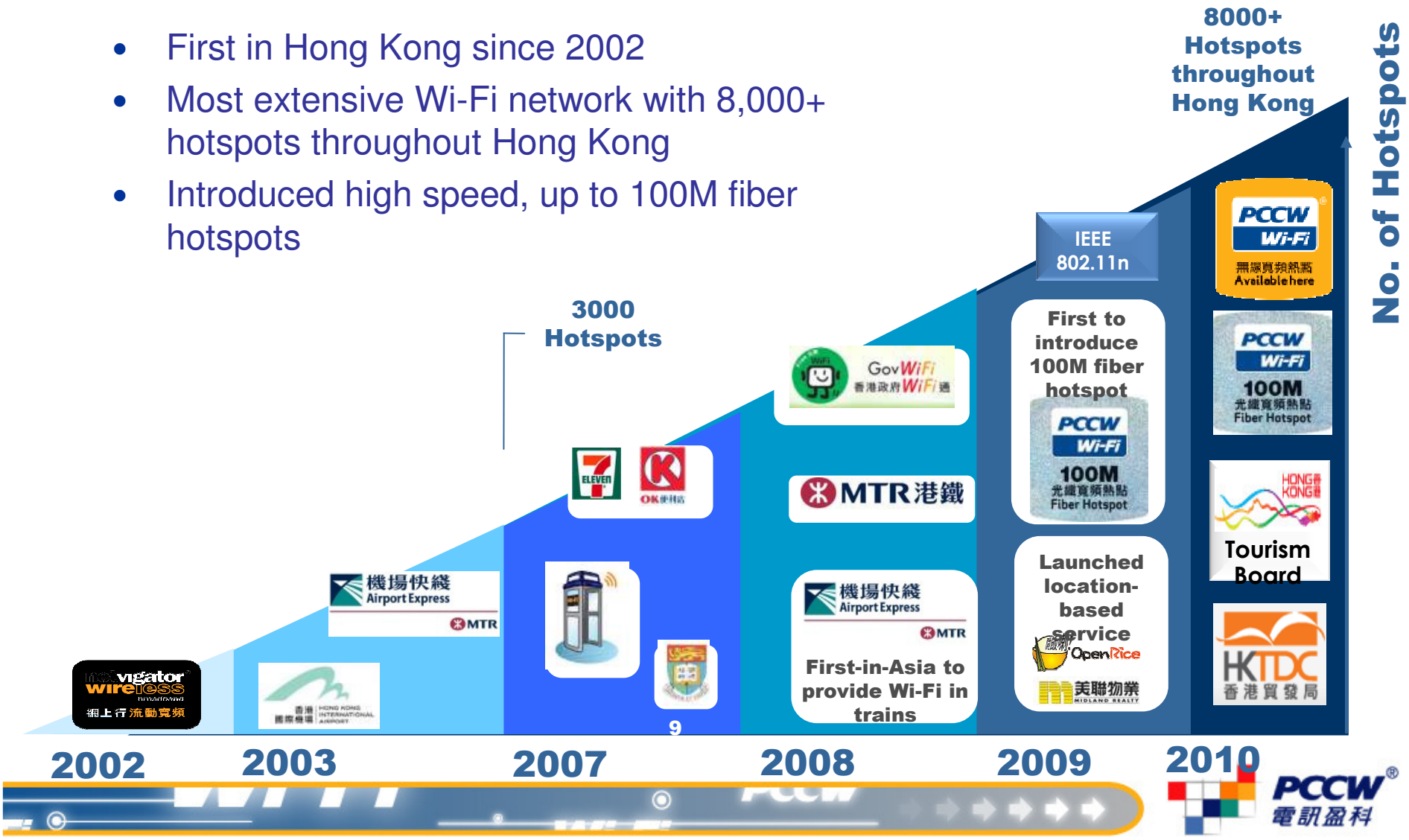
SAFE Wi-Fi @ Public Hotspots

Dr. Katherine Kwan
VP, Product Development & Management
Consumer Group

Explosive Increase in Wi-Fi Use for Consumers

- First in Hong Kong since 2002
- Most extensive Wi-Fi network with 8,000+ hotspots throughout Hong Kong
- Introduced high speed, up to 100M fiber hotspots

