

2025年10月13日

討論文件

## 立法會資訊科技及廣播事務委員會

### 有關維護資訊保安的工作

#### 目的

本文件向委員匯報本港資訊保安的最新情況和政府  
在維護資訊保安方面的工作。

#### 資訊及網絡安全的形勢

2. 在過去一年（2024年9月—2025年8月），香港生產力促進局（生產力局）成立及營運的香港網絡安全事故協調中心（事故協調中心）共處理15 722宗資訊保安事故，當中主要涉及仿冒詐騙（8 973宗）、殭屍網絡（3 337宗）和惡意軟件（1 403宗）。與去年同期相比，惡意軟件的宗數上升幅度較高。有關資訊保安事故的分項數字載於附件一。

3. 就政府資訊保安事故，在現行的應變機制下，各政府部門在發生資訊保安事故時必須向數字政策辦公室（數字辦）通報。在2025年，數字辦首八個月共接獲8宗資訊保安事故報告，較去年同期的14宗為低，當中涉及網站遭塗改、遺失存有保密資料的流動裝置或抽取式媒體等。

4. 此外，香港警務處（警務處）在2024年共錄得33 903宗科技罪案，較2023年的數字輕微下跌，累計損失金額51.3億港元，較2023年回落6.7%。當中，入侵系統活動的案件有61宗，相關宗數及損失金額的增幅均較大。在2025年，警方首七個月共錄得19 080宗科技罪案，較去年同期微跌，相關累計損失金額則有所上升至約36.4億港元。有關科技罪案的分項數字載於附件二。

5. 在個人資料方面，香港個人資料私隱專員公署（私隱專員公署）在2025年首八個月共接獲151宗個人資料外洩事故通報，較2024年同期的140宗增加近一成。其中，涉及黑客入侵的個人資料外洩事故為55宗，與2024年的數字相若。

## 維護政府層面的資訊保安工作

6. 資訊及網絡安全是數字政府的基石。政府一直致力透過多管齊下的方式，加強決策局／部門（局／部門）的資訊及網絡安全，包括於2024年8月推出多項優化資訊系統管治和保安的措施，以及於2025年4月推出修訂的《資訊科技保安政策及指引》。現時，所有局／部門已委派高級首長級人員和相關公營機構的主管或副主管負責資訊保安工作及其轄下重要資訊系統的項目管理，確保局／部門以及公營機構遵守資訊保安相關要求。相關措施的實施情況如下：

### (I) 提升資訊系統的安全和穩健性

- 額外壓力及網絡安全測試：各局／部門及其轄下公營機構已按照要求，在推出有重大公眾影響的資訊系統前，安排由獨立第三方進行額外壓力測試及網絡安全測試。數字辦亦已要求局／部門須在大型及高風險資訊系統投入運作前把系統交由數字辦安排的獨立第三方進行額外壓力測試及網絡安全測試，以協助局／部門評估系統應對異常或極端負載和壓力情況，以及提升網絡攻擊風險的恢復能力。截至今年8月，數字辦、各局／部門及其轄下公營機構合共為超過80個指定項目安排上述額外測試。
- 恆常監察及自我評估：根據數字辦的要求，各局／部門及其轄下公營機構已就其資訊系統建立恆常的監察機制及進行自我評估，例如在系統如常運作階段進行保安風險評估及審計、私隱影響評估、定期系統檢查及滲透測試。數字辦已為此向局／部門提供適切的技術意見、指引及良好作業模式等。

- 系統健康檢查：數字辦自去年12月起增設中央網絡安全健康檢查平台，定期及持續地為政府面向公眾的資訊系統及網站進行健康檢查，以加強識別各局／部門的系統潛在安全漏洞，從而加強防範資訊及網絡保安事故。
- 遵行審計：數字辦於去年9月展開新一輪的全政府資訊保安遵行審計。截至2025年8月，數字辦已為所有局／部門完成審計工作。另外，數字辦自2025年起以風險為本的方式，每年選定不少於8個重要政府資訊系統進行深入的資訊保安遵行審計，以確保局／部門遵從政府資訊保安規定。就今年選定的9個系統，當中5個的技術性審查及評估工作已大致完成，其餘的系統審計工作仍在進行中，預計會在年底前完成。
- 網絡安全攻防演練：數字辦由2024年起每年統籌主辦網絡安全攻防演練。第二屆演練於2025年10月舉行。基於去年首次演練的成功經驗，今年的演練規模已擴大至25個政府部門和9間公共機構參與作為防守隊，以及包括網絡安全企業和專上學院的14支攻擊隊，藉以提升演練成效。此次演練亦邀請了內地經驗豐富的團隊參加攻擊隊，促進兩地技術交流。

