

資安月報十月號

手機，不再只是手機，也是資安戰場

常見的手機資安風險

1. 惡意應用程式 (App):

- 偽裝成正版App，竊取個人資料、監控使用者行為。
- 隱藏在免費App中，執行惡意行為。

2. 公共Wi-Fi：

- 駭客可能設置假Wi-Fi，竊取連線裝置的資料。
- 公共Wi-Fi通常加密強度較弱，容易被破解。

3. 簡訊釣魚：

- 透過簡訊誘騙使用者點擊惡意連結，下載惡意程式或洩露個人資料。

4. 藍牙漏洞：

- 駭客透過藍牙漏洞入侵手機，竊取資料或控制手機。



案例

- 有心人士假冒某知名企業開發的高速公路電子收費APP，藉此竊取用戶的信用卡資訊
 - <https://news.tvbs.com.tw/tech/2117520>
- 公共Wi-Fi遭入侵：駭客會設定與飯店相似的Wi-Fi名稱，若不慎連線後
 - 使用銀行或購物網站APP，個資就容易外流
 - 帳號密碼被竊，導致社交媒體帳號被盜。
 - <https://ynews.page.link/TVTdK>

案例

- 簡訊釣魚詐騙：

- 一位民眾收到駭客佯裝成老師寄來的簡訊，內容提到點選連結看孩子成績單，並依畫面提示安裝外掛程式，駭客便可以因此取得手機內存放的個人資料，包括像是使用網路銀行的登入帳號與密碼等資訊。
- [https://eteacher.edu.tw/\(S\(kp5ph4th1u3wmdjpd5qgrl5l\)\)/Tip.aspx?id=4077](https://eteacher.edu.tw/(S(kp5ph4th1u3wmdjpd5qgrl5l))/Tip.aspx?id=4077)

- 藍牙技術遭爆有「底層漏洞」！近十年手機、無線耳機全有危險

- 你以為正在傳送檔案給朋友，其實是連接到駭客的設備
- 正在傳送的資訊、檔案也有可能在傳送途中遭到攔截
- <https://3c.ltn.com.tw/news/56109>

如何保護你的手機安全（一）

- 謹慎下載App：
 - 從官方應用程式商店下載APP。
 - 檢查APP的評價、授權資訊和更新頻率。
 - 避免安裝來源不明的APP。
- 小心使用公共Wi-Fi：
 - 避免在公共Wi-Fi上進行金融交易或處理敏感資料。

如何保護你的手機安全（二）



- 設定強密碼：（ [2024.6月號-密碼安全性](#) ）
 - 使用長度足夠、夠複雜的密碼
 - 避免使用生日、電話號碼等容易被猜測的密碼
 - 啟用兩步驟驗證（ [2024.7月號-兩步驟驗證](#) ）
- 定期更新系統和App：
 - 系統和App的更新通常包含安全性修補程式。
- 小心點擊不明連結：（ [2024.8月號-釣魚攻擊](#) ）
 - 不隨意點擊不明連結或開啟附件，尤其是來自陌生人的訊息。

如何保護你的手機安全（三）

- 注意藍牙設定：
 - 不使用藍牙時，將其關閉。
 - 避免將藍牙設為可被所有人發現。
- 安裝防毒軟體：
 - 選擇信譽良好的防毒軟體，定期掃描手機。
- 備份重要資料：
 - 定期備份手機中的重要資料，以防資料遺失。



總結

- 手機已成為我們生活中不可或缺的重要資產，其資安風險也日益增加。
- 提升對常見資安威脅的認識，並採取適當的防護措施，有助於保護自己免受攻擊。
- 謹慎下載應用程式、注意公共Wi-Fi的使用、設置強密碼與定期更新系統，這些步驟能有效提高手機的安全性。
- 如果手機遭遇安全問題（例如被駭客入侵或安裝了惡意軟體），可能會導致金錢損失（如銀行帳戶被盜用）、個人資料洩露，甚至影響到家人和朋友的安全。

謝謝

圖片：Gamma

本期撰稿人：Daniel