卓永興：宏志閣居民料下月可再安排上樓執拾

●卓永興表示，已通知1,730多戶宏福苑居民上樓執拾。 香港文匯報記者郭木又 攝

香港文匯報訊（記者 李千尋）大埔宏福苑居民將於下周一（20日）起分批返回單位執拾。特區政府政務司副司長卓永興昨日表示，基本已接觸7座受波及樓宇的所有住戶，當中約98%確認會按政府安排的時段上樓，其餘少數會另行安排上樓日期。另有約380戶居民提出希望二次上樓，政府會在總結首輪安排經驗並掌握實際需求後，作出積極安排。至於未受大火波及的宏志閣，卓永興指政府「當然會記住宏志閣居民」，目標在5月內再安排上樓。

建議居民上樓前先作規劃

政府上月底公布，宏福苑7座樓宇居民將於本月20日至下月4日期間分批上樓。卓永興表示，約98%住戶回覆可按安排時段上樓，至於少數未能依安排上樓的住戶，政府會主動接觸並另作日期及時段安排。

他提醒，近日有不少團體表示會向上樓居民派發物資，建議居民上樓前先作規劃，盡量減少攜帶不必要物品，空出一對手，預留袋或背囊位置，執拾想帶走的物件。

卓永興指出，有約380戶居民希望有第二次上樓機會，但具體數字可能在首輪後有所變更，例如部分單位焚毀嚴重、可執拾物品不多，住戶未必需要第二次上樓；若單位未有直接受大火波及、可取回的物品較多，住戶或會想再上樓一次。即使住戶早前在「一戶一社工」跟進時未有提出，日後仍可再反映再上樓需要，政府會作積極安排。

卓永興續指，未受大火波及的宏志閣於去年12月初已安排過一次上樓，政府「當然會記住宏志閣居民」，目標在5月內安排再次上樓，相關安排與其他7座樓宇相若。

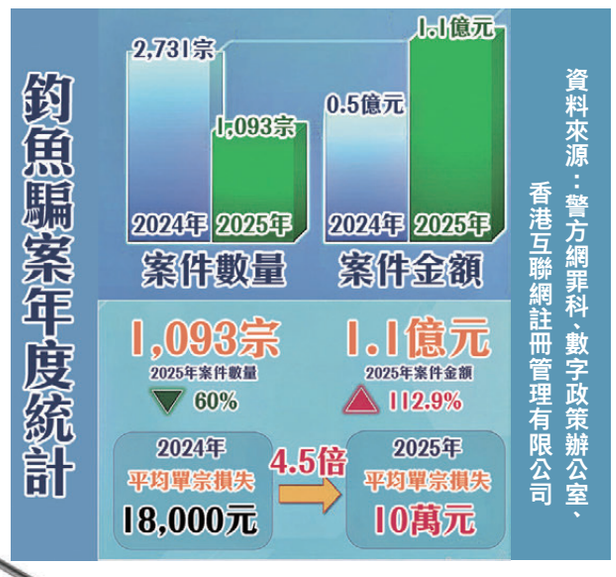
政府發言人補充，宏志閣屆時會有升降機供上樓的居民使用。

「釣魚」騙案肆虐 去年失財倍增

警方揭騙徒用AI三大進化：低成本個性化高仿真

水能載舟，亦能覆舟。隨着人工智能（AI）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，反映網絡罪案「貴精不貴多」，正向高度針對性、高度破壞力方向發展。警方分析發現，「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」；最後是利用人工智能「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。 ●香港文匯報記者 曾立本

●左起：警方網絡安全及科技罪案調查科總督察梁以德和署理高級警司許綺惠、香港互聯網註冊管理有限公司行政總裁黃家偉。 香港文匯報記者曾立本 攝



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，要求提供賬戶驗證信息。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。

每4宗網絡威脅有1宗涉「釣魚」

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「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」。

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，上升至去年的1.1億元。騙徒會設計「釣魚」連結引導受害人在假網站輸入證券戶口、網上銀行或信用卡登入資料以盜取更多款項，市民一旦登入「釣魚」連結便會「輸身家」。

暗網有販售多樣化「網釣套件」

警方觀察到「釣魚」攻擊已經全面進化，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進行大規模發動攻擊，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渠道滲透。

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。

蒐個人訊息量身訂造「釣魚訊息」

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、機構等，騙取賬號密碼或者信用卡資料。

用「深偽」工具模擬同事親友

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。

因為市民幾乎把所有的通訊和交易都集中在手機進行，短訊是最快最容易接觸用戶的渠道。去年「釣魚」騙案中「釣魚」短訊佔超過九成，「釣魚」電郵佔約2.6%，透過WhatsApp、Telegram、Messengers以及其他即時通訊軟件發放「釣魚」短訊佔6.5%。而用「釣魚」電郵或短訊行騙的手法都一樣，不過「釣魚」電郵往往涉及金額相對較大，因此市民對兩者都不能掉以輕心。