## **(II) 強化員工培訓及支援**

- 員工培訓：數字辦與公務員學院緊密合作，通過定期舉辦「創新與科技」領導系列專題講座，加強所有局／部門的高層管理人員運用數字科技的核心技能，內容涵蓋資訊系統的項目管治、網絡安全和人工智能（AI）等相關課題。自2024年11月舉辦首場專題講座起，共有約260名來自多個決策局及部門的高級首長級人員出席。此外，在2024-25年度，數字辦亦為政府員工安排了超過100個與核心數字技能相關的培訓課程，超過9 700人次參與。數字辦會持續舉辦不同類型的培訓，加深政府員工對資訊及網絡安全的認知和準備。

- 進修課程：數字辦委託了職業訓練局（職訓局）轄下的香港資訊科技學院設計及籌辦「公營機構網絡安全證書」課程，旨在全面提升政府員工的資訊保安技能。課程涵蓋基礎、中級及高級三個級別。截至2025年8月，分別共有584名及173名政府員工完成基礎及中級課程。
- 防詐騙演習：數字辦於2025年開展新一輪「全政府防範仿冒詐騙演習運動」，當中運用AI等新技術來模擬實際的仿冒詐騙電子郵件，從而加深政府人員對仿冒詐騙的認知和辨識能力。

### (III) 加強與業界協作

- 網絡安全業界協作：為應對近期頻繁的網絡安全威脅，數字辦於2025年7月聯同「互聯網基建聯絡小組」<sup>1</sup>及網絡安全業界召開會議，商討強化技術防護措施及風險管理策略。因應多項於下半年舉行的大型活動，包括第十五屆全國運動會及第八屆立法會換屆選舉，數字辦加強實時威脅監測、情報互通及攻防演練，確保相關關鍵資訊系統的穩健運作及周密部署。

## 推動社會層面的資訊保安工作

7. 安全穩妥的網絡環境是數字經濟及智慧城市發展的先決條件。政府一直致力與香港互聯網註冊有限公司（互聯網註冊公司）及事故協調中心等持分者緊密合作，推行不同計劃及支援，以提升公眾對資訊保安的認知及支援業界應對網絡安全風險。相關措施如下：

### (I) 提升企業應對網絡攻擊的能力

- 免費網站檢驗服務及漏洞測試：在數字辦的支持下，互聯網註冊公司於2025年3月推出免費的整合式安全

---

<sup>1</sup> 由數字辦副數字政策專員（數字基建）擔任主席，成員包括來自數字辦、事故協調中心、香港互聯網交換中心、互聯網註冊管理有限公司、香港互聯網供應商協會、香港警務處，以及通訊事務管理局辦公室的代表。

服務「網絡防禦一站通」，協助本地中小企、非政府機構及中小學查找網站漏洞，進行風險評估，並提供解決方案，包括推薦免費資源，賦能其提升網絡防護水平。

同時，互聯網註冊公司會繼續推行「網健通」網站安全免費檢查服務，主動提示「.hk／.香港」用戶潛在的網絡風險，並為「.hk／.香港」用戶提供免費且詳盡的網站安全掃描服務及電話諮詢，協助他們及早防範。截至今年8月，互聯網註冊公司已向「.hk／.香港」用戶提供了約52 000次檢查服務。

此外，警務處、私隱專員公署和網絡安全業界於今年6月至8月協辦第三屆「狩網運動」，運用AI技術為資源有限的本地中小企免費偵測系統漏洞，並對其AI應用程式進行安全審查。參與企業會獲得詳細的網絡安全報告及一對一專業諮詢服務，以對症下藥，全面提升安全防護水平。

2025年《施政報告》亦宣布優化數碼港「數碼轉型支援先導計劃」，以配對資助賦能中小企應用AI及網絡安全方案，提升競爭力及資訊保安。

- 網絡安全資訊共享：為促進網絡安全服務供應商與本地企業及機構之間的聯繫，數字辦聯同事故協調中心於今年7月推出「網絡安全服務供應商聯動計劃」。計劃的專屬平台上會展示經分類及審核的網絡安全解決方案，協助服務供應商接觸更多潛在企業客戶，同時為企業提供可信賴的網安解決方案。
- 免費線上員工培訓：為提高各行各業企業及其員工的網絡安全意識和知識，互聯網註冊公司推出「網絡安全員工培訓平台」，為各行各業的員工提供免費線上網絡安全培訓。截至今年8月，已有超過372 000人次透過此平台提升了相關知識和技能。
- 網絡安全嘉許計劃：為鼓勵企業積極提高員工的網絡安全意識，互聯網註冊公司與國際信息系統審計協會中國香港分會每年合辦「共建員工防火牆」嘉許計

