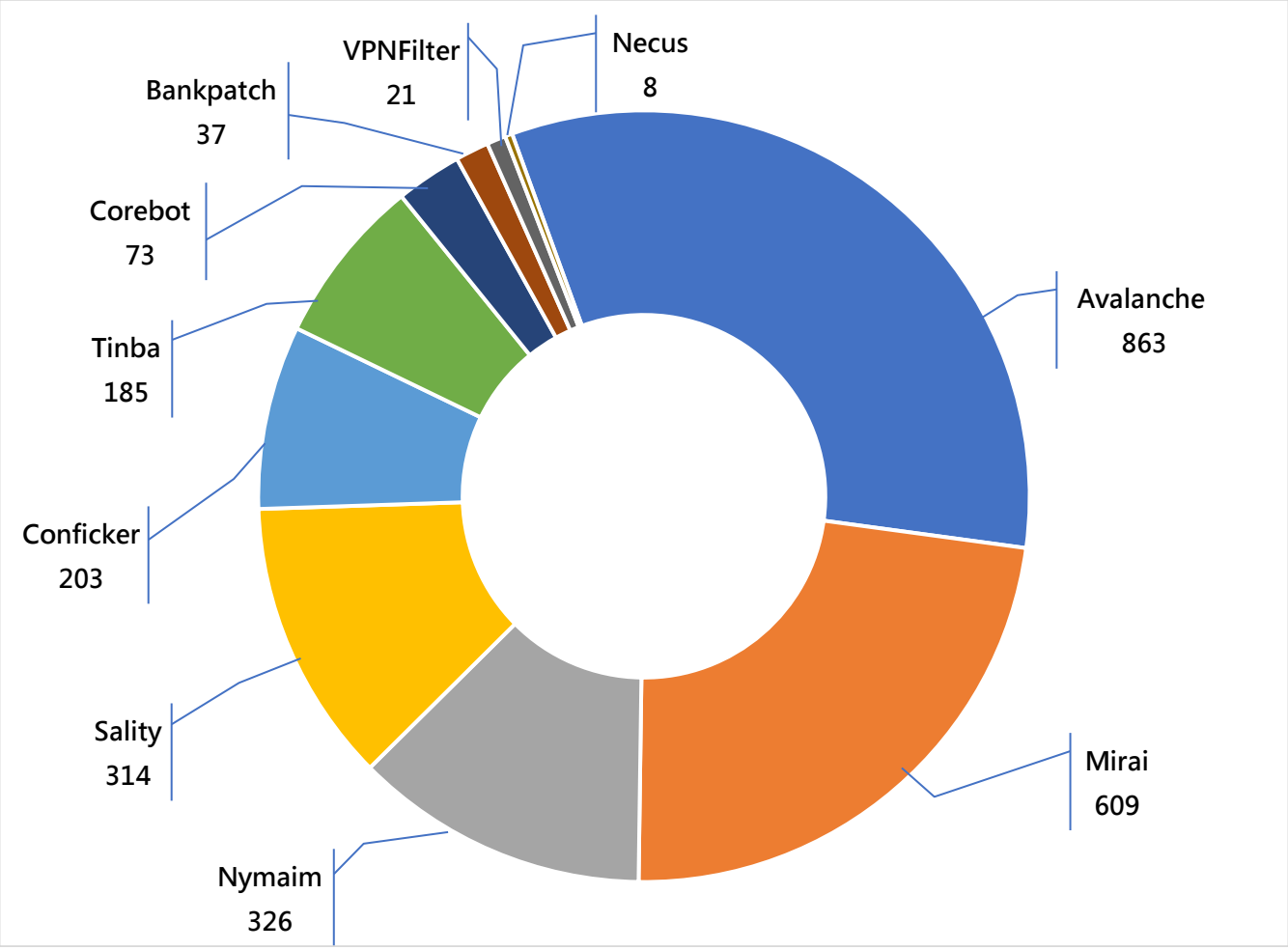
香港網絡內的主要殭屍網絡

Avalanche
863
↑ 99.3%

Mirai
609
↓ 17.7%

Nymaim	326	+176.3%
Sality	314	+1644%
Conficker	203	+13.4%
Tinba	185	+50.4%
Corebot	73	+564.6%
Bankpatch	37	-15.6 %
VPNFilter	21	-25%
Necus	8	-38.5%

