# 剖析「網絡危機」及「資訊保安」

政府資訊科技總監辦公室

cybersecurity.hk

政府資訊科技總監辦公室

# 假冒公眾Wi-Fi 截取敏感資料


# 手機上網 危機四伏

am故事

**為節省手機流動數據，公眾Wi-Fi(無線上網)服務有時確是好幫手，惟使用時須留意保障個人資料！警方發現有網絡犯罪分子會以容易令人取信的名稱設置Wi-Fi網絡，假冒一般機構提供的「公眾Wi-Fi」，以截取用家的敏感資料及上網紀錄，繼而作未經授權交易；另外，有不少商舖會將Wi-Fi密碼資料貼在當眼處，讓顧客使用，亦容易被不法之徒利用作陷阱。根據警方統計，今年首7個月，非法入侵個案，損失款項已較去年同期倍升逾13億元，當中有可能涉及不當使用Wi-Fi。**

公眾Wi-Fi日漸普及，成為騙徒盜取資料的平台 (網式明攝)

「當時當刻唔會察覺得到，亦無任何signal(訊號)會睇得到，直至發生咗唔關於佢嘅網上交易，先向警方舉報，嗰時已經係幾個月嘅事。」警方網絡安全及科技罪案調查科偵緝督察黃紬奇接受本報訪問時表示，公眾Wi-Fi每日使用者眾多，黑客亦是不動聲色地取走用戶的個人或敏感資料，其中以旅遊景點、咖啡店、餐廳的Wi-Fi成為他們「落手」黑點，「旅遊熱點的地方容易中招，因為黑客想睇番有幾多人去過那些地方用這些網絡，黑客想找一些吸引很多人去的地方，作出攻擊。」他又說，保安意識較低的商戶，會將Wi-Fi密碼資料隨意貼在店舖門外，亦成為黑客入侵的目標。

黃紬奇進一步解釋，用家使用公眾Wi-Fi瀏覽一般網站並無問題，但當登入電郵帳戶及輸入私人資料等，則有機會「中招」。黑客會透過惡意程式，或是以個人裝置建立與一般公眾Wi-Fi相類似名稱的網絡，企圖以假亂真，提供免費Wi-Fi服務，吸引公眾人士連繫上，「令用家分辨不到連個係黑客定真公眾Wi-Fi，」故黑客取得控制權時，可從中截取這些資料，並實時監察到手機用家的資料及數據。


黃紬奇稱市民使用公眾Wi-Fi時，須小心保障個人資料。

## 危機四伏

### 公眾Wi-Fi不宜處理敏感資料

警方於今年首7個月，共錄得674宗非法入侵個案，雖較去年同期的747宗少，但損失金額增加近倍，由去年的7.7億增至13億元，當中有可能涉及不當使用Wi-Fi，而入侵情況不會受手機型號所限。網絡安全及科技罪案調查科總督察(網絡安全)許崗惠指出，須密碼登入的Wi-Fi會較安全，但提供者須避免將密碼資料暴露。至於使用公眾Wi-Fi者，除了不要處理個人、交易及敏感資料，更要關閉手機檔案分享功能，以減低資料外泄的風險。

警方不諱言，經公眾Wi-Fi入侵的個案追查相對困難，因受害人發現有不明來歷的交易時，已經過了一段長時間，難以追尋源頭，「要拘捕真身好難。」惟相信這些黑客犯事時，與受害人存於同一Wi-Fi覆蓋範圍，不涉及遙距和跨境控制。

另外，警務處舉辦首屆網絡安全精英嘉許計劃，銀行與金融、交通、通訊和公共事業業界人士，即日起至本月30日可提名網絡安全從業員參加。

相關新聞片段可於am730 Facebook專頁重溫。

★一人取一份，大家都開心。 ■發行：AM730 Media Limited ■地址：香港灣仔告士打道160號海外信託銀行大廈10樓 ■承印：Brilliant Star Printing Services Limited ■地址：香港新界大埔工業邨大

資料來源: AM730 [2016-09-15] (http://www.am730.com.hk/article-329642)