劃，以表彰過去一年成功提高員工網絡安全意識和風險認知的企業。在2024-25年度，該計劃吸引了超過80間來自銀行、物業管理、零售等行業的中小企及大型企業參與。

## (II) 加強公眾教育

- 推廣網絡安全：數字辦每年響應「國家網絡安全宣傳周」，聯同業界策劃多元化的推廣活動，提升公眾對網絡安全的意識及關注。數字辦今年以「數碼賦能 網安同行」為主題，推出一系列活動，包括舉辦香港分論壇、香港網絡保安高峰會技術研討會，以及即時通訊軟件貼圖設計比賽及宣傳活動。此外，數字辦持續更新及優化「資訊安全網」和「網絡安全資訊站」專題網站，包括新增教學視頻及最新資訊，協助公眾掌握當前網絡安全趨勢，並學習有效防範網絡攻擊的實用技巧。
- 保障個人資料：私隱專員公署一直積極推動加強市民保障個人資料，一方面透過不同渠道向市民加強宣傳教育，提升市民保障個人資料的意識，同時積極和業界進行溝通協作，例如出版與個人資料保安有關的指引資料、單張及懶人包，包括一系列有關AI的刊物（例如：僱員使用生成式AI的指引清單、有關AI的個人資料保障模範框架及單張、使用AI聊天機械人的「自保」單張）、雲端運算指引、如何精明使用社交媒體及智能電話的單張、資訊及通訊科技的保安措施指引及單張等，協助業界遵從《個人資料（私隱）條例》的相關規定。
- 建立防騙屏障：警方持續透過多元化渠道加強防騙宣傳，針對網購詐騙，尤其演唱會門票騙案急增的趨勢，在「守網者」網站、Facebook專頁及電視節目等平台發布警示資訊，並舉行大型記者會，現場揭露網購門票詐騙手法及提供防範對策。警方更首次主動聯絡演唱會主辦機構，協調通過官方渠道發布防騙警示，呼籲市民交易前使用「防騙視伏器」核證賣家可信度。

此外，警方推出的「防騙視伏器」及相關手機應用程式，截至2025年9月1日，預警超過120萬次詐騙及網絡安全風險。「防騙視伏APP」更加入警示功能及增設公眾舉報平台，並推出「可疑帳號警示機制」，提醒市民提防騙案。機制已於2024年12月全面覆蓋轉數快、網上銀行、櫃位轉帳及自動櫃員機交易，為市民提供更好保障。

### (III) 推動跨地域合作

- 恆常聯繫及交流：香港政府電腦保安事故協調中心積極參與國際合作，透過加入國際性的電腦緊急事故應變小組統籌中心、全球保安事故協調中心組織及亞太區電腦保安事故協調組織，與各地的電腦緊急事故應變小組保持緊密聯繫，並定期參與如亞太區電腦保安事故協調組織演習等技術交流活動。
- 大型論壇：政府參與由國家互聯網信息辦公室舉辦的年度「世界互聯網大會烏鎮峰會」，並出席不同論壇進行主題演講，分享交流香港創科及網絡安全的最新發展。2025年4月，由世界互聯網大會主辦、特區政府承辦及創新科技及工業局協辦的「世界互聯網大會亞太峰會」首次在港舉辦，除交流會及論壇外，大會還舉辦一系列配套活動，包括網絡安全應急能力高級研修班等。

此外，數字辦於去年 12 月聯同互聯網註冊公司舉辦「網絡安全技術論壇 2024」，匯聚本地與內地的頂尖網絡安全專家，共同探索如何提升本港整體應對網絡攻擊的防禦及復原能力，是次論壇錄得總出席人次近 1 000 名。今年 5 月，數字辦及警務處亦合辦了「網絡安全多元創新論壇 2025」，逾 600 名本地與內地不同界別的專業人士共聚一堂探討當前網絡安全挑戰、行業協作及創新應對策略等議題。

