香港仔
LION ROCK DAILY
Facebook
lionrockdaily香港仔 www.lionrockdaily.com 2024.2.2 | 星期五

P.2 工作符「468」擬享僱員福利
P.5 美斯訪港追星攻略

網絡釣魚騙案按年增三成 專家籲減社交平台分享個人特徵

AI武器化 換臉扮聲詐騙

■香港電腦保安事故協調中心昨公布資訊保安預測。

電腦黑客及網絡騙徒無處不在，香港電腦保安事故協調中心去年全年就處理7,752宗保安事故，其中網絡釣魚案件佔整體一半，個案宗數按年升近三成，為近5年新高。中心昨日分析，AI（人工智能）「武器化」將成為今年重點保安風險之一，騙徒可能利用AI換臉技術仿冒事主身份，並透過社交媒體向賬戶持有人的親友騙取金錢，建議市民減少在社交網絡分享個人身份特徵；收到可疑訊息時，可利用不同渠道確認發送人身份，平時謹慎上傳帶有正面面容和聲音的影像到社交平台。

香港電腦保安事故協調中心（HKCERT）昨日舉行簡報會，公布去年香港資訊保安狀況及今年資訊保安預測。去年中心共處理7,700多宗電腦保安事故，按年微跌8%，但釣魚攻擊類別個案明顯增加，主要攻擊涉及交易、支付行為的行業，依次是銀行、金融及電子支付行業（佔37%），電子商貿（18%），加密貨幣（11%），科技（11%）以及公共服務（7%）。

展望今年的重點保安風險，中心預測人工智能「武器化」，新一代釣魚攻擊，網絡犯罪趨向組織化，針對智能設備的攻擊，以及使用第三方服務，是五大保安風險。

生產力局數碼轉型部總經理兼HKCERT發言人陳仲文表示，AI技術近年應用越發廣泛，不僅有傳統網絡公司使用AI編寫程式，黑客也會利用AI生成惡意軟件，「AI降低成為黑客的技術門檻。」他舉例指，黑客可利用生成式人工智能下達指令，產生惡意程式碼，主導大規模的網絡攻擊；黑客亦可運用人工智能產生欺詐數據，影響其他人工智能的輸出，癱瘓網絡保安措施。

值得留意的是，黑客還可能使用AI「深偽」（Deepfake）技術製作虛假影片仿冒身份，在社交平台騙取受害人信任，進而騙取金錢。同時黑客利用搜尋引擎的優化功能，令與官網域名拼寫類似的釣魚網站位列搜尋結果前列，混淆視聽，用戶很容易誤登假冒網站。

為展示「深偽」技術的「高明」，陳仲文昨播放一段中心製作的換臉影片，他在片中分別以青少年、中年人及老者的形態出現，作出張口，四面張望等表情，換臉人物表現與真人非常類似。陳仲文表示，雖然AI會被黑客利用，但相信各行各業並不會就此停止AI應用，只能在應用前先理解及平衡網絡安全風險。深偽技術亦並非完美，例如換臉者用手部遮擋部分面容時，AI會難以識別及仿冒，建議市民在收到可疑視訊時，可要求對方做出類似動作，亦可使用其他渠道聯絡對方，以確認身份。

陳仲文續指，依照目前技術，偽造聲音難度高於面容，需要較大量的素材才能生成近似原聲的效果，故建議市民盡量不要上傳帶有聲音或正面面容的影像至社交平台。

入侵電腦刪檔 慎防加密病毒

另外，專業資訊保安協會副主席兼HKCERT關鍵基礎設施網絡保安通報計劃小組代表黃詩銘，就分享LockBit勒索軟件分析及預防措施。他指LockBit勒索軟件是全球部署最廣泛的勒索軟件變種，又被稱為「加密病毒」，電腦一旦被該網絡病毒入侵，檔案可能會被黑客盜取，同時本機的檔案備份亦會被刪除，用家無法使用之餘，還要面對黑客公開檔案的威脅，許多受害人最終只能無奈接受黑客勒索，支付贖金。

數碼港和消委會去年8月及9月分別遭黑客入侵電腦系統竊走大量資料，其中數碼港被盜取逾400GB資料，黑客組織事後將資料放上暗網拍賣，底價30萬美元（約234萬港元），資料包括近170名數碼港員工及前員工資料；而消委會亦確認近八成系統受破壞，數據被盜，事後向所有可能受影響的高風險者共發出約2.5萬份提醒通知，包括訂戶、員工、前員工、曾參與消委會投票者、合作機構，包括700間學校等。

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