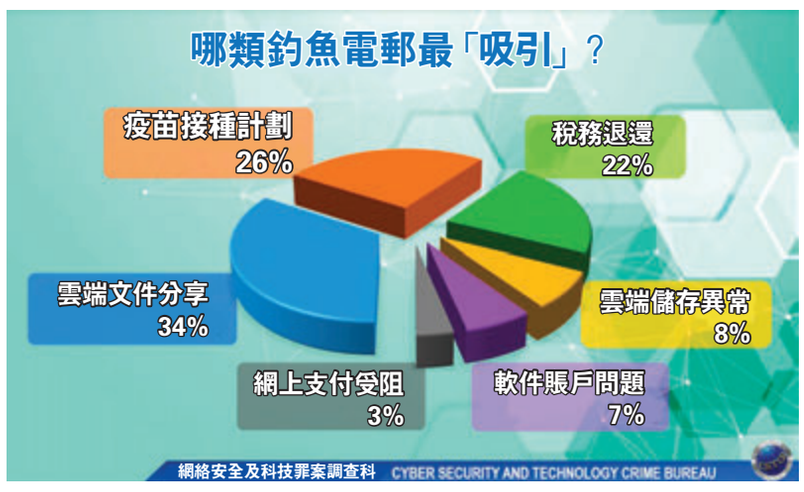
釣魚電郵去年呃逾22.5億元

網罪科演習揭近七成公司有職員中招 反映市民網絡安全意識不足

隨着個人生活及企業營運愈趨數碼化，電郵騙案肆虐全球。黑客覷準新冠肺炎疫情下，市民需家居工作而使用個人電腦連接公司網絡的保安漏洞，以不同主題作掩飾發送釣魚電郵，誘使點擊惡意軟件的連結或附件，從而入侵公司網絡竊取貿易往來及生意夥伴等機密資料，再以假冒電郵要求公司將款項轉入傀儡戶口，以致去年警方共錄得767宗電郵騙案，損失金額近22.5億元。警方為提升大眾對可疑電郵的敏感度，今年4月網罪科首次與商界進行釣魚電郵演習，邀請46間不同界別公司共1,388人參加，結果顯示近70%公司有職員中招，反映市民網絡安全意識不足。

●香港文匯報記者 蕭景源

●警方聯同業界公布釣魚電郵演習結果，希望透過演習提高大眾網絡安全保安意識。 香港文匯報記者 攝



上年度香港警方共錄得767宗電郵騙案，損失金額共22.474億元，佔整體科技罪案損失的76.5%。當中最大一宗商業電郵騙案，事主來自一間位於美國的日本銀行分行，黑客假冒與該銀行早前達成貸款協議的商業夥伴，欺騙銀行職員將3.14億元貸款，轉至香港5個銀行的傀儡戶口。

網絡釣魚攻擊年升35%

另上年度受疫情影響，市民普遍因家居工作而增加使用個人電腦，黑客亦趁機以漁翁撒網方式，發放載有惡意連結或惡意附件的釣魚電郵，市民一旦點擊連結便會中招，甚至被黑客透過個人電腦入侵公司網絡竊取機密資料。根據香港電腦保安事故協調中心發表報告，網絡釣魚攻擊的數字，由前年2,587宗上升至去年3,483宗，按年急升35%。

今年第一季，警方亦已接獲145宗電郵騙案，損失金額共4.828億元，佔整體科技罪案損失額約61%，平均每宗案件損失330萬元。

銀行金融業最醒 僅7.8%人中招

警方為提升大眾對分辨可疑電郵的敏感度，今年4月網罪科聯同香港總商會舉辦釣魚電郵演習，邀請46間來自銀行、金融、交通、物流等企業，合共1,388人參與。參加者在獲預先通知下，於一個月內收到6封不同主題的模擬釣魚電郵，包括雲端文件分享、疫苗接種計劃及稅務退還等熱門主題，當參加者點入有關釣魚電郵的連結或附件，便會被視為遭到攻擊中招。

演習結果顯示，169人至少打開一封釣魚電郵的連結或附件，即12%參加者中招，比率與外國的同類演習結果相若。若以公司計算，則有32間公司至少一名員工，曾打開至少一封釣魚電郵連結或附件，佔46間參加公司近70%。而在測試結果中，以銀行業及金融業的參加者最為機警，只有7.8%參加者中招，遠低於其他行業。

演習結果為本地網絡安全響起警號，因為當員工電腦受到惡意軟件的感染，黑客可藉着漏洞入侵公司網絡，後果可以是非常嚴重。近期警方發現，有黑客將惡意軟件化身成PDF文件檔案透過釣魚電郵散播，用戶一旦打開文件便會受感染，被竊取瀏覽器的密碼、鍵盤打字記錄，甚至被黑客透過遠端控制電腦等。不過，在169名中招參加者中，有29人開啟多過一封釣魚電郵的連結或附件，顯示他們需要提升網絡安全意識。