111



** 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。*

網絡保安風險高企　及時提醒公眾防範尤其重要

2024年第一季網絡事件數字正式出爐，今季的網頁塗改、釣魚網站及殭屍網絡錄得明顯的增長，按季分別上升32.6%、126.7% 及 41.4%。接近40%的釣魚連結包含字串”usps”或”usops”，相信黑客故意在長假期的網購熱潮後，冒充美國的郵政或送遞包裹的機構網站來博取用戶點擊。

殭屍網路Avalanche的數量較上一季增加了近一倍，該殭屍網路病毒會偷取用戶的網上銀行密碼，亦會充當其他惡意軟體的下載程式。

有關數字只反映攻擊源頭寄存於香港的情況，並不包括海外。換句話說，黑客有機會將攻擊源頭寄存海外伺服器，但針對香港用戶，而這類攻擊源頭並不反映在此報告的數字上面，所以實際數字或會更高。顯示網絡攻擊頻繁，公眾需要加緊防範。

應對日益增加的網絡保安風險，HKCERT在2024年2月於網頁新增資訊保安風險警報功能。HKCERT會收集世界各地保安情報來進行分析及評估，若發現網絡攻擊轉趨活躍，HKCERT會在網頁刊登警報提醒公眾，以應對潛在的網絡攻擊。警報包含警報種類、現況及趨勢分析、資訊保安建議及情報來源。共有三種警報類別，分別是網絡釣魚、惡意軟件和殭屍網絡。

警報類別

截至3月，HKCERT就刊登過網絡釣魚警報及惡意軟件警報，來提醒公眾預防最新的釣魚手法及惡意軟件攻擊。公眾可以在HKCERT網頁頂部或保安公告搜尋相關警報。

(過往HKCERT發出的保安警報：https://www.hkcert.org/tc/tag?q=風險警報)

2024年五大資訊保安風險

另外，HKCERT亦總結 了2023 年香港網絡保安狀況並發布 2024年資訊保安預測。人工智能等新興科技能為企業帶來額外效益，但隨新興科技發展而來的網絡攻擊陸續浮現，網絡威脅日趨複雜，企業和市民應多加認識網絡保安資訊，提高應對網絡風險的能力。

1. 人工智能「武器化」：人工智能懂得編寫程式，降低了成為黑客的技術門檻。例如，黑客可利用生成式人工智能下達指令，產生惡意程式碼，主導大規模的網絡攻擊。此外，黑客亦可以運用人工智能產生欺詐數據，影響其他人工智能的輸出，癱瘓網絡保安措施。黑客亦會使用人工智能生成虛假影片，以便進行勒索或騙取利益。

2. 新一代釣魚攻擊： 黑客除了以電郵、短訊等傳統方式作釣魚攻擊，亦會利用AI Deepfake技術製作虛假影片假冒身分，甚至於社交平台設置假冒品牌專頁，騙取受害人的信任，從而騙取金錢。同時，黑客利用搜尋引擎的優化功能，令釣魚網站位列搜尋結果前列，混淆視聽，令搜尋引擎使用者容易錯誤地登入假冒網站，欺騙更多受害者。

3. 網絡犯罪趨向組織化：2023年，香港出現多宗針對企業的勒索軟件攻擊，被勒索大額金錢及公開敏感資料。而市民則面對「毒App」和網絡釣魚的威脅。宏觀全球，2023年的勒索軟件攻擊及漏洞數量再創新高，都顯示此等有組織及系統的網絡犯罪日趨嚴重。

4. 針對智能設備的攻擊：新式的電子產品大多具備網絡連接功能，可連接其他產品或互聯網。這些產品的網絡安全標準不一，容易被入侵和惡意操控。部分產品無法修補保安漏洞，難以堵截網絡攻擊。

5. 使用第三方服務的風險：大多企業都會使用其他公司提供的IT服務，如軟件、IT人員等等，從而衍生IT供應鏈攻擊及公司內部網絡安全風險，引致數據洩漏、勒索軟件攻擊等後果。此外，研究指出，生成式人工智能或會產生錯誤的訊息，例如有保安漏洞的程式碼或不實資訊，如企業未經核實就直接採用，則為其業務帶來負面風險。

