密碼 123 ，盜用好簡單。

資安時事案例

簡訊詐騙有新招 署名「高級鐵路」是假的！

病毒盯上安卓用戶 偽裝寶可夢竊聽對話

個人資料保護法

第 41 條

輕鬆學資安

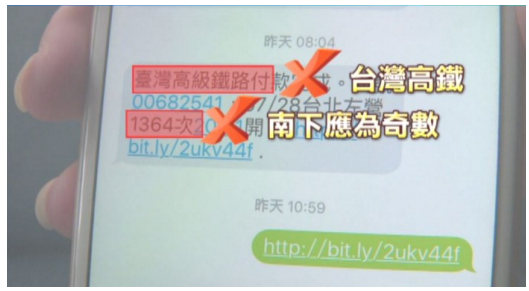
電腦安全駭客

數位學習

105 年資安動畫金像獎

資安 TRICK OR TREAT 萬聖劫

簡訊詐騙有新招 署名「高級鐵路」是假的！



2017 年 06 月 19 日 04:10 記者林瑞益 / 綜合報導

詐騙手法真的是層出不窮，新竹市副市長沈慧虹日前收到一則簡訊，她買了一班台北到左營的車票，還附上一串網址，但仔細一看，簡訊開頭寫的是台灣「高級」鐵路，最重要的是她非常確定自己沒有訂票，所以沒點開網址。警方提醒民眾，別亂點可疑簡訊網址，不然個資可能就會被盜走。

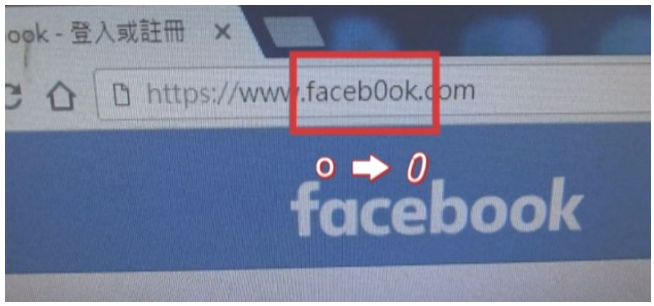
手機簡訊傳來，點開一看，上面寫著「台灣高級鐵路付款完成」，還有完整的訂單代號和列車班次時間，最後還附上一個網址。

這是新竹市副市長沈慧虹日前收到的簡訊，但她沒點開，因疑點重重。

新竹市副市長沈慧虹：「台灣沒所謂高級鐵路這個用語，不過最主要的關鍵字是車次代號，不管台鐵高鐵，他的南下編號應該是，末碼是奇數碼，我發現他是 1364 是一個偶數碼。」

台灣高鐵變成了台灣高級鐵路，南下列車應該是單號，所以這肯定是假的！不只高鐵訂票簡訊，還有餐券團購，或是恭喜中獎等等的詐騙簡訊，下頭都會附上一個縮短過的網址，點開來，就出現像這樣的網頁。

一看就是臉書的登入畫面，讓人不疑有他，直接輸入帳號密碼，但一按登入就會出現找不到帳號的提醒，一般民眾都會以為是自己打錯，或是手機、電腦出問題。



警方：「但是你只要仔細看那個，左上方的網址，他在網址內或許已經複製了，某一臉書某一個網站的網址，貼再一個的假網站，但是他的網址絕對會不一樣。」

一模一樣的網頁，但網址的「o」卻變成「0」，這類簡訊詐騙網址，通常都只和正版網站差一點點，要是沒注意到，個資馬上被側錄、外洩。提醒民眾，如果收到類似簡訊或網址，千萬要提高警覺，小心個資安全。

（民視新聞 / 葉興凱 新竹報導）

HOME

病毒盯上安卓用戶 偽裝寶可夢竊聽對話

中央社　106.7.22

（中央社記者吳家豪台北 22 日電）資安業者趨勢科技發現一款 Android 後門程式「 GhostCtrl 」，會偽裝成熱門程式 Pokemon GO （寶可夢），暗中錄音、錄影，還可隨心所欲操控受感染的裝置，但裝置使用者卻毫不知情。

