深偽騙案年增10倍 騙徒扮財務官呃2億元

香港文匯報訊（記者 蕭景源）一項研究發現，香港今年首季涉及深度偽造（深偽）的詐騙事件數目按年增幅達10倍，為亞太地區增長最高的地區之一，而香港金融科技行業涉及的深偽欺詐率為亞太區最高，市民擔心不法分子利用深偽技術製造仿真度頗高的面貌和聲音成功進行詐騙，令人防不勝防。保安局局長鄧炳強昨日在立法會會議上書面答覆譚岳衡議員的質詢時表示，警方於過去3年共接獲3宗相關成功個案，最大一宗涉及騙徒假冒首席財務官進行視像會議，騙取高達2億元。

鄧炳強表示，警方自2023年11月1日起開始立項就此類騙案作分項紀錄統計，截至今年5月31日，共接獲3宗與深偽技術相關成功進行詐騙個案，當中一宗已破案，其餘兩宗仍在調查。

香港首宗與深偽技術相關的成功騙件涉及一個本地詐騙集團，在2022年9月至2023年7月期間盜用他人身份，利用人工智能換臉程式，於網上向財務公司申請貸款，涉款20萬元。警方同年8月展開「解詐」行動拘捕9人，包括一名主腦，涉嫌干犯串謀欺詐罪，是首次偵破人工智能換臉案。

第二宗個案發生在今年1月底，警方接獲一宗利用深偽技術預先錄製影片進行視像會議的欺詐案。報案人收到假冒其英國總公司首席財務官的釣魚訊息，聲稱要進行機密交易，邀請報案人進行多人視像會議，報案人最終按指示授權轉賬至5個本地銀行賬戶，涉及損失約2億元。

預錄影片無對話互動

經調查後，警方相信騙徒先下載被偽冒職員的網上公開影片及聲音，再利用深偽技術製作預錄的視像會議。由於是預錄影片，報案人與對方其實並無對話互動。騙徒向報案人下達命令後藉詞掛線，再以即時通訊軟件繼續指示轉賬，相關個案的調查仍在進行。

第三宗個案發生在今年5月20日，有跨國貿易公司職員收到偽冒為英國總公司首席財務官的WhatsApp訊息，並進行近半小時的視像會議，其間「假上司」指示職員把近400萬元轉賬至一個本地戶口。調查後相信疑犯以網上公開資料作素材，配合深偽技術將影片內容篡改，再於視像會議中播放，以誘騙受害人進行轉數，案件正調查中。

就有關發現或接獲舉報網上深偽片段方面，自2023年11月1日至2024年3月共有21條，分涉假冒政府官員或知名人士，其中兩宗由警方主動偵查發現，19宗為市民舉報。應警方要求，相關網上或社交媒體平台已把該21條片段迅速下架。

到目前為止，警方未有接獲市民直接因為這些相關深偽片段而受騙的報告。

資科辦：年內與內地演練網絡攻防

保障政府部門和公營機構網安 加強前線培訓

隨着科技進步迅速，互聯網已成為市民日常生活中的一部分。香港特區政府資訊科技總監辦公室副政府資訊科技總監黃敬文昨日在「網絡安全論壇2024」上表示，國家「十四五」規劃明確支持香港建設國際創新科技中心，而網絡安全是確保這個目標得以實現的關鍵。他之後在接受香港文匯報訪問時透露，資訊科技總監辦公室預計在今年內與內地合作，安排一次面向政府部門及公營機構網站系統的網絡攻防演練，進一步保障網絡安全，同時會在各方面加強宣傳，讓市民無時無刻提高警惕，「任何一個短板都可能成為不法分子的突破口，因此每個人都有責任，共同維護香港的網絡安全。」

◆香港文匯報記者 黃子龍

▲圖為警務處在去年「全民國家安全教育日」中，有關網絡安全的攤位遊戲。 資料圖片

◀「網絡安全論壇2024」昨日舉行。 香港文匯報記者郭木又 攝

今年年初，網上出現以人工智能（AI）偽造的影片，內容冒稱特區行政長官向市民推介一項投資計劃。黃敬文表示，幸好政府立刻闢謠，並將此事交給警方處理，才沒有對市民造成更大損失。「從此事可看出所謂『有圖有真相』已非完全正確，即使自稱是熟人，最好也要向共同認識的人再次確認其聯絡方式，以防萬一。」

◆黃敬文 香港文匯報記者黃子龍 攝

他透露，資科辦已從特區政府內部、公眾社會兩個層面採取相應措施。在保障網絡安全方面，特區政府內部已制訂全面的資訊科技保安政策和指引，要求每個部門及工作人員都清楚認識並嚴格遵守。隨着新風險的出現，資科辦亦會不時更新指引，加強保安措施。