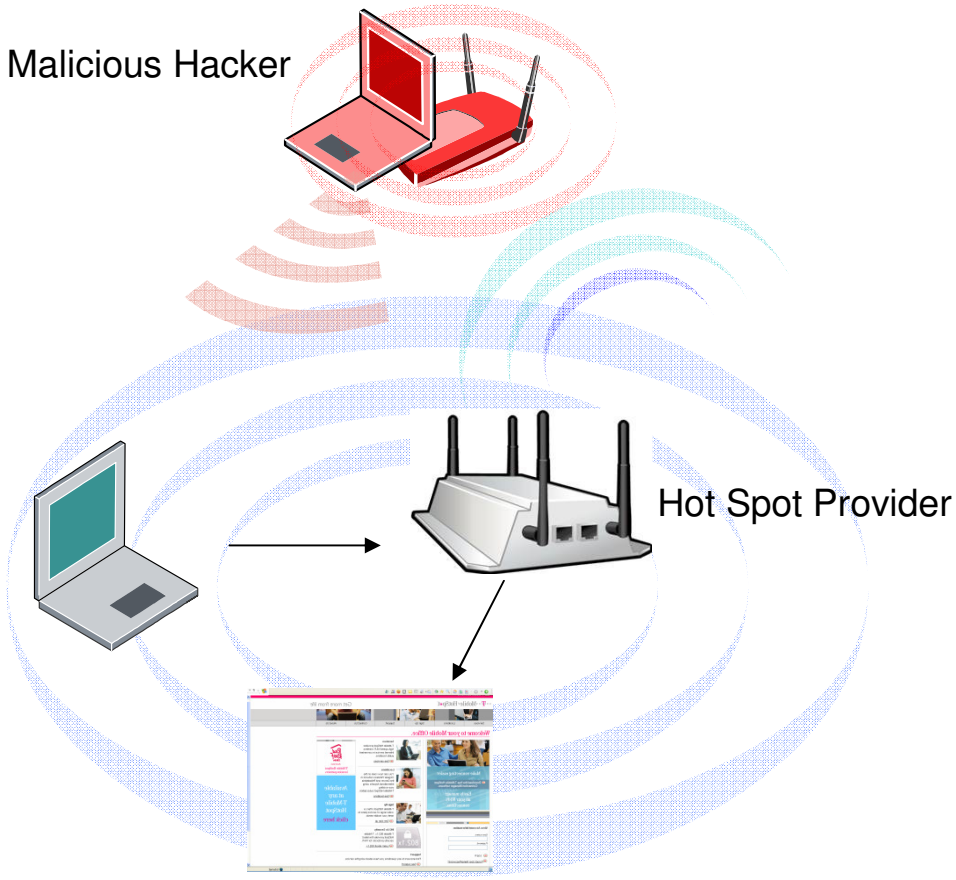


Explosive Increase in Wi-Fi Use for Consumers

- High penetration of Wi-Fi enabled smart phones and portable gadgets (e.g. iPod, netbooks, tablets)
  - 2010 Smartphone www shipment reaches 240M, which is 18% of total mobile shipment and 40% growth from 2009;
  - More powerful tablets will be expected in 2011
- Public transports, shopping malls, restaurants and other owners of public venues are seeing Wi-Fi hotspot service as one of the basic facilities, like air-conditioning
- Continuous investment from service providers in hotspot rollout
- Mobile operators are seeing hotspots as effective means for traffic off-load

Mobile / Wireless Devices are the new Targets of Intruders

- It is not just about exposing your Wi-Fi subscription password;



