香港仔
LION ROCK DAILY

Facebook

香港仔 LION ROCK DAILY

lionrockdaily香港仔 www.lionrockdaily.com | 2026.4.13 | 星期一

P.2 機械手可拆彈 亮相創科展

P.13 美封鎖海峽 伊派軍防入侵

■警方過往曾拘捕騙徒。 資料圖片

深偽技術增仿真度 針對受害人設計劇本

AI釣魚更逼真 去年騙款倍增

隨着人工智能（AI）的興起，不法之徒的騙局也變得更高智能。香港去年整體科技罪案宗數按年下跌約6.9%，但損失金額卻上升23.2%，其中滲透市民日常生活的「釣魚」騙案數字，跌幅約六成，惟損失金額增加逾一倍。警方發現，「釣魚」攻擊向三方面進化，包括騙徒以低成本網購「釣魚」套件配合自動化工具，大規模生成和發布海量詐騙短訊；針對受害人「量身訂造」個性化行騙「劇本」；利用AI「深偽技術」增強仿真度，更精準、更逼真行騙，令機構員工或市民防不勝防。去年就有一名會計員中招，令公司損失1,900萬元。

■警方呼籲市民提防釣魚短訊。

去年11月，一間公司會計職員收到一條WhatsApp短訊，騙徒假冒WhatsApp管理員聲稱系統更新，要求提供賬戶驗證訊息。事主按照指示輸入密碼，變相交出訪問權限，令騙徒洞悉賬戶所有對話，並冒充公司合作夥伴，用新手機號碼向事主發送訊息，訛稱收款賬戶已更改，並提供3個新的銀行賬戶，事主未經核實，分4次轉出合共1,900萬元。

警方網絡安全及科技罪案調查科署理高級警司許綺惠日前接受訪問時，分析「釣魚」騙案最新趨勢，她指出「釣魚」攻擊趨向更精準、更逼真、更難識別的方向發展。從香港整體網絡威脅形勢分析，去年針對香港的網絡威脅情報超過150萬宗，當中「釣魚」攻擊佔約27%，即平均每4宗威脅就有1宗涉及「釣魚」。

技術門檻降 可大規模攻擊

香港「釣魚」騙案報案從前年的2,731宗，下跌至去年的1,093宗，但損失金額則由前年約5,000萬元，升至去年的1.1億元。

警方觀察到「釣魚」攻擊已全面進化，主要集中在三方面：第一，規模化和自動化工具全面滲透。騙徒很容易從不同渠道獲取「釣魚」工具服務，降低技術門檻，令犯罪工具完全平台化，騙徒只需網購工具即可大規模發動攻擊，再配合自動化工具，可以全天候大規模生成詐騙內容，再經由短訊（SMS）、社交媒體或語音通話等多個管道滲透。據資料顯示，有一種「網絡釣魚即服務」平台，是黑客在暗網販售多樣化網釣套件與範本，提供一次性買斷或訂閱服務，騙徒能以低成本獲取技術，令近年來「釣魚」攻擊愈發頻繁及具威脅性。

第二是個人化包裝，現時愈來愈多人在社交媒體分享個人生活，令騙徒容易收集受害人背景而量身訂造「釣魚」訊息，令行騙內容更具說服力，騙取受害人的信任，精準偽裝不同政府機構、企業等，騙取賬號密碼或者信用卡資料。

第三是人工智能「深偽技術」，騙徒很容易在網上獲取「深偽」工具，製作仿冒圖片、聲音、畫面等，做到高仿真度模擬上司、同事、甚至是業務夥伴的聲音和樣貌直接誘騙。這些詐騙訊息透過AI驅動，在語氣和邏輯上，憑肉眼難分辨真假，令市民防不勝防。

「釣爾輕心」演習 高級職員頻中招

因應「釣魚」攻擊的不斷演變及高風險，警方由去年10月至今年1月，聯同香港互聯網註冊管理有限公司（HKIRC）及數字政策辦公室舉辦「『釣爾輕心』社交工程演習2025」，共有301間機構逾5萬人參與，目標透過模擬真實騙案情況，提升員工對「釣魚」攻擊的警覺性。結果可見，即使企業部署完善系統防護，攔截大量「釣魚」電郵，但只要有小量「釣魚」電郵順利進入員工收件箱，而且經理級或以上人員的超連結點擊率達15.5%，高於全體參加者13.4%的平均水平，但高級職員「中招」帶來的影響和損失可能更嚴重。

今次「釣爾輕心」演習，除涵蓋電郵渠道外，因應短訊是目前「釣魚」騙案最主要的犯案途徑，以及不少公司會為員工配備公務手提電話，所以新增「釣魚」短訊（SMS）演習。總體而言，「釣魚」電郵的超連結平均點擊率為13.4%，「釣魚」短訊的超連結點擊率為5.9%，雖然「釣魚」短訊的「中招」人數較少，但危險程度不容忽視。因短訊傳達更即時，日常接收數量多，易被忽視；另短訊內容簡潔，僅有數十到百餘字，難以辨認發送方真偽，也缺乏足夠資訊判斷是否為「釣魚」資訊。

編輯部：2873 8233 傳真：2552 6161 廣告部：2873 9888 3708 3888 發行中心：2873 9889 承印：三友印務有限公司 地址：香港仔田灣海旁道7號興偉中心2–3樓