內地專家扮演黑客查找不足

同時，每逢政府需要使用新系統前，資科辦都會對其進行獨立的安全測試，甚至嘗試攻擊系統，從而檢查是否有安全漏洞和風險。今年內，資科辦會有新的攻防演練，更將與內地的網絡專家合作，由他們扮演黑客，對政府部門及公營機構網站系統攻擊，期望進一步保障網絡安全。

在公眾社會層面上，資科辦向中小企業提供了科技券購買資訊科技服務，包含網絡安全服務或方案，增強抵禦網絡攻擊能力。

計劃從2016年11月推出，至今已資助超過1,000個涉及網絡安全的項目，資助金額超過1.5億元。香港互聯網註冊管理有限公司也會提供一些免費服務，幫助中小企業掃描他們的網站，以及進行保安測試。

特區政府還會為前線員工及管理層提供網絡安全培訓，以及積極在學校、企業等提醒和教導社會各界，讓他們對網絡安全有更全面的認識。「科技和犯罪手法會不斷變化，最重要是每個人都提高自身的風險意識，才是最好的保障。」

私隱專員教防騙 首務保護個資

擔任論壇演講嘉賓的個人資料私隱專員鍾麗玲在接受香港文匯報訪問時表示，個人資料外洩的後果可能非常嚴重，蒙受損失的可能不只自己，更會影響到朋友、家人。特區政府近年做了大量工作，包括製作一系列防騙短片、到長者中心等不同地方宣傳防騙知識、製作關於使用社交媒體及智能電話注意事項的懶人包等，從而讓市民提升保護個人資料的意識。

「可能只是不小心外洩了自己的名字、電話號碼、住址等資料，便會被不法分子有機可乘。」鍾麗玲強調，保障個人資料不要外洩顯得尤為重要，每個人都需要小心保護自己的一切訊息。

為此，她提供一些小提示：「在網上登記須填寫個人資料時，不要提供任何非必要的資訊；有『親友』致電借錢或詢問資料時，先掛斷電話，再主動核實對方身份。」

本屆論壇由中港網絡安全協會主辦，旨在探討大灣區和其他內地城市的網絡安全韌性與數據私隱挑戰。

立法將爲網安定基準 專家倡機構先自評

香港文匯報訊（記者 胡恬恬）近年網絡攻擊增加，特區政府正式提出保障關鍵基礎設施電腦系統的立法框架。多位業界專家昨日在論壇後接受香港文匯報訪問時表示，對立法表示支持和歡迎，相信立法能夠為網絡安全工作提供一個基準，幫助提升整體香港網絡安全。他們預計一些行業在轉變時會遇到成本上升等挑戰，建議相關機構根據立法框架先做自我評估，再視乎自身能力投入人手和資源。

中港網絡安全協會創會主席葉青陽表示，在香港提供必要服務的基礎設施的八個界別中，金融、電力、航空等領域一直較為注重相關的電腦系統和網絡安全，且企業一般規模較大，有足夠人手和資源去投放，相關的監管也較為成熟。不過，海運、通訊和廣播這類領域的企業則相對較弱，未必有能力投入大量的資源注重相關工作，但其提供的服務和行業的重要性又不容小覷。

他舉例說，香港很多海運公司老闆可能對網絡安全的理解尚未很到位，「他可能覺得，我的電腦壞了就用紙寫，我的貨物就這樣出貨亦一樣。」但其實，現在很多香港的碼頭全都已電腦化，若他們的系統癱瘓，一些進口香港的貨品亦會受到影響，「可能港人一個禮拜都沒有水果吃。」

葉青陽認為，企業不論大小，實際上都在相關方面有一定的認識和預算，因此法例可行性很高，並相信立法有助於推動IT等方面人才的增長，帶動相關行業的從業及就業。

余法昌：內地澳門早已立法

協會諮詢委員余法昌對立法表示歡迎。他表示，國際上已有類似的法例，而內地和澳門也早已對此立法，因此香港在這方面的立法刻不容緩，相信條例可以令整個香港的網絡安全得到提升。

他認為，條例推動營運者從三方面保障相關系統安全，一是建立整體的框架和流程進行管理，二是通過一些網絡安全措施進行有效的管控，三是事故通報。這三方面是國際通行做法，因此可行性很高，但一些細節可能需要再商討。

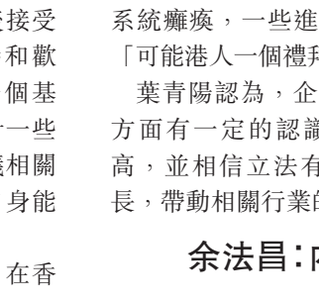
余法昌舉例，政府建議營運者在得悉事件兩小時至24小時內報告保安事故，這與當前按歐盟標準執行的慣例72小時通報時間有出入，有些企業可能要重新調整現有的事故處理和通報流程，視乎是否能夠配合法例要求，因此這一點可能在業界會有一些討論。

