2024年10月14日

討論文件

立法會資訊科技及廣播事務委員會

有關維護及推廣資訊保安的工作

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及推廣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，政府資助香港生產力促進局（生產力局）成立及營運的香港網絡安全事故協調中心（網安事故協調中心）共處理10 583宗保安事故，較去年上升約39%，當中的主要類別分別是仿冒詐騙（6 141宗）和殭屍網絡（2 663宗）。與上年同期相比，仿冒詐騙的宗數上升83%，而殭屍網絡事故宗數則減少約27%。此外，惡意軟件（包括勒索軟件）及網頁塗改的宗數均有上升趨勢。有關保安事故的分項統計數字載於附件一。

3. 香港警務處（警務處）在2023年共錄得34 112宗科技罪案，較2022年上升約50%，主要是由於盜用電腦（例如網上戶口盜用）及網上騙案（例如網上投資騙案）宗數有所增加。就盜用電腦案件方面，升幅主要來自即時通訊軟件帳戶騎劫案件。在2024年，警方首7個月共錄得19 257宗科技罪案，較去年同期上升約6%，網上戶口盜用的升幅仍最為明顯；惟科技罪案的整體案件數字及損失金額與過去兩年同期的升幅比較均明顯放緩。有關科技罪案的分項數字載於附件二。

4. 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）在過去一年共處理224宗資料外洩事故通報，主要

牽涉黑客入侵（85宗），較上年同期上升超過兩倍；遺失文件或便攜式裝置（52宗），較上年同期上升63%；以及經電郵、郵遞或傳真意外披露個人資料（31宗），較上年同期上升約120%。

推動社會層面的資訊保安工作

5. 政府一直致力提供一個安全穩妥的網絡環境，並與香港互聯網註冊有限公司（互聯網註冊公司）及網安事故協調中心等持分者保持緊密合作，向公眾提供相關資訊及支援，以應對日益增加的資訊保安及網絡安全風險，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： 為加強本地企業網絡的安全，互聯網註冊公司除了為「.hk」用戶提供免費及詳細的網站安全掃瞄服務及電話諮詢之外，更於2023年開拓全新的網站保安檢測服務—「網健通」服務，並在教育及社福界等行業中試行，主動提醒「.hk」用戶預早提防潛在網絡風險。截至2024年8月，互聯網註冊公司已向「.hk」用戶提供了約34 900次檢查服務。

  此外，警務處、私隱專員公署和網絡安全業界於2024年6月至8月協辦為期三個月的漏洞發掘及修正活動「狩網運動2024」，共有153家企業和機構參與。活動採用公私營合作模式，為參與企業提供免費網絡安全漏洞測試、網絡安全報告及一對一專業網絡安全諮詢，令企業可以對症下藥，全面提升安全防護水平。

- 免費線上員工培訓： 互聯網註冊公司於2022年8月推出「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，有助提高企業及其員工的網絡安全意識和知識。截至今年8月，共有約219 400人次參與培訓。

- 網絡安全資訊共享： 數字政策辦公室（數字辦）聯同互聯網註冊公司合作推行跨行業的「網絡安全資訊共享夥伴計劃」，以促進本地企業及機構（尤其中小企）

之間交流網絡安全資訊。截至今年8月，已有約2 400間企業及機構參與計劃，涵蓋銀行與金融、保險、公用事業、運輸、醫療、電訊、創新科技（創科）、教育等界別。

- 網絡事故電話熱線： 網安事故協調中心提供24小時免費電話熱線，接聽保安事故報告並在事故應變和復原上給予意見。

(II) 加強公眾教育

- 推廣網絡安全： 數字辦致力推廣並加強市民大眾的網絡安全意識。為響應「國家網絡安全宣傳周」活動，數字辦今年以「全城攜守 網安在手」為主題，與業界合辦「2024網絡安全宣傳運動」，透過舉辦香港分論壇、電車車身設計比賽、展覽、同樂日、技術研討會，以及提供相關學習資源等活動，向市民傳播維護網絡安全及國家安全的訊息。數字辦亦不時更新「資訊安全網」和「網絡安全資訊站」專題網站，包括更新教學視頻和測驗等，向公眾介紹最新的網絡安全資訊及防範網絡攻擊的方法。

- 保障個人資料： 私隱專員公署積極推動加強保障個人資料的做法，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，包括如何安全使用便攜式儲存裝置等，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： 警方一直透過多渠道宣傳防騙信息，提高市民大眾的防騙意識。針對涉及騎劫即時通訊軟件帳戶的騙案，警方在其「守網者網站」、Facebook等不同渠道加強宣傳，並舉行大型記者會，現場展示騙徒騎劫即時通訊帳戶的技術，及建議市民防範帳戶被騎劫的方法。警方亦通報電訊商攔截相關網頁，及向相關的網頁搜尋器及海外有關當局提出移除虛假WhatsApp網頁廣告的要求。

