網絡釣魚五類陷阱大破解

首4月相關騙案339宗涉款逾3億 香港文匯報記者整理警方案例解讀手法

在互聯網時代，特別是在新冠疫情影響下，市民依賴手機或電腦代替實體交易，已經成為生活不可分割的部分，不過，全球面臨電訊和網上詐騙的嚴重威脅，香港也難獨善其身。其中「網絡釣魚攻擊」騙案屢爆不絕，騙徒利用黑客高端技術，以隱藏的域名偽裝在不同地區，發放附帶有惡意連結、二維碼的釣魚電郵或短訊等，並應用於各類不同場景的騙案中，市民稍不留神，一旦開啟連結，便會令手機和電腦中門大開，被植入木馬程式後，所有網上交易都「裸露」給騙徒，繼而個人賬戶甚至連累公司賬戶被「騎劫」。今年首4個月香港警方接獲的報案中，「釣魚攻擊」騙案就有339宗，被騙市民損失金額約佔整體科技罪案10億港元的三分之一。今年5月至8月是警隊防騙宣傳季，香港文匯報記者根據警方講解的案例，整理和拆解五大「釣魚」陷阱。

◆香港文匯報記者 杜傑

「網絡釣魚攻擊」(今年首4個月)

類別	宗數	損失
電郵	127宗	3.3億元
短訊	135宗	470萬元
語音	77宗	90萬元

資料來源：香港警方

近年釣魚電郵騙案

時間	宗數(與上一年比較)	損失金額(與上一年比較)
2021年	549(–28.3%)	15.4億元(–31.5%)
2020年	767(–6%)	22.5億元(–11%)
2019年	816(–8.7%)	25.3億元(+48%)
2018年	894(+29%)	17.2億元(+73%)

資料來源：香港警方

防「釣」貼士

- ◆不要開啓來歷不明的郵件
- ◆切勿點擊可疑電郵內的超連結
- ◆查看清楚寄件者資料
- ◆切勿登入未經查證的網站
- ◆如網站要求提供個人或信用卡資料，應加倍小心
- ◆如懷疑受騙，應致電「防騙易」熱線18222查詢或報案

資料來源：香港警方

釣魚短訊

假短訊拎包裹 盜走銀行存款

如今手機用量已經超越個人電腦，使騙徒取得手機號碼及電郵地址更容易，故此黑客亦轉用此平台盜竊個人資料。他們會發出「釣魚短訊」給用戶，同樣附帶一個有惡意軟件的連結，而短訊的內容會視乎不同情況而有變化，但關鍵是短訊內的連結，市民一旦打開便步入陷阱。例如，時下正值疫情肆虐，購物速遞服務倍增，騙徒會冒充速遞公司包括「香港郵政」，向市民發出附有不明連結的釣魚式短訊（SMS），在短訊中訛稱受害人的包裹運送受阻，要求受害人登入連結，再輸入個人和銀行資料以繳交附加費用，然而受害人的資料全被騙徒一覽無遺，結果被盜走銀行存款。

今年首4個月，警方接獲135宗涉及假冒郵遞服務騙案，與去年同期的132宗相若，但損失金額卻增加1.3倍，由去年的208萬港元，上升到今年首4個月多達470萬港元。也有騙徒偽冒電子支付平台，向市民發出釣魚短訊，聲稱有現金禮物，誘使市民點擊連結提供手機號碼、一次性「驗證碼」及「交易密碼」等資料，繼而控制其電子錢包賬戶轉走存款。

釣魚電郵

木馬病毒「入腦」操控公司資料

今年首4個月警方接獲127宗「釣魚電郵」騙案報案，當中102宗涉商業及25宗涉個人，合共損失3.3億港元，顯示商業機構為最大受害者，而黑客和騙徒入侵商業機構電腦系統的途徑主要有兩個。其中一個途徑是向公司發出有惡意超連結的電郵，以釣魚軟件取得登錄權限，然後入侵公司或其商業夥伴的電郵系統，從而窺視所有往來電郵內容，從而掌握公司管理層、職員及生意往來等秘密，然後假冒客戶或公司高層，佯稱收款銀行戶口更改，要求職員匯款。