塗改攻擊：認識和預防

什麼是塗改攻擊？

當黑客滲透線上網站或電子廣告板硬件並用攻擊者的訊息替換其內容時，就會發生網站塗改攻擊。 這些資訊的範圍從政治或宗教聲明到惡意言語或令人尷尬的內容。

以下是塗改攻擊的一些常見原因。

1. **未經授權的存取：黑客未經授權進入網站或電子廣告板的內容管理系統，從而改變其外觀。**
2. **SQL注入：利用網站資料庫或儲存裝置中的漏洞來操縱內容。一些數位內容顯示面板設備也基於網路協定。**
3. **DNS 劫持：透過偽造 DNS 回應將使用者重新導向到不同的伺服器。**
4. **惡意軟體感染：以惡意軟體修改網站內容或感染電子廣告板的作業系統從而取得控制**
5. **雲端資源攻擊：黑客取得雲端服務的登入憑證用以入侵並控制其雲端資源，對網站儲存**

裝置或經雲端管理的裝置進

塗改攻擊的真實事故：

1. 在以色列的電子廣告板塗改攻擊事故（2023）：
    - 黑客入侵了電子廣告板，將廣告切換為反以色列、支援哈馬斯的影片。
    - 調查指出該電子廣告板的網絡僅向外開放幾分鐘，黑客對其裝置便立即進行入侵攻擊。
2. 烏克蘭政府網站塗改攻擊事故（2022）：
    - 黑客成功入侵多個烏克蘭政府網站，並在主頁上顯示發布的挑釁性訊息。
    - 烏克蘭 CERT 指出攻擊者可能利用了基於 Laravel 的 October CMS 中的漏洞。
3. 喬治亞最大規模的網路攻擊事故（2019）：
    - 15,000 個喬治亞網站遭到破壞並關閉。
    - 政府網站、銀行和媒體都成為攻擊目標。
4. NHS 塗改攻擊事故（2018）：
    - 英國國家醫療服務體系 (NHS) 網站遭到駭客破壞，引發人們對醫療資料安全的擔憂。
    - 塗改資訊已被刪除，但對 NHS 聲譽的損害仍然存在。
5. Google.ro 和 PayPal.ro 塗改攻擊事故（2012）：
    - DNS 劫持導致用戶進入被塗改的網頁，而不是 Google 羅馬尼亞網站。
    - 同樣的攻擊影響了paypal.ro網域。

塗改攻擊的影響：

1. 可信度喪失：塗改攻擊會破壞網站的可信度，影響其公司或機構的聲譽。
2. 資料外洩風險：塗改攻擊期間利用的漏洞可能會導致未經授權的存取和資料外洩。
3. 中斷服務：塗改攻擊會導致網站或數位內容顯示服務無法正常操作，繼而影響線上服務和中斷正常運作。

防止塗改攻擊：

1. 最低權限原則（Principle of Least Privilege – POLP）：
    - 將用戶權限限制為其工作所需的最低限度
    - 定期檢討並撤銷不必要的權限
2. 定期漏洞掃描：
    - 經常掃描網站或系統是否有漏洞

- 及時解決發現的問題

3. 安全編碼實淺：
    - 遵循安全編碼指南以防止常見漏洞
    - 驗證用家輸入的數據並清理資料
    - 使用可信任編碼庫進行開發，避免終止支援的編碼庫庫
4. 網站應用程式防火牆（Web Application Firewall – WAF）：
    - 安裝網站應用程式防火牆來過濾惡意流量
    - 阻止可疑請求並防止攻擊
5. 執行軟件更新：
    - 保持軟件更新到最新版本以修復漏洞
    - 設定定期檢查軟體更新

