康文署系統接連甩漏　輸入隊員「別名」 同名全顯示

SmartPLAY再揭私隱外洩風險

斥資5億元開發的智能康體服務預訂系統SmartPLAY，自本月9日啟用以來，接連出現甩漏，近日再被揭發系統有資料外洩風險。香港文匯報記者昨日凌晨實測，用戶只要於團隊成員「別名」一欄輸入常見的人名，如Alan或Ben等，系統便會把資料庫內其他曾使用該「別名」用戶的中文全名顯示出來，使SmartPLAY用戶的資料曝露予陌生人。事件被揭露後，昨午起系統已作修訂以堵塞漏洞。康文署回應指，已要求承辦商修改程式，停止顯示「團隊成員」中文全名，並於昨日作出修訂，只用星號「*」顯示部分用戶名字。個人資料私隱專員鍾麗玲表示，雖然暫時沒有收到投訴或查詢，但會跟進事件。 ◆香港文匯報記者 吳健怡

◆康文署已要求SmartPLAY承辦商修改訂場系統「團隊成員」功能設定。圖為市民正在了解SmartPLAY的使用方法。 香港文匯報記者北山彥 攝

康文署早年斥資5億元開發SmartPLAY康體通系統，推出以來問題不斷，繼系統因為過多用戶登入，不勝負荷而網絡「大塞車」後，近期有用戶反映若透過「My SmartPLAY」應用程式預訂足球場，填報團隊成員資料時，於「用戶賬號或別名」一欄，隨意輸入他人英文姓名，程式會顯示以該姓名作賬號登記的其他陌生用戶之中文全名，添加為「團隊成員」，可能導致個人資料外洩，被「炒場黨」利用。

已要求承辦商修訂堵塞漏洞

香港文匯報記者亦在昨日凌晨進行實測，在該系統預訂足球場，並在團隊成員「別名」一欄輸入十分普遍的英文名，如Alan及Ben，系統即勾出一位姓張及姓潘的登記人名字，初時只顯示姓氏，名字為星號。但按一下確定掣後，系統隨即顯示該名陌生登記人的全名。

事件被揭發後，記者昨午再進入系統，SmartPLAY已修正搜尋功能，以別名搜索用戶時只會顯示姓氏，名字部分資料會以星號取代。

康文署回應時表示，SmartPLAY用戶不論經抽籤或以「先到先得」方式預訂草地足球場時，必須填報另外4名用場人士的用戶編號，租用人亦必須與其中3人一同簽場及使用設施，功能原意為方便用戶搜尋其團隊成員。現在已立即要求承辦商修改程式，停止顯示「團隊成員」中文全名，所有加入為「團隊成員」亦須是對方接受邀請加入「朋友列表」內的用戶。

康文署署長劉明光昨日出席公開活動後表示，前日知悉有用戶反映問題後，已即時叫承辦商更改設計，不會再搜尋到用戶全名。另承辦商正進行工作，用戶在預訂足球場等場地時，在加入其他團隊成員姓名步驟，必須取得對方同意，才可加入「朋友項目」（friend list）中。當使用對方姓名訂場後，也會通知「朋友」，通知形式會是短信或電郵，「在短時間內便會推出新功能」。

他強調，前晚已第一時間知會私隱專員公署，昨日亦跟公署交流意見，暫未收到用戶查詢擔心私隱外洩。至於系統推出前有否作全面私隱測試，他透露在設計系統時曾作公眾諮詢，主動問過市民對設計、版面有何意見，今年7月進行用戶登記時，在全港各區作自助服務站收集意見。

議員促暫停運作全面檢視

民建聯立法會議員葛珮帆則建議，康文署應該暫停SmartPLAY運作，全面檢視該軟件的所有網絡安全漏洞，以及查核現時所造成的損失。她指出，SmartPLAY自啟用以來，便接連出現故障，除了被指有資料外洩的漏洞，亦出現系統「大塞車」、同一時段重複預訂的情況等，市民會因此失去信心。

康體通或存在三大安全漏洞

專家之言

康文署SmartPLAY康體通系統懷疑出現資料外洩漏洞，信息安全專家龐博文昨日向香港文匯報表示，該系統或存在三大網絡安全漏洞，其中訂場地時竟然可以獲悉陌生人的中文全名並將對方加入隊伍，顯示有關系統就使用者的角色及權限未有明確分清，屬數據庫設計邏輯上問題；網絡「大塞車」顯示負載管理預計失誤，以及與「智方便」作密鑰管理對接時出現失衡，促請康文署及相關部門作出審視，盡快修改及更正。