此外，警方推出「防騙視伏器」及相關手機應用程式，預警超過65萬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。機制將於2025年第一季進一步擴展至自動櫃員機，屆時將會實現全覆蓋，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通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，以及亞太區電腦保安事故協調組織，與負責其他地區的電腦緊急事故應變小組保持緊密聯繫及參與技術交流活動，包括定期舉行的亞太區電腦保安事故協調組織演習。

- 大型論壇： 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2023」，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。政府亦積極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」，並於去年峰會作主題演講，分享香港在網絡安全方面的發展和實踐工作。

- 合作備忘錄： 數字辦於2024年9月與廣東省互聯網信息辦公室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》，加強本港與廣東省及澳門特區在技術交流、資訊共享及緊急應對方面的合作，助力建設安全數字灣區。

(IV) 制定法規及指引

- 關鍵基礎設施電腦系統安全： 為了加強保護關鍵基礎設施電腦系統安全，推動關鍵基礎設施營運者建立良好的防範管理體系，保安局已於今年7月就建議立法框架諮詢立法會保安事務委員會，並再次諮詢業界。保安局已向保安事務委員會提交諮詢報告，預備於今年內向立法會提交條例草案。

- 數據中心基建安全：數字辦正與業界制定《數據中心保安實務指引》，涵蓋數據中心安全的管理、設計及運營和維護等方面，以提供實務指引作參考，提升本港數據中心基建的安全。數字辦預計於今年年底發布有關指引。

加強政府層面的資訊保安工作

6. 政府一直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，相關政策及措施如下：

(I) 制定及更新政策及指引

- 資訊保安政策：政府制定並不時更新《資訊科技保安政策及指引》（《政策及指引》），涵蓋管理架構、政策及技術措施，要求所有局／部門嚴格遵守。今年4月發布的《政策及指引》修訂版，進一步加強不同領域的資訊保安控制措施，同時提升對政府資訊科技系統安全的等級保護，以期更有效保障政府資訊科技系統及數據安全。創新科技及工業局及數字辦於2023年12月發布的《香港促進數據流通及保障數據安全的政策宣言》亦提出具體行動措施，加強本港的數據安全保障和設施規劃。

- 實務指引：數字辦制定了涉及不同資訊保安範疇的指引，包括《雲端運算保安實務指引》，為政府內部安全採用雲端運算技術提供實務指引和參考，同時要求所有局／部門全面檢視現有資訊保安措施，確保轄下系統和用戶均嚴格遵守相關要求，包括不可把敏感及個人資料儲存於公有雲平台上，以及妥善保護資料。今年6月發布的《流動保安實務指引》修訂版亦加強政府人員使用流動裝置的監管和安全，以有效管控政府敏感資料外洩的風險。

(II) 加強員工培訓及支援

- 員工培訓：數字辦舉辦研討會及解決方案分享會，讓政府人員認識最新的網絡安全趨勢及預防措施，藉此提升他們的資訊保安知識。截至今年9月，參加活動的年度人次已經超過7 100，較去年上升約173%。數字辦會繼續加強培訓，加深政府人員對資訊及網絡安全的認知和準備。

- 進修課程：數字辦正與職業訓練局(職訓局)轄下「香港資訊科技學院」籌辦「網路安全證書培訓計劃」課程予相關政府員工報讀，以提升他們的資訊保安專業技能。

- 防詐騙演習：數字辦將於2025年推行新一輪「全政府防範仿冒詐騙演習運動」，利用人工智能等新技術來模擬仿冒詐騙電子郵件，以加深政府人員對仿冒詐騙的認知。

(III) 優化政府及公營機構資訊科技系統的項目管治和保安

7. 為加強局／部門及公營機構的資訊科技安全，政府已於今年8月推行多項優化措施，要求各局／部門及其負責的公營機構提升資訊科技系統的項目管治和保安工作。相關措施的重點包括：

加強監督責任

- 高級人員角色： 各局／部門及相關公營機構須委派高級首長級人員負責其轄下重要資訊科技系統的項目管理，涵蓋整個系統開發及推行周期的監督及資訊保安工作，以便及早發現和處理資訊科技系統的保安風險，確保系統提供安全穩妥的服務。

- 電子系統事故機制： 優化有關政府或公營機構的重要資訊科技系統的保安事故處理機制，以更清晰地釐定在事故發生後的處理流程及跟進工作。

提升系統的安全和穩健性

- 額外測試、評估及審核：各局／部門及公營機構須在其資訊科技系統推出前安排由獨立第三方進行的額外壓力測試及保安測試，並就系統建立恆常的監察機制及進行自我評估，例如在如常運作階段的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。數字辦會提供適切的技術意見、指引、良好作業模式及其他相關資料，例如壓力測試及保安測試的規格、測試參數設定的相關風險因素等。

全面及規範化的系統檢查及防禦

- 系統健康檢查和遵行審計：數字辦會定期及持續地為政府面向公眾的資訊科技系統進行健康檢查和滲透測試，並以風險為本的方式進行保安遵行審計。

- 網絡安全攻防演練：數字辦將每年統籌網絡安全攻防演練。參與的局／部門和公營機構將組成「藍隊」，在演練期間，「藍隊」將防禦由網絡安全專家及業界組成的「紅隊」發出的模擬黑客攻擊，以測試系統在遇到網絡攻擊時的反應和應變能力，以期通過實戰演練提升局／部門和機構識別和應對網絡攻擊的技術、經驗及整體防禦能力，以攻築防。首次的實境網絡安全攻防演練將於今年11月進行。