It does not take a Genius to Perform Wireless Hacking

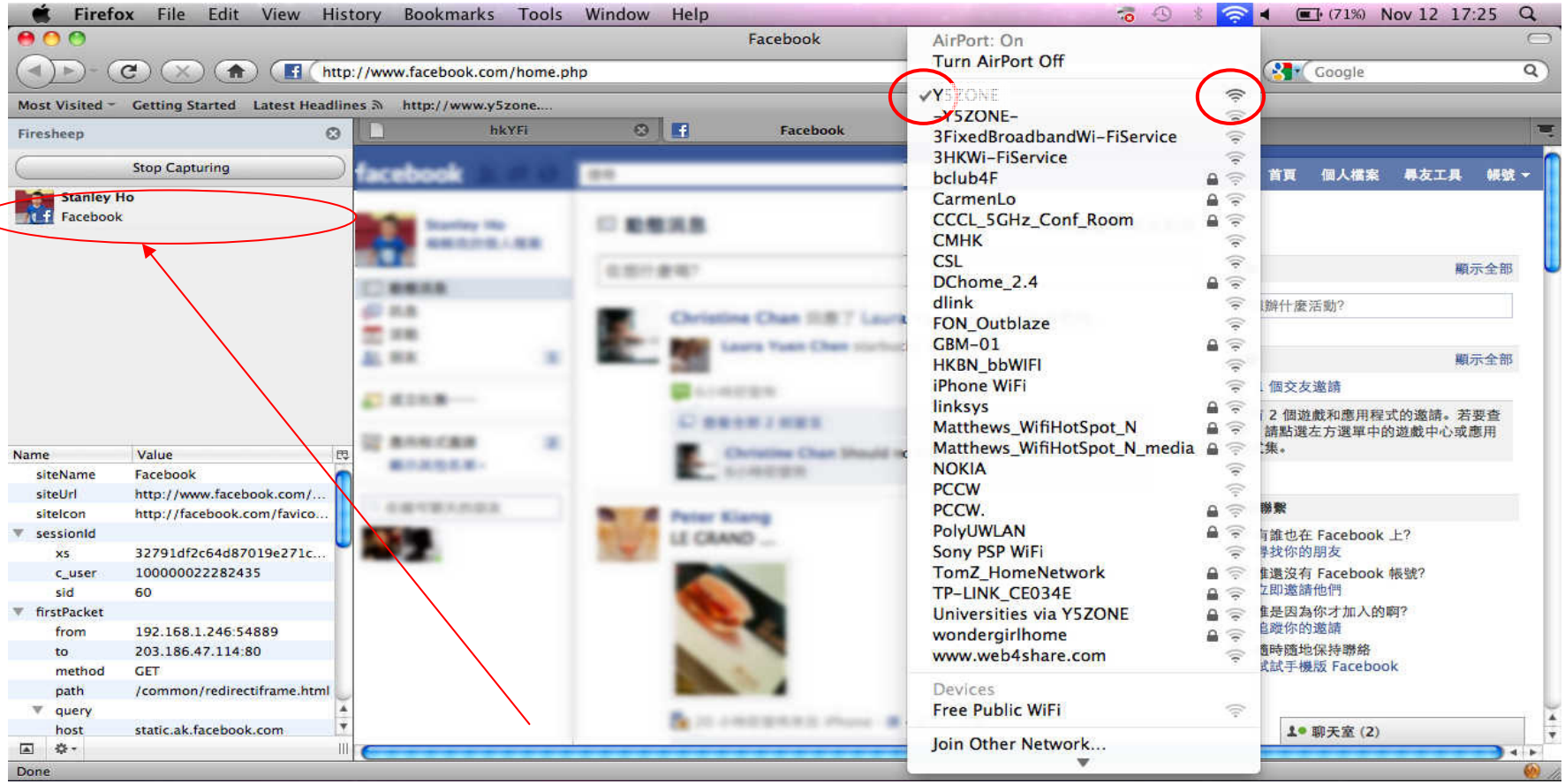
- Unsecured wireless information packets can be easily captured and decoded to show passwords or contents over applications like facebook, etc.., using readily available applications;
- E.g. “Firesheep” is an application freely available on web that allows an average computer user to hack other user under the same hotspot, without wireless protection.