龐博文認爲，SmartPLAY勾出陌生用戶的資料，除了使用者角色及權限未有分清外，亦出現負載管理預計失誤及與「智方便」作密鑰管理對接時出現失衡，他對此感到訝異：「一套面向公眾的系統在測試期間出現以上問題是可以理解，但現在推出市場應用的是『正式版』，爲何仍然漏洞百出呢？」

推出前須做風險評估及審計

他透露，嚴謹的系統在推出應用前，理應已通過一系列的安全風險評估與審計，當中包括「系統負載平衡測試」、「資料庫邏輯安全與效能測試」及「私隱風險評估」等，及早找出系統不完善的地方。與此同時，爲確保系統在「落地」使用時不會錯漏百出，事前應進行充足的「使用者驗收測試」。此外，由於有關系統可使用信用卡作支付，亦需進行信用卡安全審計(PCIDSS)，才會萬無一失

就SmartPLAY出現的問題，政府資訊科技總監辦公室發言人表示，已即時向康文署了解有關問題，並提供技術建議及要求部門盡快更新相關預訂功能。

發言人續指，因應早前有個別政府部門在推出電子服務時遇到的問題，資科辦在今年5月發布指引，加強提示及責成各政府部門須爲其電子服務在推出前進行充分的評估、測試和審查（包括資訊保安及負荷測試）；並要求部門須制定後備方案。

康文署發言人表示，新系統在推出前已經依從政府相關標準及指引進行各項測試，當中包括單元／整合測試、用户測試、負荷測試或壓力測試等，並由獨立第三方進行安全風險評估與審計及私隱風險評估等，確保新系統能滿足標書上所有列明的要求。

◆香港文匯報記者 文禮願

港企網絡保安準備指數錄最大跌幅

香港文匯報訊（記者 吳健怡）香港網絡保安頻頻出現危機，個人資料私隱專員公署及香港生產力促進局．網絡安全昨日共同公布「香港企業網絡保安準備指數及私隱認知度」調查發現，今年香港企業的網絡保安準備指數滑落至47點，較去年再挫6.3點，創設立該指數6年來最大跌幅。調查亦於9月透過電話訪問378間企業，發現超過七成受訪企業在過去12個月曾遇到至少一類網絡安全攻擊，釣魚攻擊繼續是中小企最常見的網絡安全攻擊。公署表示，正與政府緊密合作，審視個人資料私隱條例修訂，包括在企業和機構未有適時通報資料外洩事故時，建議引入行政罰款處理，以及引入強制舉報措施等。

七成企業過去一年曾受網攻

個人資料私隱專員鍾麗玲昨日出席調查發布會時表示，香港電腦保安事故協調中心在今年首9個月共計錄逾1.39萬宗事故報告，較去年同期飆升20.4%，當中最多屬「網絡釣魚」攻擊，其次為「殭屍網絡」攻擊。此外，截至10月底，公署今年共接獲119宗資料外洩通報，正與政府審視個人資料私隱條例修訂。

該署及生產力促進局今年9月亦透過電話訪問378間企業，發現「香港企業網絡保安準備指數」若以最高100點計算，今年只錄得47點。指數由「保安政策風險評估」、「技術控制」、「流程控制」和「建立員工意識」4個範疇組成，結果亦顯示「技術控制」因較少企業進行系統保安修補管理，或採取網絡威脅防禦措施，按年急挫11.2點。

◆私隱專員公署及生產力促進局昨日公布「香港企業網絡保安準備指數及私隱認知度」的最新調查結果。 香港文匯報記者涂穴 攝

據調查發現，逾七成受訪企業過去一年間曾遭受網絡安全攻擊，較去年再升8個百分點至歷年新高，「網絡釣魚」攻擊近乎是所有受影響企業最常遇到的網絡安全攻擊類型。尤其是網絡釣魚簡訊及社交媒體釣魚較去年常見，至於使用人工智能(AI)或生成式AI及使用二維碼的釣魚攻擊則成為新興現象，分別錄9%和8%。

鍾麗玲指出，情況與科技及社交媒體應用每日快速發展，令騙徒有機可乘利用新興科技詐騙有關，促請市民要有所警惕，避免輕易提供銀行、電話號碼及身份證等資料。以QR Code釣魚攻擊為例，過去亦曾有通訊軟件被假冒QR Code網址，市民若誤入很易遭黑客取得通訊錄資料等，造成風險。

