## 議員：助部門機構認識黑客工具 及早修補漏洞

# 為期三日攻防演練 提升網安防護水平

**隨着人工智能等科技應用加速發展，以及各種新興網絡威脅不斷演變，網絡安全風險令人關注。政府、社會各界都需要持續透過網絡安全防禦策略，強化網絡安全應對韌性。數字政策辦公室日前舉辦了「香港網絡安全攻防演練——以攻築防2026」，逾70個政府部門、香港和內地機構、本地大專院校組成防守隊與攻擊隊，進行為期三日兩夜、歷時60小時的網絡安全攻防實戰，測試參與部門及機構的防禦部署及應變能力，提升香港整體網絡安全防護及韌性。**

**有立法會議員表示，隨着技術迭代及AI催生新型黑客工具，網絡威脅持續演變，政府需持續透過高還原度實戰測試，加密漏洞檢測與修補，吸納更多政府部門及私營企業參與，提升整體網絡安全防禦實力。**

大公報記者 易曉彤




▲「香港網絡安全攻防演練」於前晚圓滿結束。圖為由香港和內地網絡安全專業機構和專上學院人員組成的攻擊隊。 政府新聞處

第三屆「香港網絡安全攻防演練」由10月29日展開，演練規模進一步擴大，參與的防守方（藍隊）共有51隊，涵蓋28個政府部門，23間公共機構及首次加入的私營企業的指定資訊系統。肩負攻擊任務的23隊攻擊隊（紅隊），包括來自15間香港和內地網絡安全專業機構和4間本地大專院校的代表，由廣東省互聯網信息辦公室推薦的3支攻擊隊，以及由數字辦派出的1支攻擊隊，充分體現粵港兩地在網絡安全的交流合作，以及攜手推動網絡安全人才培育的共同努力。

### 模擬眞實網絡威脅場景找漏洞

演練透過「實兵」、「實網」、「實戰」方式，模擬真實網絡威脅場景，以找出系統的漏洞。數字辦昨日回覆《大公報》查詢表示，在網絡安全攻防演練期間，紅隊透過一個經過嚴格審查的可控虛擬演練平台，向藍隊已投入運作的指定資訊系統發動模擬網絡攻擊。紅隊可以在點到即止、不影響公共服務及不影響系統資料的前提下，以多樣化的手段進行攻擊，以期找出指定資訊系統的安全漏洞。而藍隊則會在其慣常的工作地點，監測真實網絡情況，應對攻擊並作出適當的防衛，從而達到以攻築防的目標。同時，評審員通過平台的審計及存取控制功能，防止不合規的攻擊，以保障參與資訊系統所提供的服務不受影響。

### 報告將供參與機構跟進

演練在前晚（10月31日）結束。數字辦表示，所有參與的系統和服務一直運作正常，演練的報告將會提供予參與的相關政府部門、公共機構及私營企業作參考和跟進。來自逾80家不同機構的超過280人員以觀察員身份到場，了解攻防演練的過程，交流實戰經驗，並為日後參與演練作準備。

政府重視抵禦網絡安全挑戰的能力建設，今年施政報告提出，政府會推出「網絡安全防禦計劃」，為本地機構提供網絡安全認證，並發展共享防禦工具及建立威脅情報共享機制，鞏固社會數碼安全韌性。此外，政府會建立網絡安全威脅情報分析與警報系統，落實《保護關鍵基礎設施（電腦系統）條例》規定，並運用AI技術收集國際網絡威脅情報，分析針對本地關鍵基礎設施的威脅並作出風險預警，提示設施營運者。

立法會科技創新界議員邱達根向《大公報》表示，演練內容包括邀請網絡安全公司嘗試模擬入侵政府網站及相關資料庫，藉此檢視各部門及機構的防禦水平。他說，這類實戰演練可幫助各政府部門和機構，提升網絡安全的防禦和應對能力，同時可認識黑客常用攻擊工具，及早發現系統漏洞並及時修補，填補安全缺口。

邱達根表示，隨着技術持續迭代，加上人工智能衍生大量新型黑客工具，網絡威脅不斷演變。政府不能單純信賴第三方科技供應商，政府必須自行做評測和認證。面對層出不窮的攻擊手段，實際場景的漏洞檢測與修補工作，必須增加覆蓋範圍及測試頻率，方能有效抵禦外部的網絡襲擊，提升各界網絡安全意識。他期望今次攻防演練模式可進一步推廣，納入更多政府部門，同時吸引更多私營企業參與，持續提升政府網絡安全意識與整體防禦實力。

## 網安協調中心倡企業推AI治理減風險

**防患未然**

隨着人工智能技術迅速普及，網絡攻擊變得更具自動化、針對性和破壞力，威脅企業營運及資訊安全。2025年本港錄得15877宗網安事故，按年上升27%，創下歷年新高。香港網絡安全事故協調中心表示，五大網絡安全風險料於2026年對企業構成重大挑戰，當中包括黑客開始利用AI進行更高階的攻擊、企業AI規管薄弱加劇資料外洩影響等。中心建議企業要推行AI治理及規範，以降低技術應用帶來的營運風險。