確保數據內容顯示面板裝置安全：

1. 物理安全：
    - 將面板安裝在安全位置
    - 使用防塗改外殼
    - 防備對管理連接埠物理上的存取
2. 網路安全：
    - 將顯示面板與內部或公司網路隔離
    - 定期更新韌體和軟體
3. 認證與授權：
    - 限制並只授權許可工作人員的訪問
    - 使用高強度的密碼和雙重認證
4. 監控和警報：
    - 時常監察顯示面板是否有異常狀況
    - 針對未經授權的更改設定發出警報
5. 執行韌體和軟件更新：
    - 保持軟件更新到最新版本以修復漏洞
    - 設定定期檢查韌體和軟件更新

機構亦有責任積極在其IT環境內維護網路安全以減輕與公共資訊相關的風險，當中也要專注於防範塗改攻擊。 HKCERT 敦促機構對此類網路攻擊保持警惕，並採用上文提及的保安最佳實踐。

詳細資料可參閱HKCERT保安博錄
https://www.hkcert.org/tc/blog/defacement-attacks-understanding-and-prevention

深度偽造：有圖未必有真相

> 「深度偽造(Deepfake)」是「深度學習(Deep learning)」和「偽造(Fake)」的組合詞。它利用深度學習技術訓練大規模的數據，包括人臉圖像、語音，以及視頻等。這些數據用於模仿和學習不同人的特征、動作和聲音。然後，再利用人工智能（AI）技術創建虛假內容，包括假的圖像、聲音和影片，從而實現AI換臉或者語音複製等功能。

AI換臉

AI換臉是一種利用AI將一個人的臉替換成另一個人的臉的技術。這種技術通過面部識別和面部捕捉來執行臉部替換。如今，只需一張人臉的正面照片，AI就能輕鬆完成替換過程。即使使用者的頭部在轉動，AI也能追蹤使用者的臉部位置及面向方向，將其與替換的臉部自然地融合。現時AI換臉技術主要有三種形式：

1. 將你的臉替換成照片內的人臉：把照片內的人臉「套」在鏡頭前的人的臉上。

來源：HKCERT YouTube Channel

2. 將你的表情應用到一幅照片上：捕捉攝像頭前人物的表情變化，包括嘴唇、眼睛、眉毛、面頰和頭部等表情動作，並將這些表情反映到照片中另一個人的臉上。通過這種方式，觀看者會覺得在和照片的人親身交流一樣。

來源：Xpression Camera Demo

3. 將語音生成表情：根據錄製或即時的語音輸入，生成照片內的人的臉部表情和頭部動態，並將照片轉換爲影片，看起來就像照片內的人在說使用者所輸入的聲音。然而，這項技術還處於研究階段，尚有很多限制。

來源：Emote Portrait Alive (EMO) demo

AI換臉技術的效果因應用情境而異。除了透過編輯已錄制的影片以外，有些工具甚至可以在實時視訊中替換臉部。通常，這種技術會產生逼真的替換效果，難以分辨真假。

語音複製

語音複製是一種利用 AI 複製聲音的技術。複製出的聲音聽起來像現實生活中的人聲，包括速度、音調、口音和風格。語音複製有兩種呈現方式：

1. 文字轉語音：使用者輸入文字，AI 系統用所複製的聲音將文字以讀出。
2. 語音轉語音：使用者輸入語音，這種方式則是將原始聲音替換爲複製的聲音。

要達到高品質的語音複製效果，通常需要大量的訓練資料（超過 10 小時的目標人聲錄音），和長時間的訓練（超過 10 小時，具體取決於硬體性能）。
透過上述兩種 AI 換臉和語音複製的技術，再結合大規模的資料訓練，我們可以在 AI 系統中創造出任何人的逼真覆制品，使其視視覺和聽覺效果都極具真實感，達到移花接木，難以分辨的地步。

網絡安全的新威脅

儘管深度偽造技術在娛樂和醫療領域中有著積極的應用，例如數位化重現已故演員的影像，或重現因疾病或意外失去聲音的人的聲音。然而深度偽造最廣為人知的用途卻是製作虛假的名人視頻或音頻，以傳播虛假或誤導性訊息。除此之外，人們也可能濫用這項技術來製作色情影像或進行詐騙。因此，深度偽造技術的危險性不容忽視，這種危險性在一些真實案例中得到了充分證實。

