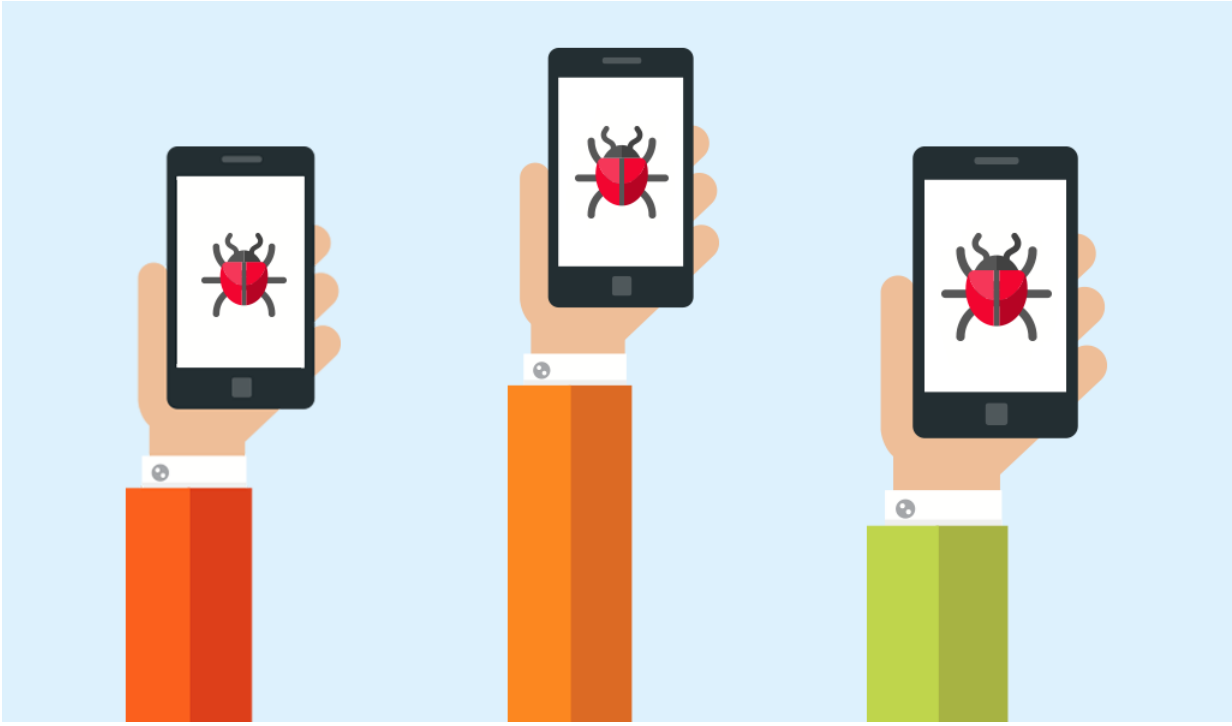
常見手機詐騙案例

:::

最後更新日期：2017/11/30

手機詐騙 (https://isafe.moe.edu.tw/public/手機詐騙?user_type=4) 165反詐騙 (https://isafe.moe.edu.tw/public/165反詐騙?user_type=4)



惡意連結是手機最大安全風險

智慧型手機就如同一臺迷你型的筆記型電腦，能用來操作各式各樣的網路服務，電腦網路使用上的各種安全問題，也同樣適用在智慧型手機的情境中，只是可能出現的形式不同，而容易被疏忽。智慧型手機使用上最常見的安全風險，就是來自於簡訊或通訊軟體等傳訊服務的惡意連結，此類的案例多半都伴隨著詐騙。以下整理 3 個常見於智慧型手機的惡意連結案例：

惡意連結案例一：搭配時事

這一類惡意連結的訊息文字會利用時事或當今流行話題， 例如在選舉期間經常傳遞到民眾手機的不明來源LINE及Facebook 訊息，請民眾前往觀看最新民調結果，或者詢問對特定候選人的支持度等；一旦點選超連結進入對方所設的網站，智慧型手機就會被植入木馬程式。

惡意連結案例二：師長簡訊

也曾經有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。

惡意連結案例三：免費貼圖

這類訊息的內容大多是要求手機使用者轉寄簡訊給10個朋友後，就可以得到免費的貼圖，包括像是蛋黃哥、櫻桃妹等知名卡通人物，都曾經被利用在這一類的簡訊中。過往也曾經發生，點選免費貼圖超連結後，進入假的 Facebook 登入畫面，一旦輸入帳號與

密碼按下「Login」後，視窗馬上就會關閉。這時，使用者的資料就被偷走，而身分也可能因此被盜用。

刑事警察局幫你查證可疑簡訊

刑事警察局提供民眾分析可疑簡訊的服務，只要將含有超連結的陌生簡訊轉發至0911-511-111，就能由刑事警察局協助分析判別並將結果回覆給民眾，不但如此，刑事警察局也可透過此服務蒐集各式各樣的惡意簡訊案例，在統計分析後，能夠對大眾提供更豐富且更準確的防詐騙宣導內容。

好記又難猜的密碼設... 上一頁 (/article/1944?user_type=4&topic=9)

下一頁 (/article/1986?user_type=4&topic=9) 智慧型手機安全大掃除

宣傳單 更多宣傳單...

(/flyers/1904?user_type=4&topic=9)

漫畫 更多漫畫...