2022 年 4 月 19 日
討論文件

立法會資訊科技及廣播事務委員會

資訊保安的最新情況

目的

本文件向委員匯報本港資訊保安的最新情況和過去一年政府在資訊保安方面的工作。

背景

2. 過去兩年，各行各業為適應疫情下的「新常態」，紛紛加速了數碼轉型，為更廣泛應用資訊科技帶來契機，但同時亦對資訊保安帶來更多挑戰。另一方面，全球針對關鍵基礎設施的網絡保安威脅，例如供應鏈及物聯網攻擊，亦有所增加，對個人、企業及社會構成安全風險。故此，政府和社會各界都要提高警覺，繼續提升網絡安全的意識和防禦能力，以期有效應對和緩解相關網絡安全威脅所帶來的風險。

資訊及網絡安全的形勢

3. 政府一直積極應對「新常態」所帶來的資訊保安挑戰。香港電腦保安事故協調中心（事故協調中心）在2021年共處理7 725宗保安事故，較2020年回落約7%，當中最主要的資訊保安事故類別分別是仿冒詐騙（3 737宗）和殭屍網絡（3 479宗）。有關保安事故的分項統計數字載於附件一。與2020年相比，仿冒詐騙的宗數上升7%，當中逾七成事故涉及網上購物或網上銀行。而殭屍網絡事故宗數則較2020年減少約16%，主要原因相信是全球其中一個最大的殭屍網絡於2020年被成功摧毀，從而令感染該病毒的本地連網設備不再受其控制。此外，惡意軟件（包括勒索軟件）、黑客入侵或網頁塗改，以及分散式阻斷服務攻擊的宗數均錄得下降趨勢。

4. 香港警務處（警務處）在2021年共錄得16 159宗科技罪案，較2020年的12 916宗上升約25%，而每宗個案的平均損失金額則持續減少，由2020年約23萬元減至約19萬元，相關損失的總金額維持約30億元，與2020年相若。當中有關電郵騙案的損失金額超過15億元，佔整體科技罪案的一半，超過七成受害者為中小企業。有關科技罪案的分項數字載於附件二。

社會層面的資訊保安措施

5. 政府資訊科技總監辦公室（資科辦）與警務處的網絡安全及科技罪案調查科（網罪科）、事故協調中心及香港互聯網註冊管理有限公司（互聯網註冊公司）一直保持緊密合作，適時向公私營機構及公眾提供多方面支援，為社會建設一個安全穩妥的網絡環境。

(I) 提升本港企業（尤其中小企）應對各種網絡攻擊的能力

監測、預防和應對網絡威脅及攻擊

6. 事故協調中心繼續為本港互聯網社群提供網絡安全資訊。在2021年，事故協調中心共發布超過370項資訊及保安建議，並提供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。為支援中小企更有效應對保安事故，事故協調中心將於今年稍後發布專為中小企而設的《資訊保安事故指南》，以簡單易明的方式介紹如何預防和處理常見的網絡攻擊。

7. 事故協調中心亦聯同業界組織舉辦活動，增強各行各業對網絡安全的認知和防禦攻擊的能力，以及推廣資訊保安良好作業模式。單在2021年，事故協調中心與各行業商會合作舉辦了28次專題講座，吸引逾2 600名不同界別的從業員參與，涵蓋金融服務、保險、工業、教育、零售、餐飲及資訊科技等界別。來年，事故協調中心會繼續透過各個商會及中小企聯會，主動接觸更多中小企並適時提供有關網絡安全的服務。

8. 為協助中小企以有限的資源應對潛在的資訊保安風險，互聯網註冊公司早於2019年開始向中小企網站提供免費檢驗服務，服務包括檢查網站是否存在安全漏洞、提供掃描報告及建議。截至2022年2月，互聯網註冊公司已為本地中小企檢查超過3 700個

網站。事故協調中心亦於2021年9月推出「評估你的網絡保安狀況」線上自我評估工具，讓中小企更了解其網絡安全狀況，並提供建議幫助中小企提升整體資訊保安能力。

9. 為降低中小企業員工獲取網絡安全知識的門檻及將知識更適切地應用於工作上，互聯網註冊公司將於今年內開發各類生動而簡便的培訓教材供有關員工使用，並會針對不同行業（例如製造業、零售業等）或員工的工作性質（例如人力資源、財務等）所面對的不同網絡風險主題及場景度身訂造培訓內容，幫助中小企提高網絡安全意識及進行網絡安全員工培訓。