最近真實案例

1. 2023 年 8 月，一個犯罪集團因爲使用深度偽造技術偽造身分以申請貸款而被抓捕。

來源：明報

2. 2024 年 1 月，一段虛假視頻開始流傳，其中香港特首李家超在銷售投資產品。罪犯透過使用深度偽造技術生成了李家超的假聲音，使這段視頻看起來更加真實。

來源：明報

3. 2024 年 2 月，香港警方指出，一家跨國公司的財務員在視訊會議中被騙。罪犯利用深度偽造技術冒充了該公司的首席財務官，從而騙取了這家公司 2 億港元。

來源：HK01

4. 2024 年 2 月，一位烏克蘭 YouTuber 發現她的聲音和臉部被盜用，罪犯同樣利用了深度偽造技術將她冒充爲一位虛假網路名人在中國社交媒體上進行商品推廣。

來源：香港經濟日報

濫用深度偽造的影響

在如今的互聯網上，有許多深度偽造軟體提供了簡易使用的介面，使罪犯可以輕易地生成深度偽造內容，甚至通過雲端服務進行詐騙。這種易於獲取性使得在網路上創建和傳播深度偽造內容變得輕而易舉。

更令人擔憂的是，深度偽造技術甚至有可能繞過生物辨識安全系統（例如，臉部或聲音認證），進一步加劇網路安全的風險。此外，深度偽造技術的濫用還可能引發更多的網絡釣魚和詐騙，虛假和誤導資訊，以及帶來信任和信譽危機等負面影響。

網路釣魚和詐騙

來自香港和全球的犯罪案件令人擔憂。深度偽造技術使罪犯能夠創建更複雜的網路釣魚攻擊。過去，網路釣魚攻擊主要依賴文字資訊。 然而，借助深度偽造技術，罪犯越來越多地利用這個技術冒充他人身份，向受害人的親朋或同事進行詐騙行為。尤其在大家已習慣使用視訊通話或透過視像會議進行溝通的年代，更會促使騙徒制作更多深度偽造影片，蒙騙受害人。

虛假和誤導資訊

罪犯制作冒充名人、政要、官員等的深度偽造影片來傳遞虛假或誤導資訊，例如假投資建議、假分享或言論等，誤導受害人的決策行為，甚至製造社會矛盾。

信任和信譽危機

深度偽造內容可能在網路上造成不信任的氛圍。由於深度偽造很難辨別，如果網絡上大量充斥著這類影片，真實的資訊亦會被影響波及。因為人們不能輕易地分清所接收的資訊是否混合了深度偽造的內容，最終變成不信任任何資訊，以防受騙。

另外，深度偽造內容會取代以往「移花接木」式的偽造影片，例如制作不雅、粗俗或暴力影片，令人誤以為受害人參與某些活動，即使觀眾半信半疑，亦會令受害人聲譽受損。

如何辨識深度偽造？

辨認深度偽造技術相當困難。雖然現在有些在線工具聲稱能夠檢測視訊中是否使用了深度偽造技術，但實際上，辨認真偽的關鍵仍然在於公眾的安全意識。尤其是在即時視訊場景中，如視訊通話或線上會議，我們需要時刻保持警惕。

如果你收到可疑的視訊通話，你可以採取以下措施：

干擾深度僞造軟體的辨識功能

1. **請對方慢慢用手遮住臉部。**這樣可能會使對方的原本樣貌顯現出來，因為深度偽造軟體可能無法辨識遮住的人臉。

2. **請對方移動攝影機，拍攝到另一個人。**在這種情況下，深度偽造軟體可能會認錯要換臉的對象，導致二人的臉瞬間改變，被來回替換。

觀察對方的臉部細節異常之處

3. **觀察對方的臉部細節，**以辨識其在頭部移動時是否有任何異常。
4. **觀察皮膚顏色，**臉部顏色可能與其他部位的膚色（例如脖子，肩膀等）有所不同。
5. **觀察皮膚紋理，**檢查是否看起來過於光滑或有過多的皺紋。
6. **觀察面部特徵，**檢查是否有任何不自然的特徵。**例如：**

    - 鬍鬚和髮型看起來是否真實；
    - 對方的眼睛看起來是否自然；
    - 面部表情是否過於僵硬；
    - 說話時是否有顯露不合理的表情，如輕鬆的內容卻表情嚴肅。