另一個途徑是，疫情下很多公司實施家中工作，若職員的私人電腦保安不足，例如未安裝防毒軟件、防火牆和定時更改密碼，當開啟個人電郵和假網頁的惡意連結，私人電腦有機會被「騎劫」，當職員利用遠端程式進入公司電腦，就會令黑客借機將木馬病毒植入公司電腦獲取資料，再行騙。

早前，一間美資投資公司員工收到假冒公司客戶的電郵，要求匯款960萬美元（約7,500萬港元）購買兩個新加坡物業，職員不虞有詐，結果由去年12月至今年1月，共分4次將金錢存到騙徒指定的兩個本港銀行戶口。

◆騙徒會以接近假冒公司名稱發放郵件，欺詐員工上釣。 資料圖片

釣魚語音

助登記消費券 若回覆墮騙局

語音釣魚攻擊是網絡釣魚的電話版，騙徒通過網絡語音電話偽造來電號碼或假冒自動語音系統，通常冒充政府機構、銀行或電子支付平台，然後利用撥號軟件發出自動撥號，電話騙徒假扮銀行或電子支付平台職員，謊稱用戶的賬號出現異常，或協助登記政府電子消費券等理由，要求用戶致電解決問題。假如用戶致電回覆，騙徒便要求對方提供交易密碼及一次性驗證碼，從而騎劫用戶賬號盜款。有時騙徒也在預錄語音信息中附帶超連結，要求客戶輸入個人資料。

「釣魚語音」騙案的前提，是騙徒由非法途徑或其他釣魚攻擊中，非法盜取了受害人的姓名、身份證等基本資料，能說出受害人名稱等，增加行騙場景的說服力，也最容易令市民中伏。而利用「釣魚語音」冒充電子支付平台的騙案，在去年5月首次發現，至去年底警方共接到270宗報案，損失330萬港元，而今年首4個月則有77宗，損失90萬港元。

虛假網站

設網站扮商戶 登入即遭「偷料」

騙徒模仿商戶官方網站建立假網站，目的是要以假亂真，竊取用戶的登錄憑證或敏感資料，當中最常見的是銀行假網站。黑客一般通過有惡意軟件的假網站，或在用戶的電腦上安裝惡意軟件，以修改電腦內部設置的網域名稱解析文件，用戶連接到惡意網站，最終目的是套取用戶資料，盜走存款。

另一方面，黑客利用網民喜歡用網上搜尋器查資料的新常態和習慣，即不用Bookmark（標註）搜尋，而在搜尋器上直接打關鍵字搜索，黑客用大數據分析出多人搜尋的網站，再相應地製作附有惡意軟件的假網站，並置於搜尋榜的前列位置「博大霧」，令網民搜尋所需網站時更容易登入假網站而被釣魚攻擊，遭黑客入侵電腦盜取資料。

首季揭806釣魚假網站

據香港電腦保安事故協調中心資料，今年第一季報告已發現806個釣魚假網站，較去年同期495宗上升約六成。香港互聯網註冊管理有限公司網絡安全經理林嘉棋指，憂慮網民使用電腦習慣的新常態，增加被黑客利用惡意軟件入侵的風險。此外有市民進入惡意網站後，明知附有惡意程式卻甚少舉報，只會即時關閉網站，而自己電腦的密碼亦沒有更改，結果使黑客輕易入侵電腦，將電腦內的資料完全裸露，亦因未及時舉報，令該存有病毒的假網站繼續留存禍害他人。

虛假手機應用程式

冒官員促裝App 女秘書失財671萬

騙徒在假冒官員的電話騙案中，同時使用有釣魚軟件的虛假手機應用程式，以套取受害人的銀行賬戶資料，騎劫賬戶轉走金錢。在電話騙案中，有時騙徒針對市民的防騙意識，不會直接叫受害人說出交易密碼，而是誘使受害人下載一個手機應用程式。因虛假程式不能在官方商店上架，騙徒會詢問受害人是使用iOS或Android系統，繼而引導事主下載和安裝假應用程式。假如事主使用iOS系統的手機，騙徒或會要求事主先安裝Testflight程式測試工具，再安裝假應用程式，以繞過官方審核，或要求事主直接購買Android系統的手機，並透過非官方渠道下載假應用程式。