10. 隨着不少企業實施在家工作，資科辦聯同事故協調中心透過多重渠道發放相關的保安建議及指南，內容涵蓋安全使用視像會議、遙距工作的保安措施等，協助用戶維持安全遙距工作環境。因應疫情再趨嚴峻，事故協調中心於2022年1月發布更新的「在家工作」保安建議，提醒企業與在家工作的員工注意工作環境的私隱和資訊保安，確保Wi-Fi網絡及帳戶安全，並對電腦系統及流動工作裝置採取適當的保安措施以防範網絡攻擊。

11. 此外，為協助中小企防範電郵騙案，警務處推出「衞郵計劃」（e-GUARD）打擊電郵騙案，並聯同香港大學共同研發「可疑電郵偵測系統」（V@nguard），協助中小企自動識別可疑電郵。系統首階段已於2022年1月開放予企業免費使用。

財政支援

12. 為配合創新及科技的發展，政府一直提供財政資助以加強企業的資訊保安水平。政府透過「科技券」計劃資助本地企業使用科技服務和方案，本地非上市企業及機構均可申請資助以提高生產力或將業務流程升級轉型。企業同時可以利用資助提升系統及推出網絡安全措施，包括防禦網絡攻擊、運作復原方案及近來漸趨盛行的網絡保安託管服務。自2016年至今，計劃已資助超過450個涉及提升資訊系統及網絡安全的項目，相關的資助金額約6,700萬元。

網絡安全資訊共享

13. 資科辦繼續聯同互聯網註冊公司合作營運跨行業的「網絡安全資訊共享夥伴計劃」，以促進公私營機構（尤其中小企）之間

交流網絡安全資訊。截至2022年2月，已有約1 000間公私營機構參與計劃，涵蓋的界別廣泛，包括金融（當中有約130間銀行）與保險、公用事業、運輸、醫療、電訊、創新科技（包括資訊保安）、教育等。我們亦正積極與保險業監管局合作推動保險業界參與計劃，現時已有超過50間保險公司登記成為夥伴計劃成員。平台亦設公眾區域，讓公眾也可以獲取專家提供的保安警報和建議。

14. 平台於2021年7月推出應用程式介面（API），讓成員機構可以自動化方式從平台取得網絡威脅資訊。我們亦會繼續探討從更多渠道（包括免費的公開來源及付費的商業來源）獲取合適的網絡安全威脅情報，讓成員機構能更迅速防禦網絡攻擊。

(II) *公眾教育*

15. 資科辦透過不同渠道（包括電台、社交媒體、網站等）向公眾提供資訊保安建議。在2021年，我們經電台節目中播放了多個系列的宣傳聲帶，內容涵蓋物聯網裝置的安全意識、安全使用流動支付、提防惡意軟件感染、密碼管理和提防仿冒詐騙攻擊等。此外，資科辦亦與香港電台聯合製作兩輯分別以提防電郵、短訊騙案及網絡禮儀為主題的「資安探訪團」節目，在2022年2月於網上平台播放，以提高公眾對仿冒詐騙的警覺性及了解相關訊息。

16. 資科辦繼續與專業團體合辦學校探訪。於2020/21及2021/22（截至2022年2月）兩學年合共進行了約30次實體或遙距模式的探訪，向逾5 200名師生傳遞資訊保安訊息。在2021年，資科辦通過實體或遙距模式到長者服務中心舉行網絡安全講座，以提高長者的保安意識。來年，我們會因應疫情採取適當模式繼續向師生及長者傳遞資訊保安訊息。

17. 為提高社會對資訊安全及預防網絡陷阱的意識，警務處透過全方位發放防騙訊息，包括舉辦「防騙月」、推出「防騙一站通」網站及舉辦「跨年全城守網運動」。警務處亦於2021年8月推出「守網者」一站式平台，提升公眾對網上欺詐和不良資訊的警覺性。

18. 為了增進公眾對網絡安全的知識，資科辦、警務處和事故協調中心在2021年舉辦了一系列宣傳活動，包括網上研討會及比賽，以提升公眾的網絡安全認知。隨着二維碼（QR Code）的使用