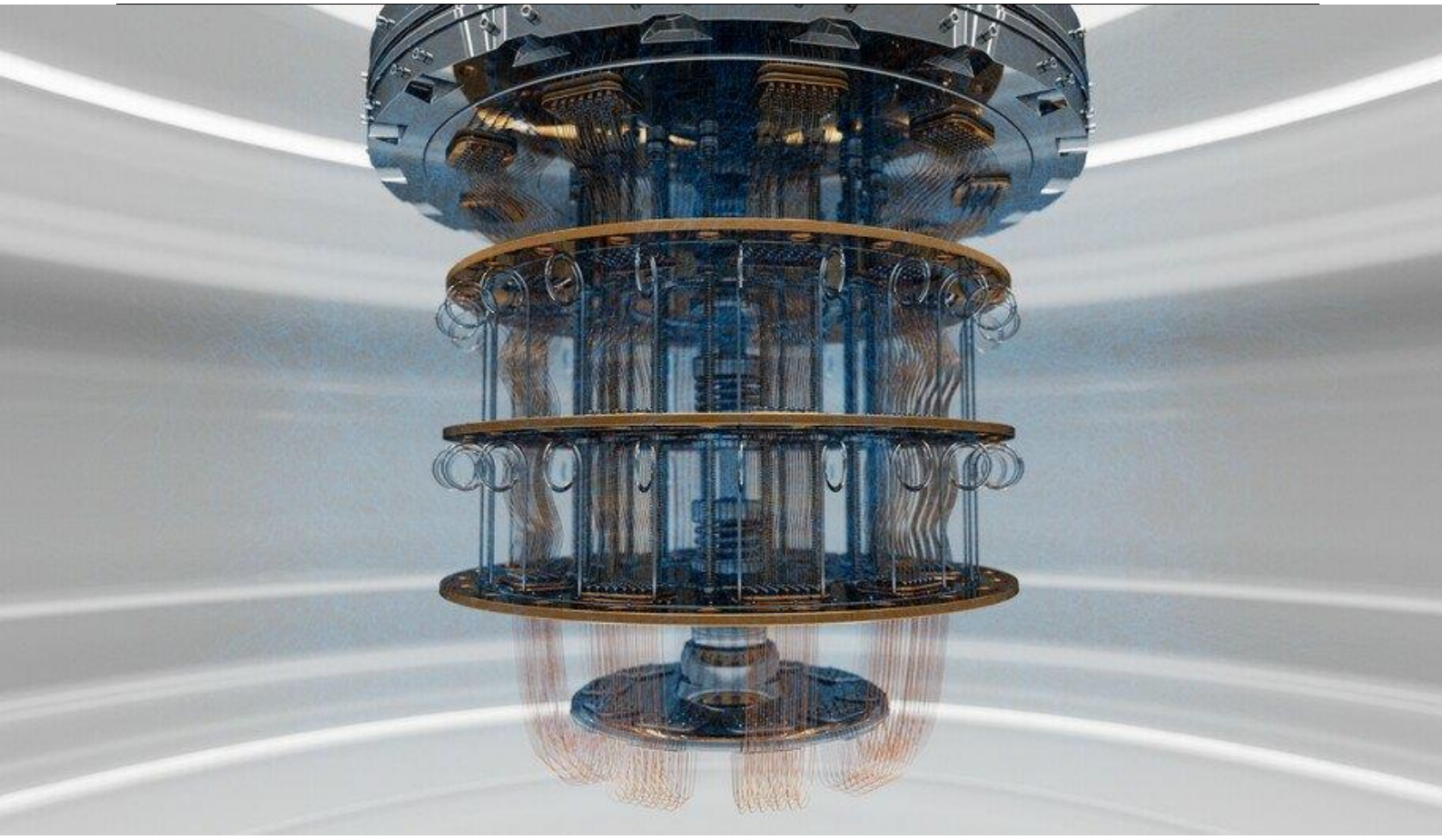
7. **觀察頭部以下的身體或背景事物**是否一直固定不動。

試探對方反應或回應

8. 詢問只有你和對方才知道的事實，以驗證對方身份。

詳細資料可參閱HKCERT保安博錄
https://www.hkcert.org/tc/blog/deepfake-where-images-don-t-always-speak-truth