在成本和預算方面，余法昌直言預算必定會增加，增加多少要視乎企業自身能力而定，一些已經在做相關工作的企業預計增加成本不會很高。他建議相關企業可以參考這個法例框架，先做一個自我評估，審視目前的安保情況、事故應變處理能力等去到哪一等級，再根據需要調整投入的人手和資源。

協會副會長、香港寬頻持股管理人及信息安全總裁鄧宏舜表示，條例為網絡安全工作提供了一個基準，讓整個行情水漲船高，除了關鍵基礎設施領域外，也為其他行業提供了參考標準。「就算做不到十成，你做三成，都好過現在的不做。」

首4個月科技罪案逾萬宗 警籲對網上資訊「零信任」

香港文匯報訊（記者 黃子龍）「對網絡資訊要保持『零信任』，抱着懷疑態度，然後小心求證，才可安心進行網絡活動。」香港特區政府警務處網絡安全及科技罪案調查科總警司林焯豪昨日在接受香港文匯報訪問時表示，今年首4個月，警方錄得科技罪案數字超過10,100宗，數量與去年同期相若，損失金額卻明顯增多，根本原因是市民的防騙意識沒有相應提升。



◆林焯豪 香港文匯報記者黃子龍 攝

科技罪案數量近年呈上升趨勢，林焯豪回顧說，去年香港科技罪案數字約為3.4萬宗，較前年上升近五成，損失金額超過55億元。今年首4個月，警方錄得科技罪案數字超過10,100宗，數量與去年同期相若，損失金額卻明顯增多。

他指出，隨着全世界社會都進行數碼轉型，愈來愈多的犯罪分子亦把目光放在網絡世界，然而市民的防騙意識卻沒有相應提升，是科技罪案數量上升的根本原因。因此，對於網絡上五花八門的資訊，市民要保持「零信任」的態度，小心求證每個資訊背後的真確性，再進行下一步的網絡活動。

林焯豪表示，香港警務處網絡安全及科技罪案調查科今年初推出的防騙視伏App，已有48萬的下載量，希望日後有更多市民使用，從而加強市民的防範意識。該程式內含每日最新版本的詐騙資料庫，在手機中安裝程式後，當用戶收到可疑來電及瀏覽可疑網站時，程式會即時發出警示，提醒用戶切勿墮入陷阱，市民亦可在收到可疑電話或網站時，透過程式作出舉報，達至全城守網的效果。

業界倡增社企高層風險意識

香港文匯報訊（記者 胡恬恬）資料外洩危機處處，市民千萬不要覺得網絡保安「唔關我事」。中港網絡安全協會副會長、香港寬頻持股管理人及信息安全總裁鄧宏舜昨日在接受香港文匯報專訪時表示，一些社企和非政府組織（NGO）都會收集一些包括姓名、電話、捐款數額等個人數據資料，或是涉及一些弱勢社群、特殊群體的資料，這些資料更為敏感，一旦洩露，往往可能造成較大社會影響，建議加強對NGO和社企高層的風險意識。

「你無須洩露幾十萬的數據資料，但就算是一百幾十個，也會引起大眾敏感、疑慮，或令他們不開心。」鄧宏舜說，一些社企和NGO的重點工作在服務層面，對IT和相關安全不夠重視。現在面臨的主要問題是資料外洩，例如儲存資料的USB沒有加密等，此外也有一些黑客攻擊的網絡安全威脅。

釣魚演習逾四成社企員工中招

他舉例說，自己公司曾幫一些社企做釣魚電郵演習，由仿真度極高的電郵地址，向十間社企近1萬名員工發出釣魚電郵，結果有逾四成人點擊進入電郵中的假鏈接，更提交了敏感個人資料，反映這些員工的安全意識和風險防範意識還不足。

鄧宏舜建議加強對NGO和社企高層的風險意識，而網絡安全的教育和防範一定是從上到下。對機構或企業來說，無論是網絡攻擊還是詐騙，對上層的攻擊往往更有效，「我偷了你總幹事的電郵賬號， 可以假裝總幹事叫財務過數， 或是拿來騙錢或者什麼，所以一定是從上到下才有效。」

除了政府機構、私營企業、社企和NGO外，普通市民也應做好家居網絡保安工作，「不要覺得網絡保安與己無關，其實很多黑客攻擊都已自動化，不是看你有多少身家才攻擊你，普通市民也是他們的攻擊目標。」

鄧宏舜指出，很多市民家中安裝的攝像頭也有潛在安全風險，建議定期更新，定期修改家中WiFi密碼，注意密碼強度且不要透露任何個人信息。