日趨普及，事故協調中心亦提供了「安全使用QR Code」指引，提醒公眾留意相關的保安風險。

(III)支持國家安全教育

19. 資科辦聯同警務處和事故協調中心於2021年9月舉辦年度「共建安全網絡」資訊保安推廣活動，加強機構及公眾對網絡安全與國家安全的認識，並提醒他們須採取穩妥的網上行為，共同維護網絡安全，提高香港市民的守法意識，避免落入網絡陷阱甚至誤墮法網。今年，政府會繼續這方面的工作。

(IV)與國際及內地合作

20. 資科辦與事故協調中心一直積極與內地及世界各地的電腦緊急事故應變中心合作，例如在2021年繼續參與由亞太區電腦保安事故協調組織舉辦的年度聯合事故應變演習，與25個來自19個不同經濟體的會員，共同測試彼此之間在協調應對跨境事故及溝通的能力。

資訊保安人力資源發展

21. 為吸引世界各地人才來港，政府會繼續推行「科技人才入境計劃」，簡化申請科技（包括網絡安全）人才入境從事研發工作的手續，從而加快吸納世界各地的網絡安全科技人才。

22. 警務處、資科辦及事故協調中心於2021年再次聯合舉辦「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，以預防及偵測網絡安全事故及共建健康的網絡生態系統。

23. 為加強年青人的網絡安全知識和技能，以及提升他們從事網絡安全工作的興趣，互聯網註冊公司於2021年5月舉辦「網絡安全青年計劃2021」。計劃吸引逾100名來自超過56間中學的學生參與為期4天的網絡安全課程及模擬訓練，內容包括網絡攻擊及防禦培訓、伺服器漏洞、系統基礎及攻擊鏈等。

24. 此外，資科辦資助香港生產力促進局和事故協調中心於2021年11月合辦「香港網絡保安新生代奪旗挑戰賽2021」，提升

學生與年青人的網絡安全知識和參與資訊保安行業的興趣。本屆比賽除原有的中學組及大專組外，更增設公開組，並邀請了內地、澳門和韓國的奪旗高手一同參與和交流。比賽反應熱烈，逾940名本地中學、大專院校學生及資訊科技精英共組成315隊參賽。

政府內部應對網絡安全威脅的措施

(I) 資訊分享及威脅警報

25. 資科辦在政府內部繼續利用大數據技術收集和分析不同來源的網絡安全威脅資訊，進行整理及評估，適時發布網絡威脅預警，提醒部門盡快修補保安漏洞。資科辦在2021年共發出超過170次關於電腦系統或軟件漏洞的保安警報，並要求各局和部門迅速採取適切的防禦措施，以妥善保護政府的資訊系統和數據資產。

(II) 在家工作的資訊保安

26. 為配合政府人員在家工作安排，各局和部門可根據《政府資訊科技保安政策及指引》，在確保資訊安全的情況下，向其人員提供已安裝並定期更新保安修補程式和抗惡意程式軟件的手提電腦和流動裝置等設備，通過安全的通訊渠道（包括已加密的虛擬私有網絡（VPN）連線，並輔以雙重認證）遠程接達政府網絡和系統在家工作。資科辦亦於2022年1月新一波疫情爆發初期再次提醒各部門在安排在家工作時的注意事項，確保政府的系統及數據安全。

27. 此外，資科辦與各局和部門會定期舉辦保安培訓，以提升人員對網絡安全的認知，包括有關遠程接達政府系統和網絡的資訊。資科辦不時提醒各部門及人員，包括慎防仿冒詐騙攻擊和安全使用視像會議應注意事項等資訊。資科辦更舉辦了多個網上研討會及解決方案展示會，以提升政府人員相關的知識。

(III)保障數據安全

28. 我們致力維護數據安全。保安局訂立的《保安規例》就政府資料作出了保密分類的定義，明確要求政府部門把其管有的資料作出適當保密分類，以及就其分類採取相應措施，確保這些資料在儲存及業務運作過程中得到充分保護。資科辦亦在《保安規

例》的框架下制訂了詳細的《政府資訊科技保安政策及指引》供各部門遵循，並要求各部門加強在數據方面的保護措施，以應對不同的資訊保安威脅。

29. 政府在開發與抗疫及防疫相關的系統時，例如「居安抗疫」家居檢疫系統、「安心出行」流動應用程式及「香港健康碼」系統等，一直嚴格遵守《政府資訊科技保安政策及指引》和《個人資料（私隱）條例》的規定，並在推行項目的不同階段，聘用獨立第三方進行私隱影響評估和資訊保安風險評估及審計，以及適時諮詢個人資料私隱專員公署的意見，以確保系統及數據的安全和市民的私隱得到穩妥保障。

