



「網絡安全面面觀講座」 — 教育篇

講座重點節錄

2022/5/26

主辦單位：



支持單位：



香港警務處
網絡安全及科技罪案調查科

「網絡安全面面觀講座」 — 教育篇

講座重點節錄

嘉賓致辭重點	—————○	2
講者分享重點	—————○	7
問與答	—————○	9
附錄	—————○	13

嘉賓致辭重點

中國聯通國際有限公司董事長兼總裁孟樹森博士



「網絡和資訊安全牽涉到國家安全和社會穩定，是我們面臨的新綜合性挑戰。香港是『一帶一路』建設的重要節點，網絡資訊安全是香港成為金融中心、實現創科中心的必備條件；而構建安全可靠的網絡生態環境，需要政府、學校、企業三方聚力，攜手推動網絡安全發展。」

嘉賓致辭重點

「網絡安全是國家安全的重要一環，教育局在國家安全教育中會包括網絡安全教育。隨著資訊科技發展迅速，在掌握使用這些新科技的能力之餘，社會更應該重視培養正向的媒體和資訊素養，讓大眾不會受到不同媒體的虛假或偏頗訊息所誤導。」



教育局局長政治助理施俊輝先生

嘉賓致辭重點

香港警務處助理處長東九龍總區指揮官羅越榮博士

「科技罪案數字由十年前3,000多宗上升超過4倍至去年16,000多宗，損失金額高達30億元；亦因此，全球對網絡安全人才的需求愈來愈多，由2013年的100萬攀升至去年350萬至450萬人，升幅高達350%。」



嘉賓致辭重點

香港警務處網絡安全及科技罪案調查科總警司鄭麗琪女士



「網絡陷阱可謂五花八門，除了我們認識的網絡攻擊、資訊安全風險以及網絡詐騙，網絡世界亦充斥著虛假資訊、不良內容和不當行為。面對著愈趨複雜的網絡世界，每個市民都應該提升自身網絡安全、防罪意識及守法意識，以免成為受害人，甚至誤墮法網，成為加害者。」

嘉賓致謝辭重點

港專校長陳卓禧博士

「港專得到業界頂級企業的支持，加上獲教育局資助，參照國家級水平興建的網絡安全實驗室和實戰靶場系統亦將接近完工，未來將善用在學術和專業上的優勢，為香港加強網絡安全盡一分力量。」



講者分享重點

中國聯通國際有限公司 高級信息安全工程師史芳玲女士

- 2021年 全球組織遭遇的網絡攻擊數量較2020年增長了50%，其中教育行業更是2021年網絡攻擊者的首要目標，單一教育組織每周平均遭受1,605次攻擊，較2020年增加了75%
- 引用與網絡安全相關的案例，如2020年加州一所大學遭遇勒索軟件攻擊後支付114萬美元贖金、香港一所公立大學線上考試遭駭客入侵，以及聊天室內傳播色情圖片等，均說明網絡安全的重要性
- 資訊安全的三要素 (CIA): 保密性 (CONFIDENTIALITY)、完整性 (INTEGRITY) 及可用性 (AVAILABILITY)



講者分享重點

港專協理副校長林森博士



- 網絡安全是關於如何確保個人、組織及國家的網絡空間在威脅及攻擊下仍能繼續生存及運作
- 網絡安全其實和大多數人關係密不可分，惟因為大眾對網絡安全缺乏認知、或心存僥倖、不想麻煩等想法令推廣網絡安全變得困難
- 港專期望一方面能透過專業優質的服務和教育，為香港培育更多網絡安全人才，另一方面從普及大眾對網絡安全的認知入手，提高他們的網絡安全意識

問與答

Q1：為何我們要教育年青人認識網絡安全？

隨着資訊及通訊科技的迅速發展，香港在經濟發展、創業、商業運作和日常生活上日益依賴互聯網、電訊基礎設施及智能裝置。資訊保安問題和網絡環境的風險對企業和個人會構成各種影響，因此有必要加深公眾對網絡安全的認識。

Q2：政府是否每一個部門都需要網絡安全的人才呢？如果年青人希望加入政府，有什麼部門或職位需要有「網絡安全」專業知識的人員呢？

政府非常重視資訊保安和保護政府的資訊及電腦資產。政府內部成立了資訊保安管理委員會及資訊科技保安工作小組，以監督整個政府內部的資訊科技保安工作。在部門層面，各部門會委任一位高級人員，作為部門資訊科技保安主任，領導該部門的整體資訊保安管理。各部門亦會設立包括管理和技術人員在內的資訊保安事故應變小組處理日常所有事項，以準備、偵測和應對所有資訊保安事件及事故。

Q3：政府會從什麼途徑向年青人教育網絡安全的重要性？未來還會投放什麼資源以推動網絡安全教育的發展？

資訊保安管理是一個持續的過程，需要公眾的承擔和關注，政府繼續通過各種渠道和方法，提高公眾對資訊保安及網絡風險的認知及認識。為加強公眾對資訊保安的認知和推廣這方面的道德標準，政府資訊科技總監辦公室已設立「資訊安全網」網站

(www.infosec.gov.hk)，方便公眾通過該一站式的入門網站，取得各類與資訊保安有關的資源和最新資料。除網站資訊外，政府資訊科技總監辦公室亦積極與專業機構及業界團體合作，共同籌辦資訊保安活動和研討會，以加強公眾對資訊保安的認知。政府資訊科技總監辦公室將繼續致力推廣和協調各界在這方面的教育工作。

(以上資訊由教育局局長政治助理施俊輝先生提供)