- 合作備忘錄：2024年9月，數字辦與廣東省互聯網信息辦公室（廣東網信辦）及澳門特區網絡安全委員會簽訂《關於促進粵港澳網絡安全領域交流合作備忘

錄》，加強粵港澳三地在技術交流、資訊共享及緊急應對方面的合作。今年5月，數字辦亦派員前往深圳，與廣東網信辦及澳門特區進行粵港澳網絡安全聯席會議，推進合作備忘錄協作內容，分享最新網絡安全工作情況及共同討論2025年粵港澳網絡安全重點合作事項的協作。

#### (IV) 制定法規指引

- 關鍵基礎設施電腦系統安全：立法會於2025年3月19日通過《保障關鍵基礎設施（電腦系統）條例》（條例）。條例向被指定的「關鍵基礎設施營運者」（營運者）施加法定責任，以確保營運者採取適當措施保護其電腦系統，從而減低因網絡攻擊導致必要服務被干擾或破壞的可能，提升香港整體的電腦系統安全。條例將在2026年1月1日正式生效，隸屬保安局的專員辦公室亦將於同日正式成立以實施條例。
- 數據中心基建安全：數字辦經參考最新的國家及國際數據中心保安全管理標準及作業模式、政府內部指引，以及建設和營運政府數據中心大樓所獲得的經驗等，於2024年12月發布《數據中心保安實務指引》，供業界就數據中心安全的管理、設計原則、技術、運營和維護作參考，以提升本港數據中心基建的安全。

### 人力資源發展

#### (I) 培育本地人才

##### 中小學階段

8. 政府高度重視在基礎教育培養學生的數字素養與技能。教育局編訂《香港學生資訊素養》學習架構，支援學校培育學生在學習及日常生活中，有效及符合道德地運用資訊及通訊科技的能力和態度，包括教導學生有關資訊及網絡安全和保護個人資料私隱的重要性。教育局亦與相關機構包括香港新聞教育基金及警務處協作，推出媒體和資訊素養學與



教教材套和一系列影片，以及舉辦教師專業發展課程，支援教師於課堂內外加強培育學生媒體和資訊素養。與此同時，配合中小學數字教育（包括AI教育）的推展，教育局將訂定「AI素養」學習架構，進一步提升學生的資訊素養。

9. 常規課程以外，數字辦推行「中學IT創新實驗室」及「奇趣IT識多啲」計劃，分別為中學和小學提供資助，以開展與資訊科技相關的課外活動，包括網絡安全相關的比賽、工作坊及課程等。截至今年8月，已有超過1 000間學校在上述兩項計劃下舉辦約7 300個活動，當中包括網絡安全相關的課外活動，例如網絡安全入門課程及技術工作坊等。此外，數字辦亦推行學校探訪計劃，向學生、教師及家長傳遞資訊保安訊息。在2024/25學年（截至今年6月），數字辦已為21間學校，超過5 100師生舉辦網絡安全講座，提高他們對網絡安全的認識。

### 專上院校課程

10. 專上教育方面，各院校近年均積極推展創科教育，包括增加資訊及網絡安全相關課程及學額。為了滿足本港的社會和經濟需要，教育局推行的「指定專業/界別課程資助計劃」（SSSDP）提供資助，鼓勵自資專上教育界別開辦電腦科學（包括網絡安全）等十個範疇的課程。在2025/26學年，SSSDP涵蓋電腦科學範疇共六個學士學位及兩個副學位課程，涉及共435個資助學額，比2024/25學年增加近一成。

11. 此外，職訓局在政府支持下已於2023年11月成立香港資訊科技學院，專注提供資訊科技及其他相關科技課程，鞏固香港資訊科技能力及回應業界的人力需要。學院於2024/25學年錄取首屆學生，並開辦一共21個課程，包括11個全日制高級文憑課程、2個全日制基礎課程文憑課程及8個兼讀制高級文憑課程。上述課程涵蓋網絡安全、AI、雲端系統及數據中心管理等範疇。其中，13個全日制高級文憑及基礎課程文憑課程共錄取新生2 111人。學院將會繼續根據市場需求和技術發展趨勢，研究持續拓展及更新課程，以全方位培育各類資訊科技專才。

## 再培訓、持續進修及在職訓練

12. 本地勞動人口培訓方面，僱員再培訓局目前為合資格僱員提供超過700項恆常培訓課程，這些課程涵蓋28個行業及多項通用技能，其中包括網絡安全及網絡管理等範疇的課程。年滿18歲或以上的香港居民亦可利用持續進修基金，報讀與電腦科學及資訊科技相關課程。