人力資源發展

中小學階段

8. 政府重視培育數字科技世代下學生的資訊素養。教育局為學校提供《香港學生資訊素養》學習架構，教導學生有關資訊及網絡安全和保障個人資料私隱的重要性。同時亦舉辦一系列相關的教師培訓課程，並開發有關教材。

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，分別資助中學及小學舉辦與資訊科技相關的課外活動，包括網絡安全相關的課程、工作坊及比賽等。截至今年9月，接近1 000間學校在上述兩項計劃下舉辦約5 500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。

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。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包括電腦科學（包括網絡安全）在內等十個範疇的課程，以配合本港的社會和經濟需要。在2024/25學年，SSSDP涵蓋電腦科學範疇共五個學士學位及兩個副學位課程，涉及共405個資助學額。

11. 此外，職訓局於2023年11月新成立的「香港資訊科技學院」會專注提供資訊科技及其他相關科技課程，包括電腦及網絡科技高級文憑、網絡安全高級文憑等，鞏固香港資訊科技能力，以及回應業界的人力需要並促進香港未來的發展。

再培訓、持續進修及在職訓練

12. 本地勞動人口培訓方面，現時僱員再培訓局為合資格僱員提供超過700項恆常培訓課程，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，報讀電腦科學及資訊科技相關課程。

13. 此外，警務處、數字辦及網安事故協調中心於2023年再次合辦「網絡安全精英嘉許計劃」，表揚和鼓勵傑出的網絡安全管理人員和從業員，並藉此交流經驗，提升其專業水平，共建創新和不斷進步的網絡生態系統。是次計劃的參與組別由上屆的五個界別擴展至八大界別，涵蓋網絡安全審定及諮詢、網絡安全教育及訓練和網絡安全初創及中小企業等界別。

展望

14. 政府會繼續全方位加強社會對網絡安全的認知和防禦能力，以及提高政府內部及公營機構的資訊科技系統保安，讓香港成為一個更安全穩妥的智慧城市。

徵詢意見

15. 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
2024年10月

附件一

香港網絡安全事故協調中心
處理的保安事故分項統計數字

事故類別	上年度同期（2022 年 9 月-2023 年 8 月）		過去一年（2023 年 9 月-2024 年 8 月）		
	宗數	百分比（%）	宗數	百分比（%）	與上年度同期比較
仿冒詐騙（釣魚網站）	3 350	44	6 141	58	+83%
殭屍網絡（殭屍電腦）	3 671	48	2 663	25	-27%
惡意軟件（包括勒索軟件）	136	2	618	6	+354%
黑客入侵/網頁塗改	15	<1	19	<1	+25%
分散式阻斷服務攻擊	2	<1	2	<1	0
其他 [1]	422	6	1 140	11	+170%
總計：	**7 596**	**100**	**10 583**	**100**	**+39%**

[1] 包括盜用身份、資料外泄等

附件二

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

	2022 年	**2023** 年		**2024** 年（截至 **7** 月）
案件性質	宗數	宗數	與 **2022** 年比較	宗數
網上騙案	**19 599**	**27 314**	**+39.4%**	**14 898**
（i）網上商業騙案	*9 279*	*9 883*	*+6.5%*	*6 612*
- 網上購物	*8 735*	*8 950*	*+2.5%*	*6 280*
- 信用卡盜用	*544*	*933*	*+71.5%*	*332*
（ii）電郵騙案	*391*	*208*	*-46.8%*	*134*
（iii）網上銀行騙案	*7*	*16*	*+128.6%*	*15*
（iv）社交媒體騙案	*3 605*	*3 372*	*-6.5%*	*1 829*
（v）網上雜項騙案（包括網上投資騙案）	*6 317*	*9 513*	*+50.6%*	*4 849*
（vi）釣魚騙案 [2]	*-*	*4 322*	*-*	*1 459*
網上勒索	**1 557**	**2 428**	**+55.9%**	**1 437**
（i）裸聊	*1 402*	*2 117*	*+51%*	*1 365*
（ii）其他網上勒索	*155*	*311*	*+100.6%*	*72*
盜用電腦	**192**	**3 471**	**+1 707.8%**	**2 428**
（i）網上戶口盜用	*168*	*3 434*	*+1 944%*	*2 389*
（ii）入侵系統活動	*24*	*37*	*+54.2%*	*37*
（iii）分散式阻斷服務攻擊	*0*	*0*	*-*	*2*
其他性質	**1 449**	**899**	**-38%**	**494**
總計（宗數）：	**22 797**	**34 112**	**+49.6%**	**19 257**
財政損失（百萬元）：	**3,215.4**	**5,496.8**	**+71%**	**3,075.1**

[2] 釣魚騙案自 2023 年 1 月起被列為科技罪案其中一類分項