能源及醫療業網絡攻擊趨增

網絡安全及科技罪案調查科網絡安全組警司范俊業提醒，市民不要以為黑客只會集中攻擊跨國企業或特定行業，根據外國資料顯示，近期黑客開始對不同行業進行網絡攻擊，其中以能源及醫療業的網絡攻擊有明顯上升趨勢，個人或公司必須加強網絡保安意識及措施，才能有效防止墮入網絡攻擊陷阱。

釣魚電郵演習結果

參與公司數目	46間
參加者數目	1,388人
點擊釣魚電郵人數及百分比	169人或12%(有29人開啓多於一封釣魚電郵的連結或附件)
點擊釣魚電郵公司數目及百分比	32間或70%(至少一名員工點擊釣魚電郵)

參加者中招主題點擊率分布

主題	點擊率
雲端文件分享	34%
疫苗接種計劃	26%
稅務退還	22%
雲端儲存異常	8%
軟件賬戶問題	7%
網上支付受阻	3%

疫下家居工作增 風險更高

香港文匯報訊（記者 蕭景源）黑客趁新冠肺炎疫情肆虐全球，居家工作盛行，去年展開全球性大規模網絡進擊，攻擊企業伺服器及發出含有惡意程式附件電郵，均以倍數激增。但有電腦安全公司在香港進行問卷調查及網絡安全課程發現，多達73%受訪者從未接受過網絡安全相關的培訓，90%公司員工在網絡安全課程中答錯網絡安全問題，反映潛在嚴重網絡安全漏洞。

卡巴斯基實驗室香港及澳門區區域經理張國保表示，受新冠肺炎影響市民居家工作情況普遍，但去年4月他們在香港進行一項問卷調查發現，需要家居工作的受訪者中，73%人從未接受過網絡安全相關的培訓、42%的人會使用私人郵箱處理公司電郵或文件、38%的人會使用個人即時通訊軟件與商業夥伴聯絡、53%的人會使用未經公司電腦部門審批的網上文件分享(file Share)工具進行工作。

90%員工答錯網絡保安問題

張國保續說，在他們提供的網絡安全課程中，發現90%公司員工曾答錯至少一條問題，反映很多人不知道自己以為正確的選擇其實是錯，造成網絡安全漏洞。當員工家居工作，便增加即時軟件溝通，令不慎將惡意軟件下載及散播傳開的情況有所上升，但同時員工又使用慣常與朋友網上聯絡方法處理公司文件，若公司的伺服器開啟「遠程桌面協議(RDP)」，但缺乏適當網絡保安，便很容易被黑客直接攻陷伺服器。

根據資料，去年1月至11月全球共發生多達33億次黑客直接攻擊公司伺服器，較前年同期9.69億次增長241%。另去年同期，他們共偵測到166萬個不同的惡意文件，偽裝成時下流行的即時通訊或視訊軟件發放；但今年第一季，已偵測到全球逾3,800萬封電郵含有惡意程式的附件，若個人網絡安全意識及公司網絡保安措施不足，容易被黑客有機可乘。

個人提防釣魚電郵騙案貼士

i)不要開啟來歷不明的郵件
ii)查看清楚寄件者的資料
iii)切勿點擊可疑電郵或訊息內的超連結
iv)切勿登入未經查證的網站
v)如網站要求提供個人或信用卡資料，應加倍小心
vi)如懷疑受騙，應保存相關電郵或訊息，並盡快致電18222或報警求助

公司提防假冒電郵騙案貼士

i)加強公司網絡保安措施防止被入侵
ii)公司透過電郵貿易往來時，小心查證電郵眞僞
iii)留意生意合作夥伴電郵地址與過往地址有否偏差，如英文「l」變成數目字「1」
iv)根據電郵標頭了解發出地區與相關公司所在地點是否有出入
v)生意合作夥伴突然電郵通知轉用新銀行戶口時，便應有所警惕
vi)留意生意合作夥伴電郵的語法及語氣有否改變
vii)當發現有任何懷疑時，直接致電對方核實

滬公司中招數月始揭發 損失980萬美元

香港文匯報訊（記者 蕭景源）釣魚電郵專以商界為攻擊目標，商業層面「遇襲率」佔整體高達86.2%，黑客一般會將釣魚電郵假冒成公司慣常往來的電郵發送，當職員點擊便會中招，黑客藉機入侵公司網絡封鎖檔案、竊取客戶及商業敏感資料，從而勒索檔案開鎖費、出售商業敏感資料、勒索或詐騙公司客戶等，進行二重或三重犯案。

警方資料顯示，去年10月上海一間汽車零件公司，疑有職員誤中釣魚電郵導致公司貿易往來資料被竊，黑客假冒公司的美國供應商發電郵聲稱提供低匯率兌換方案，黑客甚至發送偽冒有供應商副總裁簽名的電郵，成功騙得公司分7次將合共980萬美元（約7,640萬港元）存至香港銀行傀儡戶口。直至今年1月，公司發覺可疑致電對方查詢始揭發案件。