如何在量子時代保護你的數據



量子電腦代表著計算領域的一個重大突破，它引用量子力學的複雜原理，令執行某些特定工作的計算速度甚至比傳統電腦快千百倍。

傳統電腦的運行依賴傳統位元(bit)的二進制單位，以 0 或 1 來儲存數據；而量子電腦的運行前提則完全不同：量子電腦使用量子位元（qubit），量子位元具有以疊加態(Superposition)存在的獨特特性，可同時表示 0 和 1。此外，量子位元亦具有量子糾纏(Quantum entanglement)的特性，其狀態可以與另一個量子位元的狀態相互關聯。

量子演算法就是利用這些特性來執行複雜的計算，在執行特定任務時（如量子世界模擬、演算法加速和人工智慧），效率比傳統電腦有指數級的提升。

除量子演算法外，其實量子電腦亦可執行傳統電腦演算法，但由於量子電腦需要特殊的運行設備和環境，以及可行的量子糾錯方案， 所以在處理日常任務（如文字編輯或電子表格管理 ）方面，傳統電腦會更有效率且成本更合理。因此，人們普遍認為量子電腦不會取代傳統電腦，而是與傳統電腦協同處理不同領域的任務。

量子演算法：對加密技術的潛在威脅

在現今的網絡傳輸和資料儲存中，加密是保護資料的主要方法之一，能夠確保敏感資料的保密性和隱私性。現代加密方法大致有兩種：對稱式與非對稱式加密。前者所謂的「對稱」，指發件人和收件人共同擁有一條由隨機亂數生成的密碼匙，既可用於加密，也可用於解密資料。因對稱式加密的效率較高，所以很多數據傳輸和資料儲存的加密方式都是採用對稱式加密技術。

「非對稱式加密」則需要使用不同的密碼匙進行加密和解密，公開密碼匙用於加密，對應的私人密碼匙用於解密。密碼匙生成時會選擇兩個隨機質數將它們相乘以生成一個整數，這個整數就成為了計算公開密碼匙和私人密碼匙的一部分。對於黑客而言，要破解密碼匙就需要找到整數的質因數，即進行質數因式分解(Prime Factorisation，例如整數3233，要透過演算分解得出質數61和53)。但是這個過程需要花費黑客大量的時間，儘管對於小的數字，質因數分解可能相對容易，但對於大的數字，目前沒有已知的快速算法可以有效地解決這個問題。例如，要從一個1000位的數字找出是哪兩個質數組合，可能便需要反覆嘗試數十億次，這需要大量的計算時間和資源，使得破解密碼匙變得非常困難。

因此，質數因式分解在非對稱加密算法中扮演了關鍵角色，它的複雜性和困難性保證了對非對稱加密的安全性，使得黑客無法輕易破解加密訊息。

破解技術發展

在量子計算的崛起背景下，由洛夫·格羅弗（Lov Kumar Grover）提出的「格羅弗算法（Grover’s algorithm）」對對稱式加密構成了一定程度的威脅，但其只能將破解對稱密碼匙的時間縮短至一定程度，影響較小。

相比之下，對於非對稱式加密，彼得·肖爾（Peter Shor）提出的「肖爾算法（Shor’s algorithm）」卻可能顛覆現今的加密技術。該演算法利用了量子的疊加和量子糾纏特性，將質數因式分解的計算時間大幅縮短。例如，如果我們使用一個2048位元的RSA密碼匙，這可能需要傳統計算機耗300億年的時間來破解。但如果使用量子計算機和肖爾算法，理論上黑客僅需8個鐘便可以破解該密碼匙(使用一部有二千萬量子位元的量子電腦)。這一突破展示了現代加密技術在量子電腦的挑戰面前的脆弱性。

儘管目前的量子技術尚未能夠實現肖爾算法來突破非對稱式加密，但隨著科技的進步及新因式分解法的發明，迅速突破任何現有的加密方法並非不可能，人們甚至將量子電腦能夠真正應用於破解非對稱式加密技術的未來那一日命名為Q-Day。