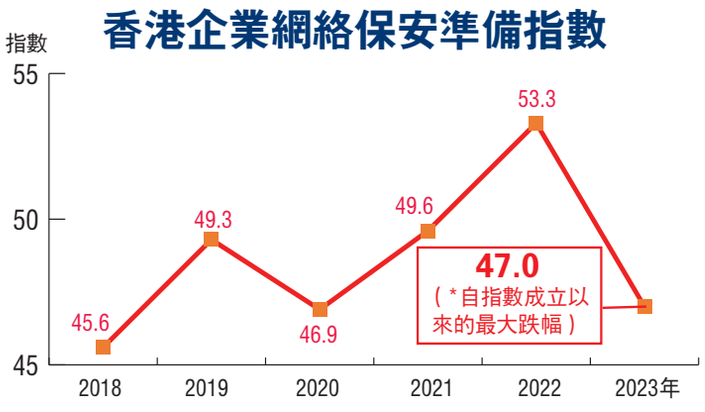
生產力促進局數碼轉型部總經理陳仲文補充，AI技術可利用現有影像、影片或錄音資料，進行人面模仿及假扮聲音，且生成性文字模版亦已進化，變得更少語誤和像真，提醒市民要實行「零信任」政策，避免提供敏感資訊，且要留意通話對象舉動與過去是否有差別，「如『老闆』突然要求匯大筆款項，不應馬上照辦，而應再作求證。」

建議加強培訓員工安全意識

調查亦發現逾半中小企未有考慮實施或採取不同保護私隱及資料保安措施。鍾麗玲認為，保護個人資料私隱與維護網絡安全不可或缺，建議不論大小企業均應實施私隱管理系統，以及制訂個人資料外洩應變計劃和通報機制，加強員工培訓及網絡安全意識，以加強數據治理及數據安全。

陳仲文認為，很多網絡攻擊之所以成功，是基於人員疏忽所致，其中「建立員工意識」分行指數，今年繼續於25點低位停留，反映人員的網絡安全意識有急切改善的需要，強烈建議企業盡快加強員工的網絡安全意識，包括定期為員工提供培訓，甚或定期進行網絡安全演習。

香港企業網絡保安準備指數



行業分類指數

行業	2023年的指數	2023年的級別	按年變化
金融服務	64.9	具管理能力	−0.8
資訊和通訊技術	63.3	具管理能力	+2.2
製造、貿易和物流	48.6	具基本措施	−8.9
非牟利機構、學校和其他	45.9	具基本措施	−1.2
專業服務	43.5	具基本措施	−4.9
零售和旅遊相關	33.3	措施不一致	−12.5（*跌幅最大）
香港企業網絡保安準備指數（所有行業）	47.0	具基本措施	−6.3

資料來源：私隱專員公署、生產力促進局
整理：香港文匯報記者 吳健怡

阻街亂拋垃圾電子繳罰款修復

香港文匯報訊 香港特區政府上月將亂拋垃圾等公眾潔淨罪行的定額罰款增至3,000元；針對店舖阻街的定額罰款亦增至6,000元，但因為電子繳費系統未同步修訂，一度令收到罰單的市民無法使用電子方式交罰款。食環署昨日公布，署方的電子繳費系統經更新後，收到定額罰款通知書的市民，現已可用通知書上列明的多種電子方式繳交罰款。

食環署發言人表示，相關的電子繳費系統經更新後，市民可選擇用貼有「繳費服務」標誌的銀行自動櫃員機、繳費靈、電話理財服務等電子方式繳交罰款，亦可選擇郵寄支票、匯票、本票或親自到郵政局繳款。網上銀行繳款服務方面，各銀行正陸續完成系統更新，市民如有查詢可聯絡食環署。

早前在電子繳費系統進行更新期間，食環署已提醒受影響市民留意繳款安排。仍未繳交罰款的市民會收到繳付定額罰款通知書（表格2），上面載有他們現時可使用的繳款方法。

食環署在上月22日至本月12日期間，就相關公眾地方亂拋垃圾發出1,039張定額罰款通知書、在公眾地方吐痰有55張、未經准許而展示招貼或海報103張、店舖阻街50張，以及海上棄置廢物1張定額罰款通知書。

◆食環署電子繳費系統經更新後，市民已可在網上繳交阻街及亂拋垃圾罰款。 資料圖片