WhatsApp 賬戶安全教學

WhatsApp 是港人最常用的通訊軟件之一，涉及 WhatsApp 網絡騙案手法層出不窮。本文特此整理了 WhatsApp 安全功能、保障個人資料私隱，以及如何搶回被盜用賬戶的方法，以供大家參考。

保障個人資料私隱7招

1. 啟用 WhatsApp 的雙重認證功能。
2. 定期在 WhatsApp 設定中檢查已連結裝置，並登出不再使用或不明的裝置連結。
3. 切勿向他人透露任何密碼或驗證碼。
4. 在網上搜尋 WhatsApp 網頁版時，小心留意網頁連結，不要誤按虛假的 WhatsApp 網頁版。
5. 切勿從非官方渠道下載及使用 WhatsApp 應用程式。
6. 一旦收到他人在 WhatsApp 要求借錢、匯款或提供個人資料的訊息，應先確認發送者的身份。
7. 收到不明來歷或可疑的短訊時要提高警覺，切勿隨意打開連結或披露個人資料。

保障賬戶安全 8大功能

1. 啟用雙重認證設定

在啟用該功能後，無論是重置或是驗證賬戶，系統都會要求用戶輸入6位 PIN 碼，以保護用戶免受網絡釣魚或賬戶盜用的攻擊。

2. 封鎖及舉報可疑訊息

若然用戶舉報某個聯絡人、商家或特定內容，WhatsApp 就會收到其最近傳送給用戶的5個訊息。一旦審查後發現被舉報的用戶行爲違反相關的服務條款，WhatsApp 就或會對該賬戶停權。當收到滋擾訊息時，用戶亦可簡單地封鎖特定聯絡人，而被封鎖的聯絡人將無法再致電或傳送訊息給用戶。

3. 使用官方版本

在 Android 及 iOS 下載時應保持警覺，以防下載由第三方開發的非官方版本或僞造的 WhatsApp 應用程式。非官方應用程式可能含有惡意軟件，有機會偷取用戶資料或損壞手機，加上未有端對端加密的保護，將會把用戶個人私隱及賬號安全置於危險之中。若用戶收到「這是僞造的應用程式」的安全防護警告，請馬上刪除應用程式並下載官方版本。

4. 於群組對話中保護私隱

WhatsApp 的私隱設定及群組邀請功能可以讓用戶控制誰可以將自己加入群組，增加用戶的私隱度，亦避免被胡亂拉進陌生群組。

5. 閱後即刪功能及自動刪除訊息

爲增加訊息傳送的私隱度，用戶可在發送照片或影片時選擇閱後即刪媒體，收件者將只能檢視該訊息一次，並不能儲存、轉寄、截圖或分享。其他功能如關閉已讀標記及自動刪除訊息亦能有效爲用戶的個人對話提供多一層私隱保護。

6. 保護個人檔案

用戶可管理 WhatsApp 上的個人資料，當中包括個人頭像、最後上線時間、在線狀態、「關於我」、動態更新等，並設定哪些用戶可以查看相關資訊。另外，用戶亦可選擇向誰分享其在線狀態，讓聯絡人以外的用戶無法看到有關資料，避免讓不法之徒有機可乘。

7. 定期檢查已連結裝置

定期檢查所有已連結至賬戶的裝置，如果用戶無法識別某特定裝置，請立即登出。若用戶懷疑有他人於 WhatsApp 網頁版或桌面版上使用其賬戶，可在手機上進行設定，將其 WhatsApp 賬戶從所有電腦中登出。

8. 賬戶防護

賬戶防護的功能會在有人打算擅自將賬戶移到其他裝置時，提醒該賬戶的擁有者，包括在舊裝置上進行詢問，以便確認用戶是否要採取這個步驟作爲額外安全檢查。用戶亦可以啟用 WhatsApp 的鎖定功能，往後須使用指紋或臉孔解鎖應用程式，進一步保障私隱。用戶可輕易地於手機的私隱設定中設定生物辨識，從而使用此項功能。

如何搶回被盜用賬戶？

1. 重新輸入註冊手機號碼登入。
2. 選擇透過以手機短訊(SMS)或來電方式，收取及輸入一次性驗證碼
3. 奪回賬戶主導權。

被黑客啟用雙重認證，應如何是好？

當用戶再次登入賬戶時，WhatsApp 便會要求用戶輸入騙徒所設定的雙重認證 PIN 碼，用戶沒有該 PIN 碼便不能使用 WhatsApp。不過根據 WhatsApp 的官方指引，WhatsApp 會容許用戶七天後重設該 PIN 碼及重新登入。除了等待七天外，WhatsApp 亦允許用戶以預先設定的電郵地址重設 PIN 密碼。

預先設定電郵地址步驟：設定＞雙步驟驗證＞變更電子郵件地址

不過，無論用戶是否知道該 PIN 碼，只要用戶輸入六位數的登入驗證碼後，對方都會被強制登出，不能再繼續使用用戶的 WhatsApp 賬戶。