(IV) 員工培訓及技術支援

30. 為加強各局和部門的防禦及應對網絡安全事故的能力，資科辦每年會舉行大型跨部門網絡安全演習。另外，為有效針對仿冒詐騙相關攻擊，我們於2022年1月推行新一輪「防範仿冒詐騙演習運動」，除了透過模擬仿冒詐騙電子郵件加深員工對仿冒詐騙的認知外，我們同時推出「防範仿冒詐騙資源中心」專題網站，網站內容包括教學視頻和測驗等，介紹如何識別仿冒詐騙的電子郵件和各種常見陷阱。

31. 資科辦在2021年舉辦了多個研討會及解決方案分享會，以提升政府人員的資訊保安知識。去年有超過2 000名政府人員藉此認識最新的網絡安全趨勢及預防措施。資科辦亦鼓勵員工考取國際認可的資訊保安證書，鞏固在資訊保安方面的專業知識。

32. 此外，資科辦會繼續透過網絡及系統檢測平台的功能，協助各局和部門為其網上系統及網頁進行安全檢測及滲透測試，及早找出潛在漏洞並進行修補，維護系統安全。在2021年，檢測平台為超過820個政府網站進行測試。我們正籌備推出更新的平台為政府網上系統及手機應用程式進行更深入的安全測試。

(V) 遵行審計

33. 為確保各局和部門嚴格執行政府的保安規定，資科辦定期為各局和部門進行獨立資訊保安遵行審計，並向部門提供建議協助他們持續改善資訊保安管理系統，以應對新興資訊保安威脅。

前一輪審計工作已於2021年12月完成，有關報告已呈交各部門首長作參考和跟進。新一輪審計工作將於2022年第二季展開。

展望

34. 為有效提升社會對網絡安全的整體防禦能力，政府會繼續積極與各持份者合作，透過多方面措施加強商界，特別是中小企，以至公眾對網絡安全的認知和防禦能力。同時，創新及科技局和資科辦會繼續加強措施以提高政府內部的網絡安全水平，並支援保安局就訂立網絡安全的法例進行準備工作，通過立法方式清晰界定關鍵資訊基礎設施營運者的網絡安全責任，加強保障本港網絡系統及重要基礎設施資訊系統的運作及數據安全，讓香港成為一個更安全穩妥的智慧城市。

徵詢意見

35. 請委員備悉文件內容。

創新及科技局
政府資訊科技總監辦公室
2022 年 4 月

附件一

香港電腦保安事故協調中心
處理的保安事故分項統計數字

事故類別	**2020** 年		**2021** 年		
	宗數	百分比	宗數	百分比	與 **2020** 年比較（百分比）
仿冒詐騙（包括釣魚電郵及網站）	3 483	*42*	3 737	*48*	*+7*
殭屍網絡	4 154	*50*	3 479	*45*	*-16*
惡意軟件（包括勒索軟件）	181	*2*	112	*1*	*-38*
黑客入侵／網頁塗改	36	*<1*	19	*<1*	*-47*
分散式阻斷服務攻擊	53	*<1*	10	*<1*	*-81*
其他[1]	439	*5*	368	*5*	*-16*
總計：	**8 346**	***100***	**7 725**	***100***	*-7*

[1] 包括盜用身分、資料外泄等

附件二

香港警務處處理
有關科技罪案宗數及其導致的財政損失的統計數字

	2020 年	**2021** 年	
案件性質	**宗數**	**宗數**	**與 2020 年比較（百分比）**
網上騙案	10 716	13 859	*+29*
（i）網上商業騙案	*6 941*	*6 491*	
（ii）電郵騙案	*767*	*549*	
（iii）網上銀行騙案	*0*	*87*	
（iv）社交媒體騙案	*1 988*	*3 638*	
（v）網上雜項騙案	*1 020*	*3 094*	
網上勒索	1 144	1 317	*+15*
（i）裸聊	*1 009*	*1 159*	
（ii）其他網上勒索	*135*	*158*	
盜用電腦[2]	111	142	*+28*
其他性質	945	841	*-11*
總計（宗數）：	**12 916**	**16 159**	***+25***
財政損失（百萬元）：	**2,964**	**3,024**	***+2***

[2] 包括網上戶口盜用、入侵系統活動和分散式阻斷服務攻擊