Firesheep Testing procedures:

1. Both victim and hacker connected to same Wi-Fi network
2. Hacker using Firefox & Firesheep add-on and start to capture http packet
3. Victim surfs Facebook & Hotmail…etc.
4. Hacker click on captured session to access victim’s Facebook & Hotmail

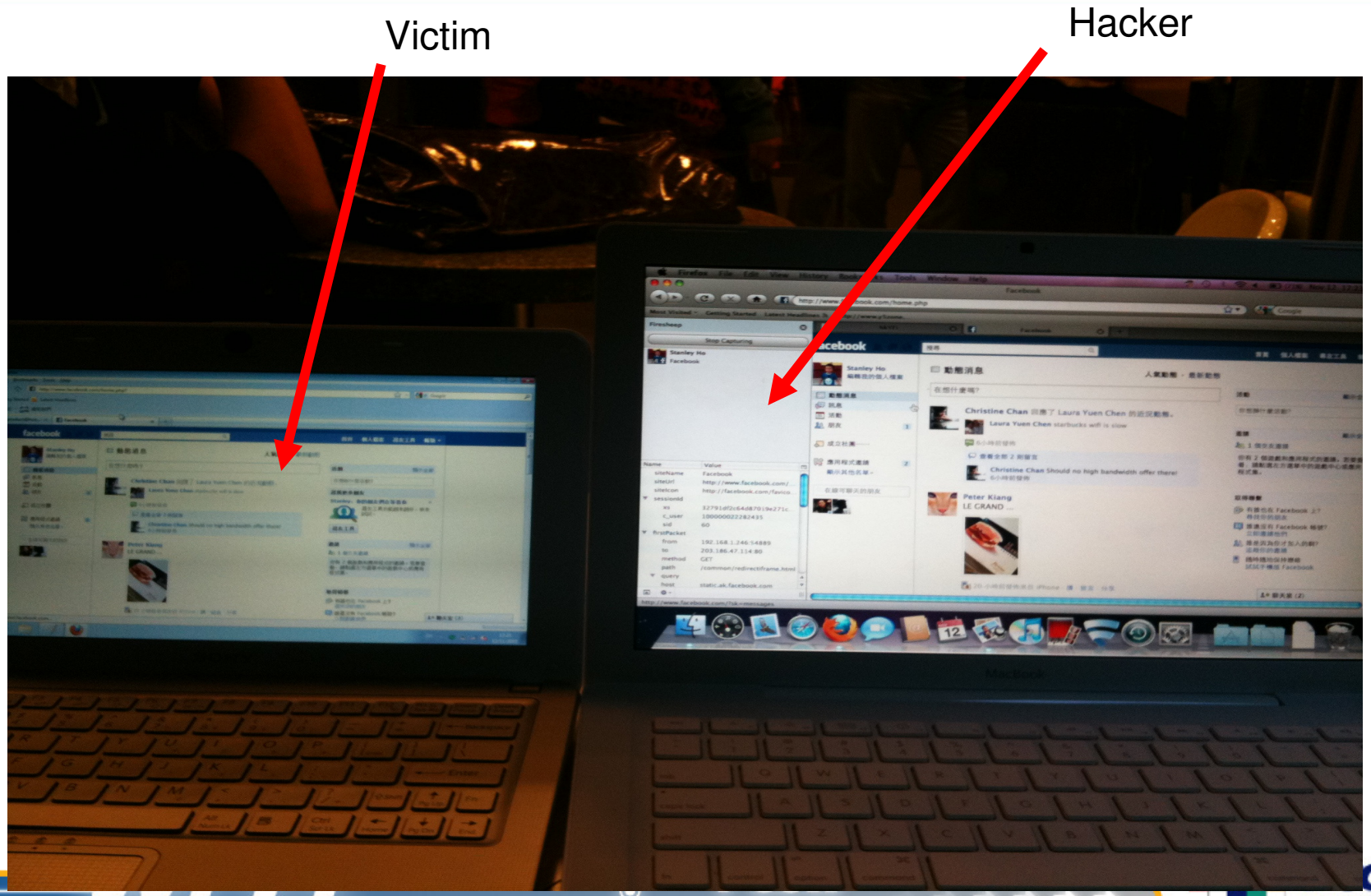
It does not take a Genius to Perform Wireless Hacking