13. 為響應政府擴大本地資訊保安人才庫的方針，並促進香港與內地在資訊安全領域的人才交流與合作，中國信息安全測評中心已於2024年年底授權香港專業進修學校及與職訓局轄下的香港資訊科技學院合作提供註冊信息安全專業人員（CISP）培訓課程，讓香港專業人士能直接在本地取得國家認可的網絡安全專業資格，提升本地資訊安全從業員的專業技能和競爭力。

14. 數字辦、互聯網註冊公司及警務處於2025年7月繼續合辦「網絡攻防精英培訓暨攻防大賽」，活動獲學界及業界廣泛支持和積極參與。除了透過一系列免費的培訓和比賽，為學界和業界的精英提供實踐與交流的平台，亦以模擬實戰提升他們的網絡事故應變能力，培養新一代的網絡攻防專家。

15. 此外，數字辦、生產力局及網安事故協調中心於2025年1月合辦年度「香港網安奪旗賽」，賽事亦設立國際組別，除有效提升參賽者的網絡攻防能力，為本地培育網絡安全專才，更提供國際化交流平台，促進全球網安人才交流。

## **(II) 吸引海內外人才**

16. 政府積極吸引海內外網絡安全人才，壯大本地網絡安全人才庫。「科技人才入境計劃」為合資格公司輸入海內外科技人才來港從事研發工作，實施快速處理安排。截至今年8月底，共有40名來自網絡安全界別的非本地人士根據「科技人才入境計劃」獲准入境。政府亦已在「人才清單」下納入「資深網絡安全專家」等創科領域專業工種，方便業界透過相關的入境計劃輸入科技人才。根據入境事務處的資料，截至今年8月底，在「優秀人才入境計劃」、「一般就業政策」

及「輸入內地人才計劃」下，共有48個符合「人才清單」上「資深網絡安全專家」資格的申請獲批。

17. 此外，政府於2025年5月公布的「技術專才清單」將「資訊科技技術員」納入為八項指定技術工種之一，容許從事網絡安全、網絡支援和程式編寫三個工作範疇、且年齡介乎18至40歲的非學位中層技術專才，透過「一般就業政策」及「輸入內地人才計劃」下的新增渠道，定居香港發展，豐富本地業界人才資源。新增渠道為期三年，設有共一萬個申請配額，每項技術工種的申請配額以三千個為限。技術專才類別已於今年6月30日開始於網上接受申請。

### 徵詢意見

18. 請委員備悉本文件的內容及提供意見。

創新科技及工業局

數字政策辦公室

2025年10月

香港網絡安全事故協調中心  
處理的資訊保安事故分項統計數字

事故類別	2023 年 9 月至 2024 年 8 月		2024 年 9 月至 2025 年 8 月	
	宗數	百分比 (%)	宗數	百分比 (%)
仿冒詐騙（釣魚網站）	6 141	58	8 973	57
殭屍網絡（殭屍電腦）	2 663	25	3 337	21
惡意軟件 （包括勒索軟件）	618	6	1 403	9
黑客入侵／網頁塗改	19	<1	11	<1
分散式阻斷服務攻擊	2	<1	4	<1
其他 <sup>2</sup>	1 140	11	1 994	13
總計：	10 583	100	15 722	100

<sup>2</sup> 包括盜用身份、資料外洩等

香港警務處  
處理的科技罪案宗數及其導致的財政損失的分項統計數字

	2024 年	2025 年 (截至 7 月)
案件性質	宗數	宗數
網上騙案	27 485	16 748
(i) 網上商業騙案	12 215	7 924
- 網上購物	11 559	7 594
- 信用卡盜用	656	330
(ii) 電郵騙案	197	69
(iii) 網上銀行騙案	20	19
(iv) 社交媒體騙案	3 039	1 347
(v) 網上雜項騙案 (包括網上投資騙案)	9 283	6 631
(vi) 釣魚騙案	2 731	758
網上勒索	2 559	915
(i) 裸聊	2 434	857
(ii) 其他網上勒索	125	58
盜用電腦	3 055	960
(i) 網上戶口盜用	2 989	935
(ii) 入侵系統活動	61	24
(iii) 分散式阻斷服務攻擊	5	1
其他性質	804	457
總計(宗數):	33 903	19 080
財政損失(百萬元):	5,129.0	3,639.4