港聞

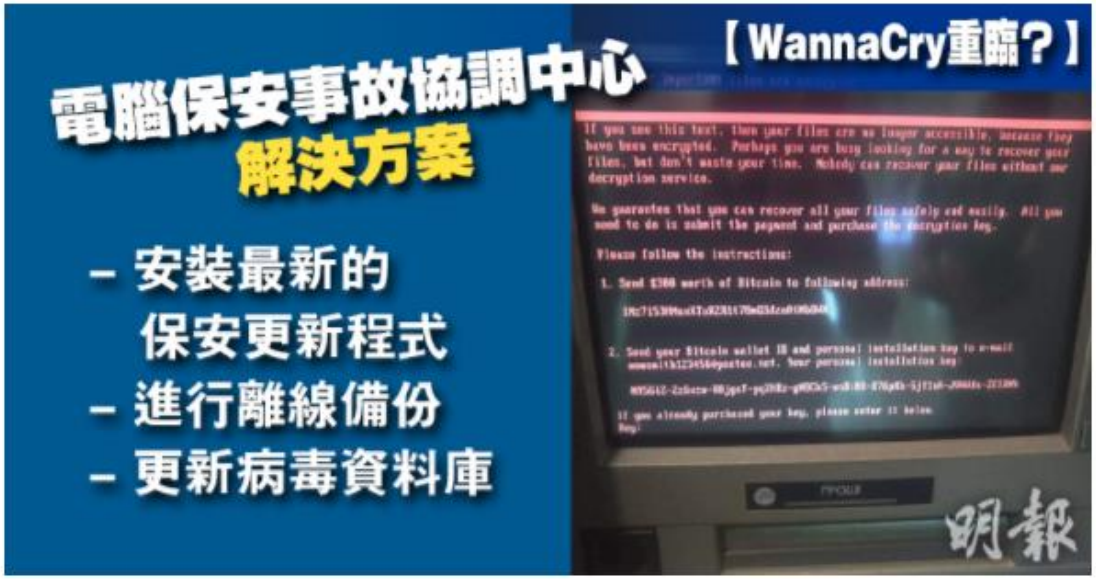
【新勒索軟件殺到】電腦保安事故協調中心列極度危險　稱被加 ▼

2017年6月28日 星期三

上一篇　下一篇

# 【新勒索軟件殺到】電腦保安事故協調中心列極度危險　稱被加密數據無法還原 (11:27)






資料來源: 明報 [2017-06-28]
(https://news.mingpao.com/ins/instantnews/web_tc/article/20170628/s00001/1498620088089)

# 黑客入侵Google Play商店　2100萬人或受害

09月15日(五) 22:00 


Google Play Store發生大型黑客入侵事件。（資料圖片）

以色列網絡安全公司Check Point Software Technologies周四（14日）發表報告披露，智能手機作業系統Android發生大型的黑客入侵事件。有黑客透過在Google Play Store上架的逾50個應用程式，植入惡意程式「Expensive Wall」，向受害者發短訊騙取金錢，估計受害者可能多達2110萬人。

資料來源: 東網 [2017-09-15]
(http://hk.on.cc/int/bkn/cnt/news/20170915/bknint-20170915220055210-0915_17011_001.html)

永隆銀行 WING LUNG BANK
招商銀行集團成員
Member CMB Group

新聞稿　　2017 年 10 月 4 日

# 永隆銀行出現欺詐網站
# 呼籲公眾及客戶提高警覺

(*2017 年 10 月 4 日，香港*) －永隆銀行有限公司（下稱「本行」）呼籲公眾提高警覺，注意一個網址為（https://www.winglungonline.com/）的網站，該網站為欺詐網站。

本行特此聲明，本行與該網站絕無任何關係，亦非由本行所設立，現提醒公眾及客戶切勿登入或瀏覽該網站。

本行建議客戶採取適當的措施。為確保登入正確的本行相關網站，客戶應在瀏覽器的網址列內鍵入以下資料:
永隆銀行官方網址：（www.winglungbank.com）及
永隆「網上證券」服務網址：（www.winglungsec.com）。

本行已就該欺詐網站向有關監管機構及香港警務處通報。

資料來源: 永隆銀行有限公司 [2017-10-04]
(https://www.winglungbank.com/wlb_corporate/files/hk/upload/about-us/special-notice-fraud-alerts-20171004.pdf)

兩岸國際 2017年10月05日 雅虎30億賬戶資料外洩

# 雅虎30億賬戶資料外洩

5,438

讚 1


A A

今年7月才入主雅虎（圖）的美國電訊商Verizon Communications前日證實，雅虎2013年被黑客入侵事故中，資料外洩的賬戶數目並非去年估計的10億，而是所有30億賬戶無一倖免，令Verizon面臨的法律風險大增。

資料來源: 蘋果日報 [2017-10-05] (http://hk.apple.nextmedia.com/international/art/20171005/20172991)

# 保護你的個人電腦

1. 
帳戶密碼

2. 
帳戶權限

3. 
訪客帳戶

4. 
屏幕保護

5. 
抗惡意程式碼工具

6. 
個人防火牆

7. 
軟件更新

8. 
互聯網瀏覽器

9. 
數據備份

10. 
徹底刪除

# 保護你的流動裝置

1. 
購買

2. 
限制程式安裝

3. 
屏幕鎖定功能

4. 
抗惡意程式碼工具

5. 
軟件更新

6. 

裝置加密

7. 
Wi-Fi 連接

8. 

位置服務

9. 
應用程式權限

10. 
裝置備份

11. 
安全刪除

# 妥善的帳戶及密碼管理

1. 密碼易記難猜
2. 不同帳戶採用不同密碼
3. 密碼要好好保存
4. 使用雙重驗證
5. 定期更改密碼

# 怎樣預防勒索軟件？

不要開啓可疑電郵

保持抗惡意程式碼軟件及
其識別碼為最新版本

不要瀏覽可疑網站


為軟件安裝
最新的修補程式


經常備份資料及
不要將備份連接至電腦

關閉辦公室軟件
內的巨集功能

# 勒索軟件

## 受到感染後應如何處理？

切斷受感染電腦
的網絡連線

向警方報案

從備份復原數據
至未受感染裝置

# cybersecurity.hk

## 政府資訊科技總監辦公室


**Twitter**

https://twitter.com/cybersecurityhk

www.infosec.gov.hk

**Youtube Channel**

# infosecgovhk


**Facebook Page**

# 共建安全網絡


**2017年「智慧家居 安全生活」一頁漫畫創作比賽**

**公開組 亞軍作品**

網絡安全做得好，上網輕鬆冇煩惱

左永祥

**2016年「數據安全 交易放心」**
**吉祥物設計比賽**

**中學組 冠軍作品**

線雲密探

高苡琳
(嘉諾撒聖方濟各書院)


2015年「網絡保安 四面八方」圖像設計比賽

小學組 季軍作品

加密鎖先生

林志澄
獻主會小學

# 謝謝!!

cybersecurity.hk

政府資訊科技總監辦公室