資料來源：香港電腦保安事故協調中心

保護社交媒體平台帳戶 提防資料外洩或遭受網絡攻擊

2021年4月初，全球三個主要社交媒體平台接連爆出嚴重的數據外洩事件，讓大家再次關注這類平台在保護個人資料的保安問題：

- **33億個 Facebook 用戶的個人資料被公開披露；**
- **5億個 LinkedIn 用戶資料被收集並於線上販賣；和**
- **130萬個 Clubhouse 用戶記錄被洩露在一個黑客論壇中。**

以上一連串發生的事故已使社交媒體平台營運者提高對數據保護的警覺，並改善其針對數據洩漏的保安防禦能力。與此同時，用戶亦要經常積極保護社交媒體帳戶上的敏感資料，並要保持警惕，以防外洩的個人資料遭黑客用來發動網絡攻擊。

利用外洩個人資料進行的網絡攻擊

黑客可以使用外洩的個人資料進行多種網絡攻擊，例如利用受害人的電子郵件地址和電話號碼冒充受害人，並向其關係親密的人（如家人、朋友、同事等）作出網絡釣魚和其他社交工程攻擊。同時，亦可透過不同的數據外洩事故，大規模地收集各式各樣的資料，然後向個人或機構發起精密而有針對性的攻擊。

自我檢查：是否過往數據外洩事故受害人

自2013年開始，互聯網用戶可以利用一個網上免費自檢工具 HaveIBeenPwnd（https://haveibeenpwned.com），檢查其個人資料有否在過往的數據外洩事故中曾被公開。最近此自檢工具已作出更新，可讓用戶檢查自己是否 Facebook 數據外洩事故的受害人。

如果用戶發現自己涉及數據外洩事故，應保持冷靜並採取以下保安建議，加強對網上帳戶和資料的保安，以及防範網絡攻擊。

留意私隱設置和保安功能

用戶應仔細檢查和管理在社交媒體平台上公開可見的資料。一些個人敏感資料（例如身份證號碼、住址、電話號碼和財務資料等）都應保密。用戶需要：

- 充分善用社交媒體私隱設置來控制資料的公開程度；

- 定期檢查公開的資料，如無需公開時應將其刪除；以及
- 參考各社交媒體平台官方的私隱設置指南。

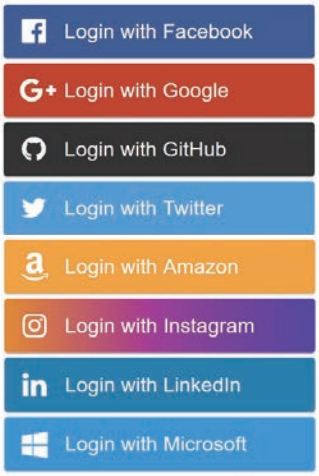
Facebook　LinkedIn　Twitter

Google　Microsoft

各社交媒體平台都有其官方的私隱設置指南（掃瞄以上二維碼可瀏覽）。

對以社交媒體帳戶為第三方應用程式作認證的保安建議

許多第三方應用程式已採用社交媒體帳戶作登入時的身份認證，用戶可用單一帳戶登入不同的網上服務。此功能讓用戶在使用第三方應用程式時，省去登記另一個帳戶和記住登入名稱及密碼的麻煩，提升用戶體驗。



具有透過社交媒體平台單一登入功能的圖示。

不過，萬一有關社交媒體帳戶被入侵，亦會影響相關的第三方應用程式。這種情況下，用戶應在社交媒體帳戶上採用保安程度更好的認證方式，亦要定期檢查被允許認證的第三方應用程式，如不再需要便應立即移除，更可參考各社交媒體平台的官方指南，更改與第三方應用程式分享的資料類別。

Facebook　LinkedIn　Twitter

Google　Microsoft

請參考各社交媒體平台的官方指南，更改與第三方應用程式分享的資料類別（掃瞄以上二維碼可瀏覽）。

保持良好網絡環境的建議

除了確保社交媒體帳戶設置安全外，保持良好的網絡環境也同樣重要。用戶可以參考以下建議來防範網絡攻擊。

- 參閱網絡帳戶的私穩設定，盡量減少個人資料的公開程度；
- 定期更改帳戶密碼及啟用雙重認證，以減低密碼被盜影響；
- 檢查及移除不再需要使用社交媒體單一登入功能的第三方應用程式；
- 經常更新應用程式至最新版本，以保障資料安全；
- 定期檢閱帳戶有否可疑的登入紀錄；
- 提防利用個人資料進行的釣魚詐騙電話及短訊，切勿點擊可疑電郵、短訊內的連結或附件；和
- 如無故收到平台的登入警示，請立即檢查帳戶狀況及更改密碼。

社交媒體平台漏洞：提防 WhatsApp 帳戶遭人無故停用

最近一名海外保安研究人員示範了利用 WhatsApp 的 SMS 驗證和帳戶停用程序的一個保安漏洞，攻擊者能在 WhatsApp 用戶不知情的情況下停用其帳戶，即使採用了雙步驟驗證也無法阻止有關行動。由於 WhatsApp 是香港最被廣泛使用的即時通訊軟件之一，因此潛在影響相當大。

根據示範，攻擊者會先使用受害人的電話號碼來設立 WhatsApp 帳戶，當 WhatsApp 要求輸入透過 SMS 發送給受害人手機的驗證碼時，攻擊者會重複輸入錯誤的驗證碼，觸發 WhatsApp 的保安機制來禁止繼續輸入。然後，攻擊者會冒充受害人聯絡 WhatsApp 的客戶服務部，訛稱手機被盜，要求停用帳戶。

香港電腦保安事故協調中心（HKCERT）建議 WhatsApp 用戶採取以下措施保護帳戶：

- 啟用雙步驟驗證，並填寫電子郵件地址；
- 切勿將 SMS 驗證碼轉發或分享給任何人。若沒有要求接收驗證碼，應立即向 WhatsApp 報告有關情況；以及
- 設置手機的屏幕鎖定功能，防止陌生人使用。

由於 WhatsApp 是使用手機號碼來驗證用戶身份，因此若遺失了手機，應該：

- 立即向電訊商報失；
- 拿到新 SIM 卡後，重新以電話號碼登錄 WhatsApp，這會強制登出帳戶內的所有使用者；以及
- 使用裝置遺失追蹤功能（例如 Apple 的 Find My iPhone 或 Google 的 Find My Device）鎖定裝置或清除資料，以防止數據外洩。

《網絡保安動畫 黑客之日常》

HKCERT 的一系列網絡保安動畫，講述中小企及市民應如何加強網絡保安，題目圍繞遙距工作和視像會議的安全攻略、雲端保安、提防釣魚郵件的攻擊及注意物聯網保安。

此集講述該如何應對遙距工作時遭受的惡意入侵。當中提到加密措施的好處、六個遙距工作保安貼士，以及視像會議自保招式。

此集介紹有關做妥雲端服務配置的三步曲，以及有關雲端安全的五個措施。

此集分享應對和防範釣魚郵件的七個方法，包括定期更新系統程式及保安軟件的病毒識別碼。

此集講述智慧辦公室配合物聯網（IoT）的注意事項，特別是密碼管理，以免黑客有機可乘，入侵公司系統。

如欲觀看全片，歡迎瀏覽 HKCERT 網站：
www.hkcert.org/tc/publications/awareness-education/cyber-security-animation-video
（或掃二維碼）