Hacking with Firesheep at a free, unprotected hotspot



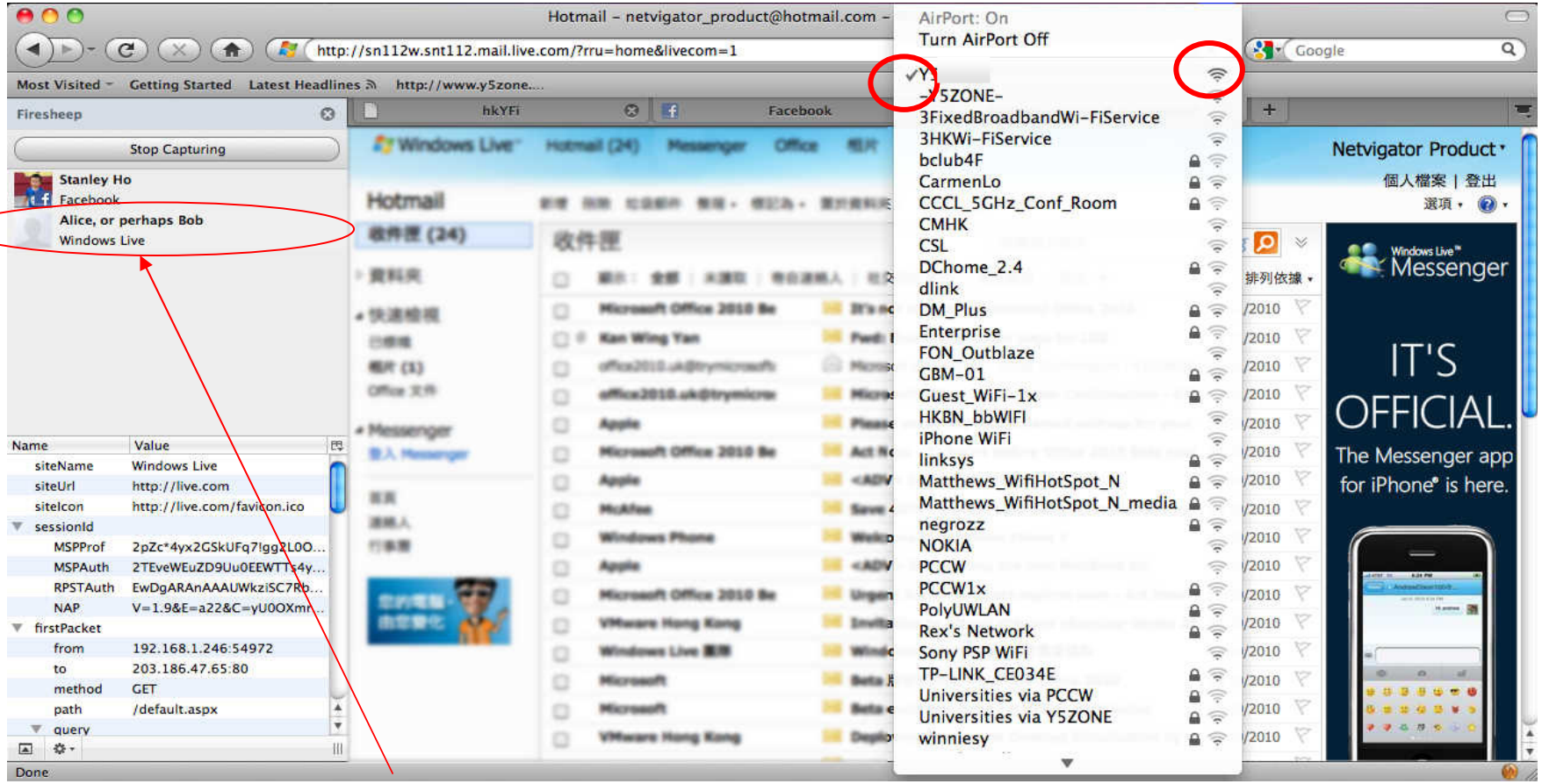
Victim's Facebook session

It does not take a Genius to Perform Wireless Hacking



It does not take a Genius to Perform Wireless Hacking

Using Firesheep to intrude victim's hotmail session



Victim's Hotmail session

It does not take a Genius to Perform Wireless Hacking

Cannot capture any session when access through the protected air path on “PCCW1x”

Rouge/ Fake APs

- Hackers may also setup ‘rouge AP’ with SSID names like ‘Free WiFi’ to capture users traffic;
- Ever noticed the SSID’s like “Free Public Wi-Fi” or “hpsetup” ?
  - They are ad-hoc mode Wi-Fi (broadcasted from clients, without real AP infrastructure)
  - Result of a Windows OS bug
  - No direct harm to end users but hackers can further leverage on this well propagated SSID to setup rouge APs
- End users have to be careful on choosing the genuine hotspots and not to disclose sensitive / personal data at public venues

Options are Available to the Consumers

- Free or paid hotspots are widely available, with different login/ authentication methods …But not all are secured !
- Users could have option to turn on wireless protection or use VPN connection
  - Trade-off between performance and security – strong encryption solution could be very secure, but the heavy overheads would impair network performance
  - Complexity of solution is also dependent on type of device/ OS
- Hotspot service providers should have implemented necessary network security measures
  - Firewall protection
  - Wireless Intrusion Detection & Protection system
  - User Authentication & Usage log
  - **Wireless Encryption**

Options are Available to the Consumers

- PCCW offers various choices of authentication and wireless protection methods to suite different type of user requirements

IEEE 802.1x EAP-MSCHAPv2 / EAP-PEAP supported

-Forced Portal user login with option to turn on wireless protection

- Single Device Plan: initial setup with security credential and choose SSID with protection on

