【庖丁篇】— 刊於《經濟日報》，2021 年 9 月 16 日

個體缺風險意識　網絡騙案難杜絕

許佳龍
科大商學院資訊、商業統計及營運學系講座教授、
艾禮文家族商學教授

網上情緣騙案手法最近頻密發生，且手法層出不窮。日前，有從事專業行業的年青女事主，抵受不住自稱台灣 IT 男施展的甜言蜜語攻勢，放下戒心，聽從其指示，購買加密貨幣「泰達幣」（USDT），再匯到偽造網上賭博平台，參加疑似網上賭博，初可獲數百元回報，之後逐漸加大注碼，最終損失近 100 萬元，其中約一半更屬借貸。

據警方今年上半年的統計，網上情緣騙案大幅上升，由去年同期的 429 宗增加至 822 宗，上升 91.6%，損失金額超過二億八千八百萬，上升 1.6 倍；受害人通常經過一段長時間才發現受騙，致損失較大。除了網上情緣騙案，虛擬貨幣交易行騙和網絡商業犯罪的案件，近年也不斷增加。

疫情改變線上線下行為

很顯然，網上騙案近年趨多的原因有多端——

由於從 2019 年底新冠病毒肺炎（COVID 19）疫情大規模爆發，生產以及社交活動受到影響，在禁足外出、限聚令下以至「遠程工作」模式大規模應用的情況下，使用電腦的人和使用時間都較以往為多，上網的時間當然也更久；另一方面，過去習慣在線下的行為或交易活動，無論是自願或無奈地都多了在線上進行。

一些相對較高風險的交易行為，譬如投資買賣證券、商品甚至朋友之間的借貸活動，原本多傾向在線下進行交易，但在疫情下，過往線下的交易或行為模式，如今不少轉到線上進行。這樣改變帶來什麼影響，在疫情後這種改變情況是否持續，是值得注意的。

另一方面，互聯網科技近年的長足發展，包括人工智能等，這些技術使騙徒假扮成一個什麼身份、什麼樣子的「人」，都更輕易。在網上用一些技術做成與某

人同一個聲音，甚至打扮成跟電影裡主角相似的面孔，使得網上的資訊變得真假難分，似真還假，可信性很低。不過，往往又有人相信。

個體不慎 殃及別人

可以說，網絡保安的一個關鍵節點，是參與網上活動的人必須有高度警惕的意識；同一時間，要知道騙徒常用的行騙手法。從這些騙案看到，迄今仍然有大學生墮入「公安騙案」，把錢轉帳到一個不知是何人的銀行戶口；網上情緣的騙案，苦主把大筆金錢，存到只認識了幾個月「想像情侶」所指定的海外銀行戶口之中，這些重覆又重覆，不斷發生的騙案，居然還有不少人「中招」，委實令人感到「匪夷所思」。

問題的癥結在什麼地方？很顯然，雖然很多人上網，到處瀏覽，但他們所接觸的訊息和上網目的，往往只是玩遊戲或交友，沒有留意到社會發生的新聞。換言之，在上網的人群中，存在不少「無知的人」，成為騙徒狩獵成功的對象。

解決之道，通過對「無知網民」進行教育，提高其受騙的警惕，是其中有效的方法，但知易行難，因為「無知」的人往往以為自己「有知」，沒有把「忠告」放在心坎裡。譬如，一些存放了大量客戶訊息的企業，只因其內部個別員工的網絡保安意識不足，便釀成系統保安漏灑，讓黑客有可乘之機，入侵了公司的網絡系統，把客戶資料予取予攜，類似的案件屢見不鮮。

誠然，各國政府已愈來愈提倡推出一些保護網絡安全的措施，如金管局於 2016 年推出「網絡防衛計劃」，以提升香港銀行的網絡防衛能力，到去年 11 月，再推「網絡防衛計劃 2.0」版。這個計劃其中的「網絡防衛評估框架」（Cyber Resilience Assessment Framework），是一個以風險為本的框架，讓銀行根據這個框架，去評估本身的風險狀況，以定出適當防範網絡攻擊，需要採取的防禦措施。

分擔風險　分配責任

事實上，要求企業或機構進行風險「自我評估」，然後再作出防範風險的應對措施，這類網絡的保安措施和構思並非新鮮，而是沿用一直以來在商業世界裡的「風險管理」概念。從風險發現，評估，繼而作出應對管理。這是全球性的通行做法。

然而，潛在的風險在未發生前，往往未被保安系統辨識出來。譬如，異國情緣的因素，網絡保安系統就不容易事前發現出來、識別出來。可能只因機構內部一名員工，在網上交友過程警惕不足，一不小心，讓認識不深的網絡朋友製造了一個入侵公司電腦系統的缺口。因此，即使風險系統有辦法針對機構有多少個員工，有什麼服務產品，相對作出了一些保衛措施，但不能保証到公司每個員工，都有足夠對保安風險的認識，形成「防不勝防」的保安漏洞。

歸根究抵，網絡防衛的關鍵，在於用戶不清晰或不在意自身在網絡保安上的角色，對公司的電腦安全系統的保安意識也不足夠。筆者對網絡保安多年的研究，一直提倡機構不僅需要教育員工對互聯網保安的認知，還需要政府、機構以至僱員各方在網絡保安上的角色分配和風險分擔，而不是由一方來單獨應對。

「第三方」風險不容忽視

筆者對網絡保安曾提出過「第三方」風險的概念，即企業自身的網絡系統相當安全，但當這家企業增加了一些由外判供應商(第三方)提供的額外服務時，便可能從外而內引入了可能的潛在安全風險。一旦「第三方」的系統安全性出現漏洞，黑客便可以乘虛而入，順藤摸瓜，直闖企業的網絡系統。

另一方面，企業與企業之間、企業與用戶之間，以至用戶與用戶之間，大家互相勾連，這種千絲萬縷的網絡關係，使網絡保安無可避免帶有相互依賴的「集體性」，很難單靠一方獨力完成。因此，我們需要從責任分布的角度，去檢視網絡安全問題，令網絡安全得到更全面、更踏實的「整體性」維護。

很顯然，企業除了做足網絡安全的裝置和措施，還需要提出誘因，去激勵企業內員工做好自身保安付出和保安責任投入的部分。因為如果他們付出的部分不足，沒有切膚之痛，粗心大意，往往便會成為整個保安系統「致命」之處。出了事的員工，也需要負上責任。

溢出效應 害己害人

與此同時，網上的交易機構，對其他的持份者都會造成影響，如商業夥伴、供應商以至顧客，因為顧客用這家網上交易機構的網絡，都會為自身帶來網絡安全的風險，以銀行為例，過去也有銀行的資料庫為黑客入侵，被非法盜用，銀行當然有損失，但同時引伸一個經濟學上的「溢出效應」（Spillover Effect），這種負面的界外效應，造成各方都受損害，因此，網絡的保安，必須從一個寬

濶的角度來考慮，而不是由一方來應對安全風險，因為一方個體的不小心，會牽連到很多方面同受影響和損失。換言之，網絡保安是需要「整體性」的維護。通過教育，提高網絡用戶的風險意識；與此同時，在防禦網絡風險的責任分擔，合理分配，在損失後果共同承擔的基礎上，制訂一個全面的、集體性的防禦系統，相信才能有效管控網絡風險和攻擊的進一步肆虐。