問與答

Q4: 從事網絡安全工作的人員需要具備哪些條件（例如學歷、專業資格、經驗、年紀、性格特質）？

網絡安全相關工作一般可分為兩個類別，一是專門做網安的安全專業公司，他們對人員的技術实操能力要求較高、學歷相對寬鬆一些，一般專科也是可以；二是大型非安全專業公司，如電訊企業、金融行業等，他們對學歷相對會有一定的要求，一般都會是本科起步，有的更有學校類別限制；而在技術方面，他們會要求人員具備基本的技術能力，根據不同的崗位職責在工作中慢慢提升技術能力。

Q5: 在電訊行業內有什麼有關網絡安全的職位？

電訊行業內有關網絡安全的職位名稱一般如下：網絡安全工程師（初、中、高）、資訊安全工程師（初、中、高）、安全營運/安全運營總監、安全產品經理、安全諮詢經理等。

Q6: 從事網絡安全工作的人員的事業發展前景好嗎？

資訊時代，網絡空間已成為陸、海、空、天之外人類活動的「第五空間」。世界上主要國家普遍對網絡安全人才問題高度重視，並把人才發展作為國家關鍵基礎設施網絡安全保障的基礎和先決條件；網絡安全人才培養戰略被推上前所未有的高度，所以目前來看從事網絡安全工作的前景是比較樂觀的。

Q7: 你認為未來五年各行各業對網絡安全工作人員的需求會持續上升嗎？能否預計五年後香港需要約多少位網絡安全工作專才？

2021年11月11日，根據Cybersecurity Ventures最新發佈的全球網絡安全人才報告，過去8年全球網絡安全空缺職位的數量增長了350%，從2013年的100萬個職位增加到2021年的350萬個。但是數據顯示，2021年全球網絡安全人才缺口10年來首次停止擴大，即便是這樣，報告也是預測未來5年，全球網絡安全職位空缺數量將維持平穩。預計5年後香港需要的網絡安全工作專才數量可參考政府資訊科技總監辦公室網站：

https://www.ogcio.gov.hk/tc/our_work/business/industry_support/ict_manpower/student_ict_corner/career_corner/hk_ict_manpower/

(以上資訊由中國聯通國際有限公司高級信息安全工程師史芳玲女士提供)

問與答



Q8：網絡安全及科技罪案調查科（網罪科）的工作範疇是什麼？這個部門是否有很大的人力資源需求？

網罪科是負責維護香港的網絡安全和打擊科技罪行，工作範疇包括調查科技罪案、收集和分析網絡罪案情報、進行數碼法理鑑證、保護重要基礎設施、防罪宣傳教育和內部人員培訓。網罪科的前身（即科技罪案組）在2001年成立，當時只有45人，至今部門已經有超過350人，而且不斷在擴展，以應對數碼年代的挑戰。

Q9：網罪科的警員需要具備哪些條件（學歷、知識、經驗、年紀、性格特質）？

年齡、學歷、背景和經驗並不是重點；雖然具有IT相關學歷和工作經驗在工作上有優勢，但最重要的條件是勇於接受挑戰、喜歡學習新知識和技能，做到終身學習。事實上，很多網罪科人員都沒有IT相關學歷和背景，他們的IT知識都是從在職培訓取得。

Q10：新加入警隊的人員可以加入這個部門嗎？會否有特別考核或必須經過一定年數或職級才可以加入呢？

一般而言，警員或督察級人員均要通過基礎培訓（即學堂培訓），並完成職業發展途徑，累積一定警務工作經驗後，才能加入網罪科。

Q11：近年網絡安全犯罪率有上升趨勢嗎？

科技罪案數字在過去10年可謂升幅驚人。在2012年，警方只錄得3,015宗科技罪案。直至去年，科技罪案數字錄得新高，達到16,159宗，相關經濟損失亦由2012年3.4億元飆升至30億元。在香港發生的科技罪案的犯案者主要身處境外，至於在香港的科技罪案犯案者則來自不同年齡層和背景。

(以上資訊由香港警務處網絡安全及科技罪案調查科提供)

問與答



Q12: 香港現時的網絡安全職位晉升階梯及未來的發展是怎樣?

常見網路安全職位及進升階梯如下:

- 首席資訊安全官 (Chief Information Security Officer/ Chief Security Officer/ Head of Cyber Security)
- 資訊安全主管 (Information Security Executive/ Cyber Security Executive)
- 資訊安全總監 (Information Security Director/ Cyber Security Lead)
- 資訊安全經理 (Information Security Manager/ Cyber Security Manager, SOC Manager, Cyber Security Product Manager, Security Operations Center Manager)
- 資訊安全分析師／工程師／顧問 (Information Security Analyst/ Cyber Security Engineer/ Pentester/ AWS Cloud Architect/ Security Consultant)
- 初級資訊安全工程師 (Entry Level Cyber Security Engineer)

未來仍會以這些職位為主，但相信在不同領域如軟件開發安全、數據安全、產品安全或雲計算安全等會有所細分。

Q13: 若果本身已經從事資訊科技相關的工作，想入職網絡安全工作有什麼要準備，例如考取相關認可證書?

專業上最好能有網絡及系統，尤其是Linux的知識及技能，懂得如何使用常見的網絡安全工具；並要對本地及海外相關法律法規有一定認識了解，以及能遵守相關行業的操守準則。想入行者亦可嘗試獲取CISSP (Certified Information Systems Security Professional)、CISA (Certified Information Security Auditor) 及CISM (Certified Information Systems Manager) 3個保安認證資格。

(以上資訊由港專協理副校長林森博士提供)

活動花絮：



<https://bit.ly/3zoTb3i>

講者簡報：



<https://bit.ly/394EN5I>

網絡安全課程發展：



<https://bit.ly/3MxpmRd>