黑客複製銀行電郵掩飾

香港總商會數碼、資訊及電訊委員會副主席黃玉娟表示，商界最普遍遇到的網絡攻擊，是假扮滙豐、中銀或渣打等非常熟悉的銀行電郵，黑客會複製銀行與公司慣常往來信息作掩飾，容易令人放下戒心。但其實在電郵中加入一條「link」（連結），聲稱是「更新」或「新資料」要求點擊入內查看，職員一旦點入便「中招」。

她強調，即使職員只是處理私人電郵賬戶，但只要是使用公司網絡開啟，黑客也能透過職員私人電郵賬戶而入侵公司網絡。

近期總商會接獲數宗涉會員公司遇到網絡攻擊個案，有黑客假扮公司使用「Microsoft 360」的電郵，以版本需要升級為藉口，要求點入電郵內的連結，中招後被黑客竊取公司電腦內所有資料，包括貿易情況及與供應商等往來資料。

黑客根據取得的資料假冒公司或供應商，再向有生意往來的公司發出發票或單據，佯稱公司已轉換銀行，要求將交易款項存入新的銀行賬戶進行詐騙，甚至封鎖公司檔案勒索金錢，幸公司檔案本身有備份，黑客無法得逞。

警方亦強調，不建議公司向黑客支付任何金錢，因為此舉變相鼓勵黑客繼續犯案，特別是近期波幅非常大的加密貨幣，如果事主以加密貨幣支付勒索費，會令警方攔截及追查的難度非常高。

「老作」遭3警圍毆案 巴裔律師准保釋

香港文匯報訊（記者 蕭景源）一名42歲巴基斯坦裔律師，去年11月進入尖沙咀警署代表另一名涉嫌販毒的巴籍同鄉後，投訴其在警署內被警員辱罵、恐嚇，以及在升降機內被3名警員襲擊。警方調查後發現與事實不符，早前控告該律師誤導警務人員，案件昨在東區法院首次提堂，被告暫時毋須答辯，裁判官鄭紀航批准將案件押後至7月29日再訊，以待控方索取文件及法律意見。被告獲准以2,000元保釋。

巴基斯坦裔男被告周祖樑（42歲），為執業事務律師，涉嫌於2020年12月3日在香港灣仔軍器廠街3號堅偉樓附翼地下投訴課警察報案中心1號會面室，在明知情況下提供虛假資料或作出虛假的陳述或指控，以誤導處理該宗投訴的警務人員，即警長34229。

據悉，被告來港9年，持有香港身份證，任事務律師逾5年。他去年11月24日到尖沙咀警署代表一名涉嫌販毒被捕的巴基斯坦籍男子，其後他向投訴警察課及香港律師會投訴在警署內被「不禮貌對待」，包括被警員辱罵、恐嚇、襲擊等。

據悉警方在收到投訴人投訴後向他錄取口供，投訴人仍堅稱在電梯內曾被3名警員襲擊。其後警方亦收到香港律師會來信，要求對事件展開調查。投訴警察課警員在翻看相關閉路電視，及向當日有關警務人員錄取口供後，發現在升降機內並無發生投訴人所聲稱的襲擊，警員全程與事主均無任何身體接觸，懷疑有人說謊「屈警」。警方在取得律政司意見後，於5月25日以涉嫌「誤導警務人員」罪將周祖樑拘捕。

空頭支票呃二手車 主腦情侶被捕

香港文匯報訊（記者 蕭景源）警方在元朗破獲一個專騙二手車的黑社會詐騙集團，成功追回10輛失車。該集團於網上平台接觸出售廉價二手車車主，以空頭支票騙取車輛及牌簿後，再以低價轉售給二手車中介套利。集團更在有關車輛轉手前，肆無忌憚駕駛騙來的失車四處耍樂或作違法勾當，包括加油或進出停車場時拒絕付費不顧而去，終驚動警方調查，發現有關拒絕付費案涉及4月至5月全港13宗總值約58萬元的失車案，並在上周五（5月28日）在天水圍等多區一舉拘捕6人。

被捕的4男2女（21歲至38歲），當中包括屬該集團主腦的一對情侶，6人分別報稱無業、任職廚師及侍應等，4名男疑犯均有三合會背景，其中主腦情侶早前已被控以「以欺詐手段取得財產」提堂，其餘人則涉嫌串謀詐騙、盜竊、及不付款而離去等罪名被扣查。行動中除起回10輛失車外，另有大量空頭支票、車輛文件及少量毒品等。警方正設法追查另外3輛失車下落，至於多宗不付款離去案共涉約5,000元。警方呼籲有類似遭遇的失車車主盡快與元朗警署重案組聯絡，電話3661 4643。