警方提醒市民，AI時代的騙案，已不再是騙徒「識唔識做」，而是可以做得「多快和多真」，市民一刻放鬆警惕，隨時被「釣爾輕心」損失金錢。

演習證高級職員較易中招

香港文匯報訊（記者 曾立本）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，即便企業部署完善系統防護，攔截大量「釣魚」電郵，只要有少量「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為嚴重。

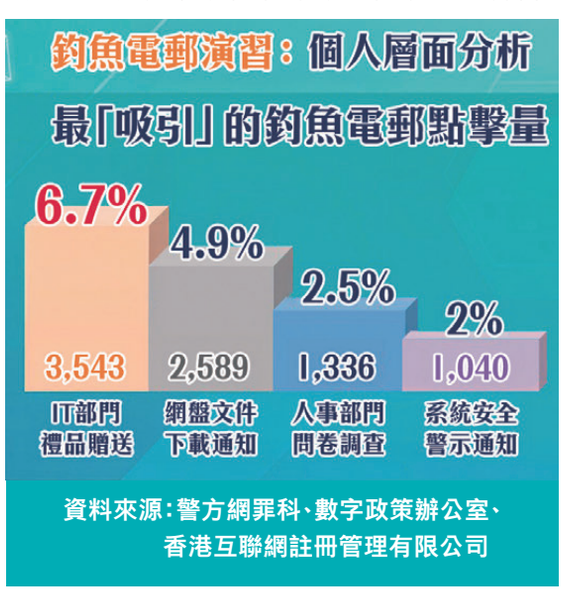
警續用科技及跨界合作提供防護

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。

總結而言，「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。

網絡安全及科技罪案調查科總督察梁以德表示，要有效打擊「釣魚」騙案，各界必須要通力合作才可發揮最大成效。警方一直積極和各持份者致力防騙工作，達到一加一大於二的協同效應；其中包括匯集逾130個來自政府、銀行、電訊商和科技公司的守網者聯盟，以及「守網者」和香港互聯網註冊管理有限公司的「網絡安全員工培訓平台」，剖析最新騙案手法，幫助市民迅速掌握資訊及早防範。

另去年10月，警方推出全新AI+升級版「防騙視伏App」，更新公眾舉報平台，結合人工智能的分析技術，能即時分析市民舉報的情報，自動評估風險及納入資料庫，並按風險程度用黃色或橙色作初步標示；經人工覆檢確認後，高風險項目就會升級為紅色。平台還新增詐騙手法排行榜，每日統計最新的罪案趨勢，自動整理出全港最流行的詐騙手法。總括而言，警方將持續運用科技及跨界別協作平台，為市民提供更全面、更主動的安全防護。



「上傳個人資料」較謹慎 「下載文件」欠警覺

香港文匯報訊（記者 曾立本）香港互聯網註冊管理有限公司行政總裁黃家偉表示，今次「釣魚」電郵演習，模擬參加者收到「IT部門禮品贈送」、「網盤文件下載通知」、「人事部門問卷調查」及「系統安全警示通知」等為主題的「釣魚」電郵。結果顯示，有7,121名參加者（約13.4%）至少點擊其中一封電郵內的超連結。

黃家偉續說，當中以「IT部門禮品贈送」最多人點擊開啟，有3,543人中招，其中約1,500人更上傳個人資料；其次為「網盤文件下載通知」，有2,589人點擊，其中約1,600人進行下載操作，人數超過點擊率一半，估計員工對「上傳個人資料」相對謹慎，但對「下載文件」警惕性較低。事實上，一旦點擊可疑超連結下載文件，可能導致賬戶資料外洩或電腦被惡意軟件入侵。

今次新增的「釣魚」短訊（SMS）演練，共有30間機構共3,620名使用公司配發公務手機的員工參與，分別收到「系統維護更新」、「員工資料驗證」及「新春禮券贈送」共3條含可疑超連結的短訊。結果顯示，有214人（5.9%）至少點擊一條超連結。

四招防範釣魚騙案

第一，保持警覺，切勿隨意輸入資料。任何突如其來的電郵或短訊，例如要求更新賬戶、重設密碼、領取獎賞或退款，都應該先存疑。即使對方聲稱來自銀行、政府部門，甚至同事，都有可能是假冒。在未經核實之前，切勿輸入任何敏感資料，包括密碼、信用卡資料、驗證碼或公司賬戶資料。

第二，勿隨意點擊連結或下載附件，可以先查看網址，但不要點擊；不明附件更加不應該開啟。

第三，留意網址真偽。釣魚網站往往和真網站只差一兩個字，例如拼寫錯誤或異常域名。如需登入服務，應直接輸入官方網址。

第四，務必核實身份。只要涉及金錢或敏感資料，必須透過官方渠道，例如致電銀行或直接聯絡相關人士確認。雖然騙徒手法不時更新，但市民只要不掉以輕心，做到「一停、二諗、三核實」，就不會被騙徒「釣」中。

資料來源：警務處