PCCW mobile®

IEEE 802.1x EAP-SIM / EAP-PEAP supported

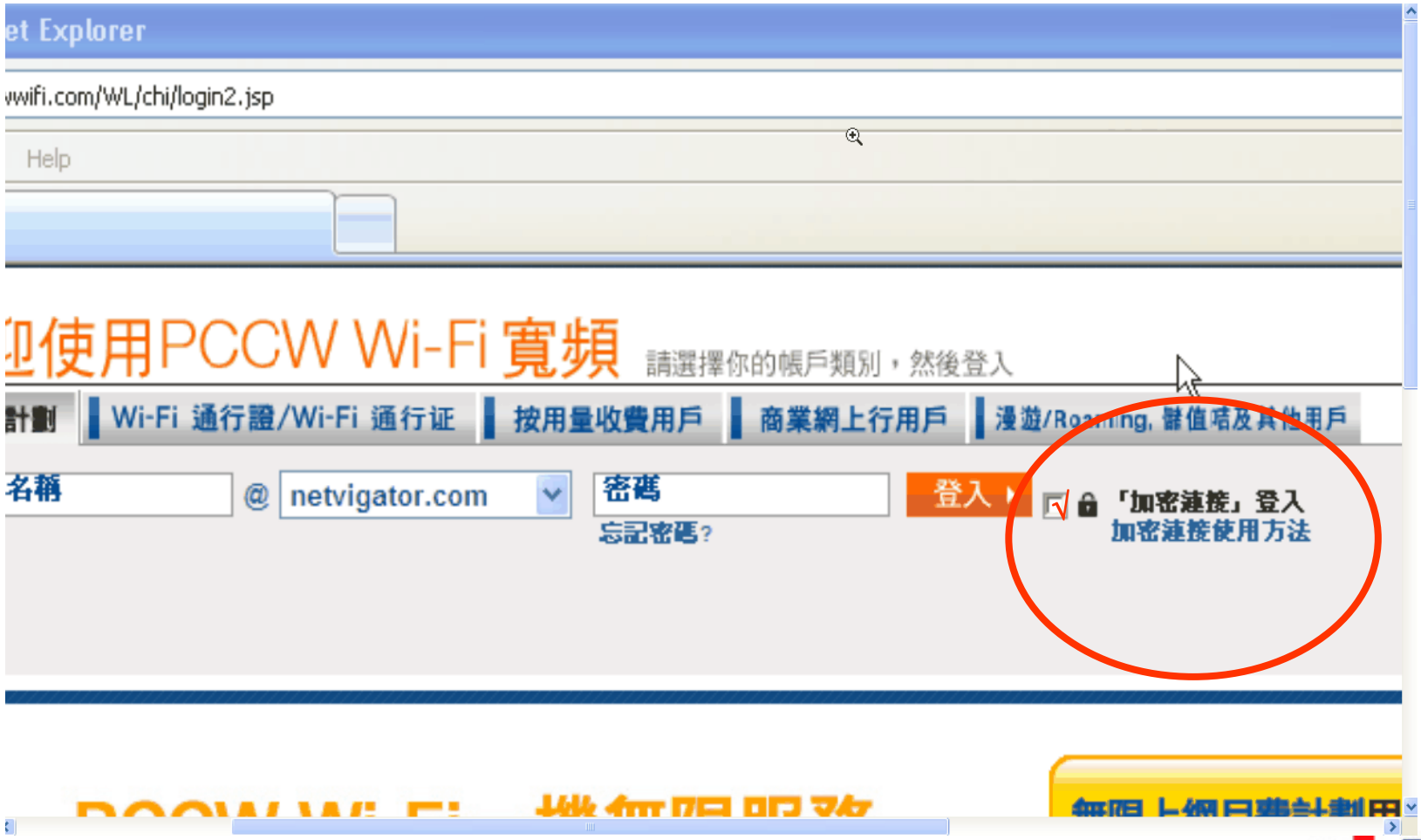
-Mobile Auto Connect – authenticate with SIM