趨勢科技指出，最近攻擊以色列醫院的 RETADUP 資訊竊盜蠕蟲，還會引來一個更危險的威脅：可操控受害裝置的 Android 惡意程式，也就是趨勢科技命名爲 GhostCtrl 的後門程式。

GhostCtrl 共有三種版本。第一版會竊取資訊並掌控裝置的特定功能，第二版會進一步操控更多功能，第三版則吸收了前兩版的優點之後再加入更多功能。趨勢科技認爲，從該程式的技巧演進情況來看，未來只會越來越厲害。

GhostCtrl 其實是 2015 年 11 月曾經登上媒體版面的 OmniRAT 商用多功能惡意程式平台的變種之一。它宣稱只要在 Android 裝置上透過觸控方式，就能遠端遙控 Windows 、 Linux 和 Mac 系統。

趨勢科技發現，此惡意程式會偽裝成一般正常或熱門的應用程式，名稱大多叫做 App 、 MMS 、 whatsapp ，甚至是 Pokemon GO 。當應用程式啓動時，它會從資源檔解開一個 base64 編碼的字串並寫入磁碟，這其實是惡意 Android 應用程式套件（ APK ）。

接下來，惡意 APK 會連線至幕後操縱（ C&C ）伺服器來接收指令，但裝置使用者卻毫不知情；駭客可以暗中操縱裝置的功能，包括蒐集並上傳各種對網路犯罪集團有價值的敏感資訊，例如通話記錄、簡訊記錄、通訊錄、電話號碼、 SIM 卡序號、地理位置、瀏覽器書籤等。

面對 GhostCtrl 這樣的後門程式，趨勢科技建議企業應部署多層式資安機制才能有效管理資料風險，包括隨時保持裝置更新、採用最低授權的原則，以及建置一套可偵測並攔截惡意和可疑應用程式的信譽評等系統。

舉討債洩個資

違反個資法第 41 條「非公務機關未於蒐集特定目的必要範圍內利用個人資料罪」

舉牌討債洩個資　高校生收 500 元換 2 月牢

蘋果日報 106.7.10

高雄一名 19 歲吳姓高職生去年受討債集團僱用並收受 500 元報酬後，到欠債的史姓男子經營的機車行前高舉「欠錢還錢」告示牌，還附上放大影印的史男身分證及本票，史男認爲隱私遭侵害怒提告。高雄地院今依違反《個資法》判吳男 2 月徒刑，得易科罰金 6 萬元，並宣告沒收 500 元犯罪所得。判決指出，去年 8 月 8 日下午，吳男受 2 名男子雇用，收受 500 元報酬後，到史男經營的機車行前高舉貼有史男身分證及其簽發本票放大影本告示牌，並寫上「欠錢還錢」標語，展示給過往群眾觀覽，史男見狀立即報警查扣告示牌。法院審理時，吳男辯稱他高舉告示牌上揭露的史男個資已經用馬賽克部分遮隱，並未違法，但法官認爲，該告示牌直接張貼史男放大影印之身分證及其簽發之本票，而身分證影本上登載有史男照片、姓名、出生年月日、身分證統一編號；本票影本則記載史男居住地址，其中雖將姓名中間一字、出生月份、身分證統一編號末三碼、住址巷弄號等小部分遮隱，但身分證上本人照片全露，若與其他未經遮隱資料對照，仍能識別就是史男。法官還指吳男在史男經營的機車行前舉牌向往來民眾展示上述資料，更足以使人辨識其所指欠債者爲何人，因此依違反《個資法》第 41 條「非公務機關未於蒐集特定目的必要範圍內利用個人資料罪」判他有期徒刑 2 月，得以 6 萬元易科罰金。仍可上訴。（王吟芳／高雄報導）

HOME

Computer Security Hacker
電腦安全駭客

資料出處： iThome

電腦安全駭客是指擁有電腦與網路知識的駭客，這樣駭客懂得網路運作原理與其資安風險，比如在一個有 IPS 的網路環境，他知道如何避開 IPS 的偵測與阻擋進行攻擊。