在今年首季，單一損失最大的電騙案中就涉及裝有木馬程式的假手機應用程式。例如，一名43歲公司女秘書接到假冒官員的電話，指她登記的內地手機應用軟件涉及販賣假新冠肺炎疫苗案，又指她洗黑錢，佯稱會凍結其賬戶作調查，其後騙徒指由於案件屬高度機密，需女秘書下載一個手機應用程式去監控其有否與其他可疑人聯絡，並附上相關下載連結。

至翌日，騙徒再稱需要調查其公司賬戶，指示事主將公司所有銀行賬戶的資金都轉賬到事主個人銀行戶口，事主不虞有詐照辦，其實騙徒也利用事主下載的假手機應用程式洞悉其賬戶資料，並盜走671萬港元。當騙徒再指示事主加碼238萬元作保證金時，事主因已掏空公司資產及擔心公司賬戶被凍結，於是致電相關銀行查詢始知受騙。

警方網絡安全及科技罪案調查科指出，黑客和騙徒都是取易不取難，要預防被黑客入侵，市民除了不要點擊可疑電郵連結外，在公司或家中也要做好安全措施，包括經常將資料備份、設定高強度密碼、安裝防惡意軟件，並須定時更新、開啟防火牆、使用雙重驗證等。此外，亦不要胡亂在網上下載軟件，以及要提升員工對不明來歷電郵的警覺性，尤其遇到要求提供個人資料或轉賬的電郵須加倍小心，要核實有關的電郵真確性。

反映公司防「釣」意識不足

釣魚電郵演習八成中招

香港文匯報訊（記者 杜傑）警方網絡安全及科技罪案調查科為提醒政府及商業機構員工小心網絡釣魚攻擊，繼去年進行首次「釣魚電郵演習」後，今年4月再邀請61間公司合共3,175名員工參加，經約一個月測試後，發現仍有八成共48間公司中招，以及三成半共1,099名員工曾至少點擊釣魚電郵一次。警方及網絡專家日前講解網絡詐騙新趨勢及演習結果時表示，演習反映公司員工對釣魚郵件的敏感度及警覺性依然不足，若電腦受惡意軟件感染，黑客可藉漏洞入侵整間公司的網絡，若公司未有做好保安措施，後果十分嚴重。

拎包裹最多人「上鈎」

網罪科總督察葉卓譽指出，演習中曾向各公司發出5封模擬釣魚電郵，包括包裹領取通知、稅務問題、雲端儲存續期、銀行指示通知及軟件啟用通知，結果發現最多人「上鈎」的是包裹領取通知共佔20.4%，其次稅務問題有15.9%，其餘3項則由6%至11%不等，另統計又顯示有353人即佔32%的員工開啟多於一封電郵。

葉卓譽續指，今年演習中的點擊率與去年情況相若，平均是12.5%，而外國同類釣魚演習點擊率為17.8%。但他強調，一間公司只要有一名員工的電腦受惡意軟件感染，黑客便可藉漏洞入侵整間公司的網絡。

網罪科警司范俊業亦表示，根據國際網絡安全機構調查報告指出，在2021年共有83%受訪企業曾遭釣魚電郵攻擊，較2020年的57%有明顯上升。另外，亦有其它相關網絡安全調查發現，有65%網絡安全從業員認同電郵是導致企業數據外洩的最危險渠道，當中有一定數量的資料外洩是由於員工在使用電郵溝通時警覺性不足所致。

◆警方網罪科連同網絡安全專家講解「網絡釣魚攻擊」的最新趨勢，提醒企業員工要加倍小心可疑電郵，提高警覺性。 香港文匯報記者 攝