### 提升員工網安意識

香港網絡安全事故協調中心早前預測，今年有五大網絡安全風險浮現，主要分為AI應用及供應鏈風險兩大類。在AI應用方面，具備自主學習與執行能力的代理式AI，能夠在無需人手介入的情況下自行判斷並採取實際行動，一旦被黑客入侵，將自動執行潛在惡意指令，令攻擊更難預測與防範。此外，在缺乏內部AI管治框架的情況下，企業敏感資料可能因員工誤用公共AI平台而外洩。

在供應鏈方面，企業在業務過程中，愈來愈依賴外判服務及第三方平台處理業務流程，當這些合作夥伴遭受網絡攻擊或安全系統有漏洞時，亦會嚴重影響企業的網絡安全。過度依賴單一雲端供應商而缺乏備援方案，將令企業在遇上平台故障或供應商中斷服務時無法運作。此外，隨着智能設備（如語音助理、辦公或客服機械人等）廣泛應用於營運環節，這些具AI功能的設備開始暴露出潛在的安全風險。

中心建議，企業應指派具備基本網安知識的員工，負責日常監察與應變工作，確保能及時應對突發情況。企業應制定AI相關政策與操作指引，清楚列明可使用的工具、資料輸入範圍，降低技術應用帶來的營運風險。同時提升全體員工網安意識和落實關鍵的網絡安全技術。

大公報記者 易曉彤

責任編輯：鄭小萍 美術編輯：何振紹


# 訃告

香港著名愛國教育家與社會活動家、第四屆至第十屆全國人民代表大會代表、香港特別行政區籌備委員會委員、全國人大常委會香港基本法委員會委員、香港教育工作者聯會創會會長、培僑教育機構榮譽主席吳康民大紫荊勳賢，於二〇二六年十月十八日上午辭世，享壽一百歲。

謹訂於十一月四日（星期三）下午五時在香港殯儀館一樓設靈，晚上七時舉行追思會；翌日十一月五日（星期四）上午十時舉行公祭大殮儀式。

謹此訃告

吳康民先生治喪委員會 啟

二〇二六年十月二十日

聯絡處：香港北角天后廟道190號培僑中學
電話：852-2566 2317 傳眞：852-2887 8737
電郵：spevent@pkms.edu.hk

## 吳康民先生治喪委員會

主　任：梁振英　曾蔭權　林鄭月娥
副 主 任：陳國基　孫尚武　李慧琼　葉劉淑儀　范徐麗泰　譚耀宗　蔡若蓮　孫玉菡　麥美娟　曾鈺成　馬逢國　袁　武　譚惠珠　楊耀忠
委　員：（按繁體字姓氏筆劃排序）
伍煥杰　吳育智　吳佳錡　李子建　李詠怡　李潔儀　李耀熙　汪明荃　周世耀　周志榮　周俊恒　周娟娟　周熾昌　林友浮　邱沿益　胡定旭　馬有禮　高佩璇　張華峰　張澤松　梁劉柔芬　莊金耀　許學之　陳克勤　陳　勁　陳　勇　陳　恒　陳鑑林　陸勁光　傅金珠　程介明　費　斐　黃金平　黃瑞英　黃錦良　楊金溪　葉淑娟　詹洪良　劉智鵬　蔣曉冰　鄧　飛　盧富球　顏婉明

# 聞

鼎惠懇辭
如蒙賜賻
撥充吳康民
教育基金

先嚴

# 吳康民

痛於公曆二零二六年十月十八日（農曆九月九日）壽終
享年一百歲遺體奉移香港殯儀館治喪謹擇公曆十一月
四日（星期三）下午五時於該館一樓設靈晚上七時舉行追思會翌日十一月
五日（星期四）上午十時舉行公祭大殮 十一時辭靈隨即出殯 哀此訃

妻　黃穗良
孝男　小鋼　媳　黃慧嫻
孝男　小欣　媳　何巧平
孝女　小惠　婿　黃永波
孫　男　海　榆
孫　女　海　盈　婿　顏天立
外孫男　黃岸平
曾孫男　顏浩洋
曾孫女　顏逸晴

胞兄　逸民　嫂　楊知英
胞兄　健民　嫂　方　藍
胞弟　新民　弟媳　林頌美
胞弟　穎民　弟媳　付肖萍
胞弟　衛民　弟媳　吳麗萍
胞妹　映珠　妹夫　鐘若瓊
胞妹　映瑛　妹夫　徐　奕

親屬繁衍　恕未盡錄

聯絡處：香港北角天后廟道一九零號培僑中學
電　話：二一五六六二三一七

泣告