-Netvigator Everywhere – authenticate with SIM

PCCW® 電訊盈科

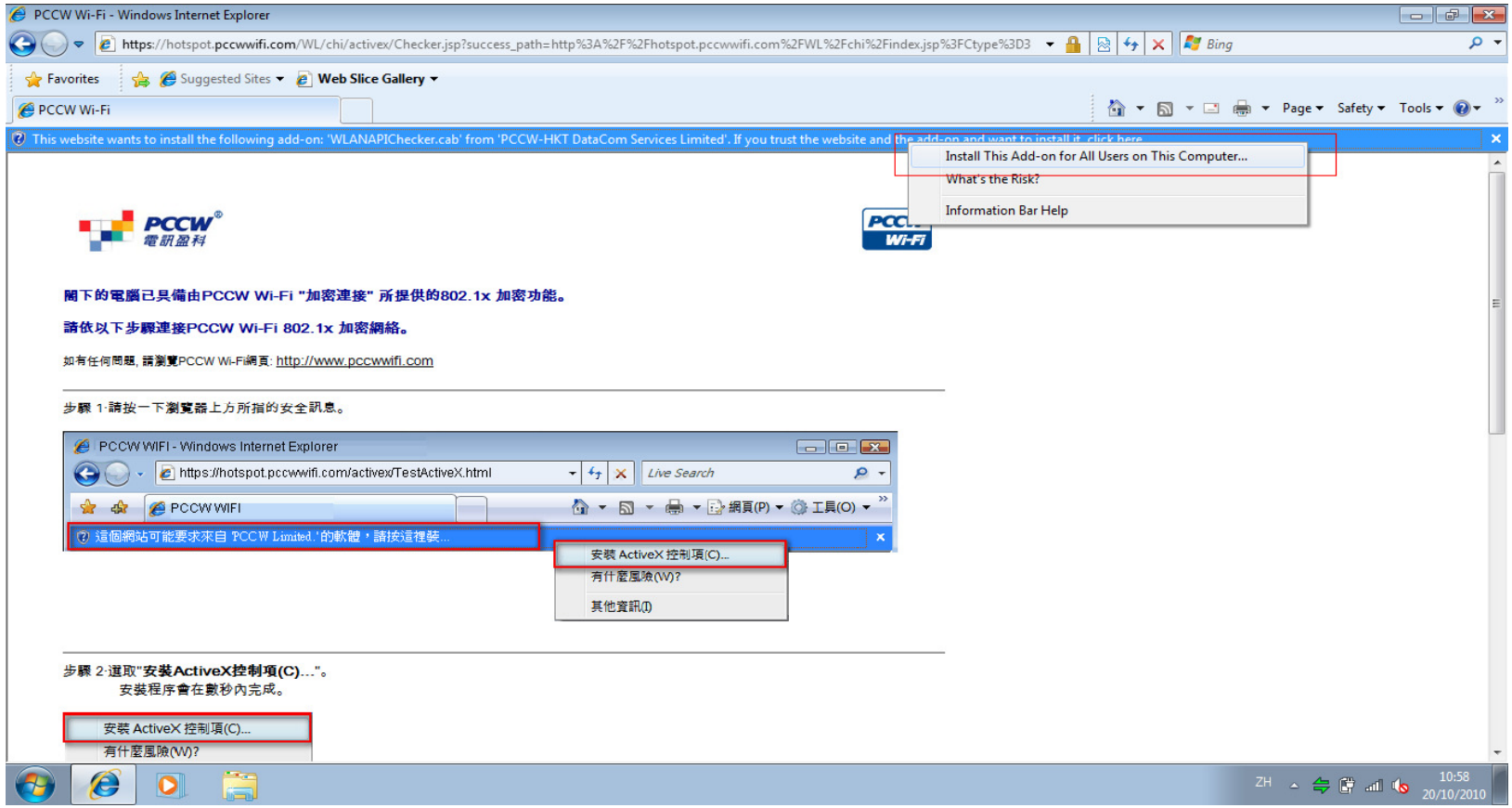
PC Set-up

- Secured connection option on Forced Portal



PC Set-up

- Active-X installation (one-time) on PC



Auto redirect to “PCCW1x” SSID after set-up

Mobile Set-up for Auto Connect (one-time) with EAP-SIM

1. 登入「網頁瀏覽器」(Safari)，輸入 http://wap.pccwmobile.com 到「PCCW mobile頻道」，並選擇「服務專區」

2. 選擇「 Auto Connect」

3. 按「下載」

Mobile Set-up for Auto Connect (one-time) with EAP-SIM

4. 按「 安裝 」

5. 開啟Wi-Fi後選擇 PCCW1x網絡

Mobile Set-Up for Auto Connect (one-time)

User Tips

- **Secure Your Real-time Traffic**
  - Use a protected connection.
  - Don't visit any private or sensitive Web site unless it's secured (for example, implementing SSL) if you are not using a VPN.

- **Prevent Others from Connecting to Your Laptop**
  - Disable any sharing of files, folders and services.
  - Use personal firewall software.
  - Make sure your operating system is kept up to date.

THANK YOU