另外，許多人也在擔心，犯罪分子可能會收集現有的加密資料，一旦量子電腦變得足夠強大時

便破解密碼，讀取資料，這將會對資料安全構成嚴重威脅。

目前的量子電腦對資料加密威脅相對較低

目前，量子電腦的發展對當前的資料加密應用構成直接威脅的機會較低，原因如下:

- 首先，能夠破解加密演算法的大型量子電腦仍處於實驗階段，其製造仍然相當困難。
- 其次，目前爲止，用肖爾演算法來破解一般所建議的非對稱式加密法RSA-2048(需要對一個有617個數字的整數進行質數因式分解)從未得到實證，因它需要超乎現今科技的能力。
- 此外，對稱式加密與非對稱式的演算法安全程度都取決於密碼匙的長度，即密碼匙越長，需要的破解時間更長，所以只要密碼匙有足夠長度，現今並未發展出相應的量子演算法能於短時間內破解它們。
- 另外，建立和維護穩定的糾錯量子電腦是一項艱鉅的技術挑戰。
- 再者，即使實現了這樣的量子電腦，也需要大量的資源和基礎設施來運作。

後量子加密演算法及其挑戰

儘管目前的量子計算發展還不能直接威脅到現代加密技術，但人們仍然擔心，當實用量子電腦出現時，現有的加密資料是否會受到影響。為了解決這個問題，電腦科學家和密碼學家正在積極研究後量子加密演算法，研究方向包括格密碼學(Lattice-based cryptography)和散列密碼學(Hash-based Cryptography)等，旨在開發出即使是量子電腦也需要大量時間才能解決的覆雜數學問題，以此來保護數據免受量子電腦的影響。

美國國家標準與技術研究院（NIST）於2022年便從眾多的後量子加密演算法中，揀選了四種被認為可抵禦量子電腦攻擊的演算法，分別是用於資料加密的CRYSTALS-Kyber、用於數字簽名的CRYSTALS-Dilithium、SPHINCS+和FALCON。

市場上已有企業開發及應用這些演算法來保護資料，例子包括即時通訊軟件Signal 的 "PQXDH 協議(建基於CRYSTALS-Kyber演算法)"和谷歌推出的 "FIDO2 安全密碼匙"(建基於CRYSTALS-Dilithium演算法)。NIST仍在進行著相關後量子加密演算法的測試和揀選，未來可能還會有更多不同的演算法推出。

然而，即使是後量子加密方法也可能面臨挑戰。近期，CRYSTALS-Kyber公開密碼匙已被發現有漏洞。 研究團隊利用人工智能對使用這種加密方法的設備時序和功耗等信息進行了深度學習分析，成功破解了這一漏洞。這也凸顯了後量子加密演算法的不斷發展和持續研究對保護

資料免受量子威脅的重要性。因此，鑒於許多後量子演算法仍處於早期開發階段，用戶可採用混合加密技術來保護資料，即同時使用傳統加密方法和後量子加密方法，而不是完全依賴後量子加密，以確保資料得到全面保護。

結論

綜上所述，量子電腦開啟了計算領域的新篇章 。雖然量子電腦在特定任務中有出色表現，但也對傳統數據加密技術提出了挑戰。儘管目前存在技術限制，但後量子加密方法的積極發展為未來數據安全提供了新的可能 。然而，這些方法也存在不足之處，想要在不斷演變的量子威脅面前保持領先，持續的研究和適應性至關重要。混合加密技術為保護數據安全提供了一種有效的途徑，它結合了傳統加密技術和後量子加密技術以應對這一複雜局面。

在未來的數字化時代，隨著量子技術的發展，保護個人和組織的數據安全將變得更加重要。為了應對量子威脅，HKCERT建議大家關注後量子加密演算法的發展，採用混合加密技術以確保數據安全。此外，加強對資料安全的重視也是必不可少的，例如資料分類、存取控制、密碼匙管理、資料分隔儲存和備份、外洩防護等。只有不斷提高警覺，才能保護資料安全，共築安全的未來網絡環境。

詳細資料可參閱HKCERT保安博錄
https://www.hkcert.org/tc/blog/how-to-protect-your-data-in-quantum-age

完

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