



【資安】我不敢相信是你？假 YouTube 連結！學著保護臉書帳密

用假的 Facebook 登入頁面來騙取用戶帳號密碼的個資詐騙手法已出現多年，但有心人士仍持續以不同方法向用戶「釣魚」，引導大家到假的 Facebook 登入頁面。近期民眾回報這類詐騙手法，主要是以臉書私訊發送假的 YouTube 連結與「我不敢相信是你」的文字，誘使使用者點擊至假的 Facebook 登入畫面，進而騙取臉書的帳號密碼，真的要多方小心，有些辨識方式和補救方法也可以學起來唷！



假 YouTube「我不敢相信是你？」的連結
你可能會在某一天於 Facebook 收到親友在 messenger 傳來一個「我不敢相信是你？」的連結，並以 YouTube 圖案縮圖並搭配引人好奇的文字，冒充臉書好友傳送，吸引接收方點擊。

部分發佈貼文者，有的則是製造帳號在群組發佈的假象，有的則是假冒新聞單位與社團貼文，加上訊息發送者是自己臉書好友，試圖增加可信度而讓人卸下心防，提高點擊的機會。

根據「趨勢科技防詐達人」實測，這個「偽 YouTube 連結」會把你引導到一個山寨臉書登入頁面，一旦用戶在此頁面輸入帳密，將導致帳密外流，進而被盜取。

Facebook 帳號密碼被盜用會發生什麼事

當你的帳號密碼被盜取，你的帳號將會被冒用，比照相同手法將釣魚連結傳送給你的臉書朋友，導致更多人受害。像是在各大社團張貼的直播帳號、買賣文，不少都是盜用帳號從事的行為，更惡劣者會私訊病毒連結給遭受盜用者的臉書朋友。

如何保障 Facebook 帳號安全？

根據臉書官方公告，提及詐騙份子可能會製造與 Facebook 相似的假網站，並要求用戶使用電子郵件和密碼登入。

因此在輸入登入資料前，請再三檢查網站的網址。如有疑問，請在瀏覽器中輸入

www.facebook.com 以前往 Facebook 的正確網址，並且勿點擊可疑連結，即使看起來是認識的朋友或公司所傳送的連結也不例外。

已經輸入帳密了該怎麼辦？

1. 更換密碼並開啟雙重驗證

如果萬一已經輸入帳號密碼，請立即更換密碼並開啟 Facebook 雙重驗證及時補救，以提高帳號安全性。

2. 開啟「接收不明登入活動的警告」

如果有人試著從我們無法辨認的裝置或網頁瀏覽器登入時，開啟「接收不明登入活動的警告」會讓你收到警告，如此可加強保障你的 Facebook 帳號安全，而且這些警告會告訴您哪部裝置遭人嘗試登入和其位置。

資料來源：MyGoPen 反詐騙網站

<https://www.mygopen.com/>、趨勢科技防詐達人

雲林縣莿桐鄉公所