



SAFE Wi-Fi @ Public Hotspots

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



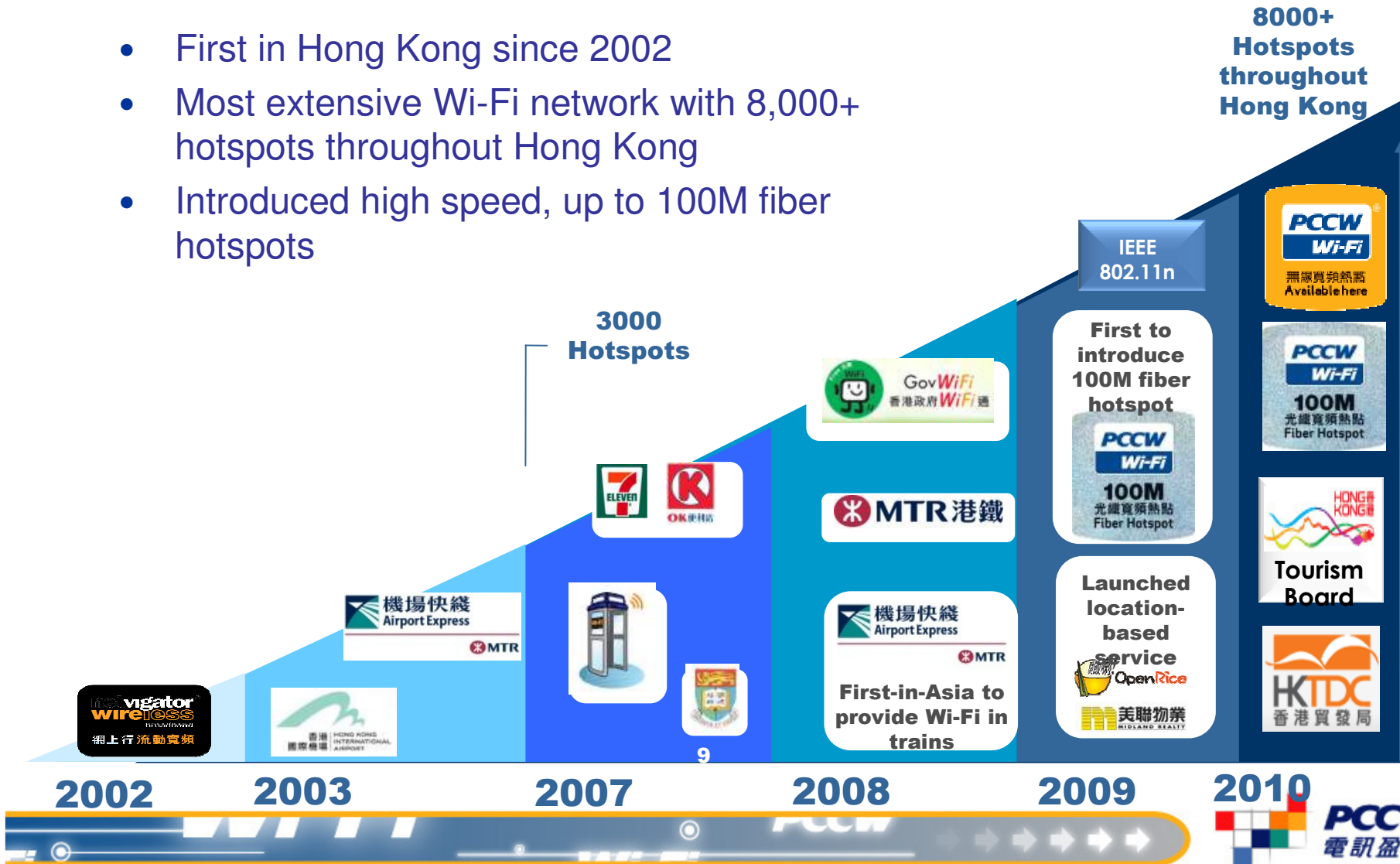


Explosive Increase in Wi-Fi Use for Consumers

- 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

8000+ Hotspots throughout Hong Kong

No. of Hotspots



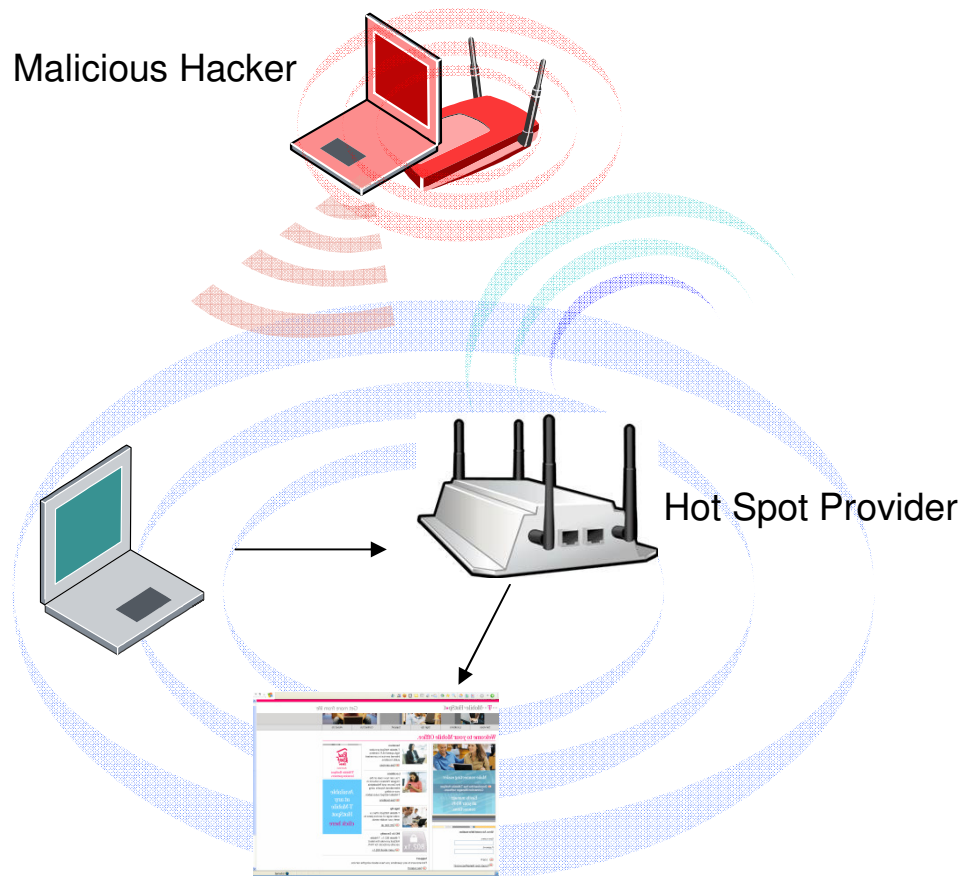


Explosive Increase in Wi-Fi Use for Consumers

- 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.

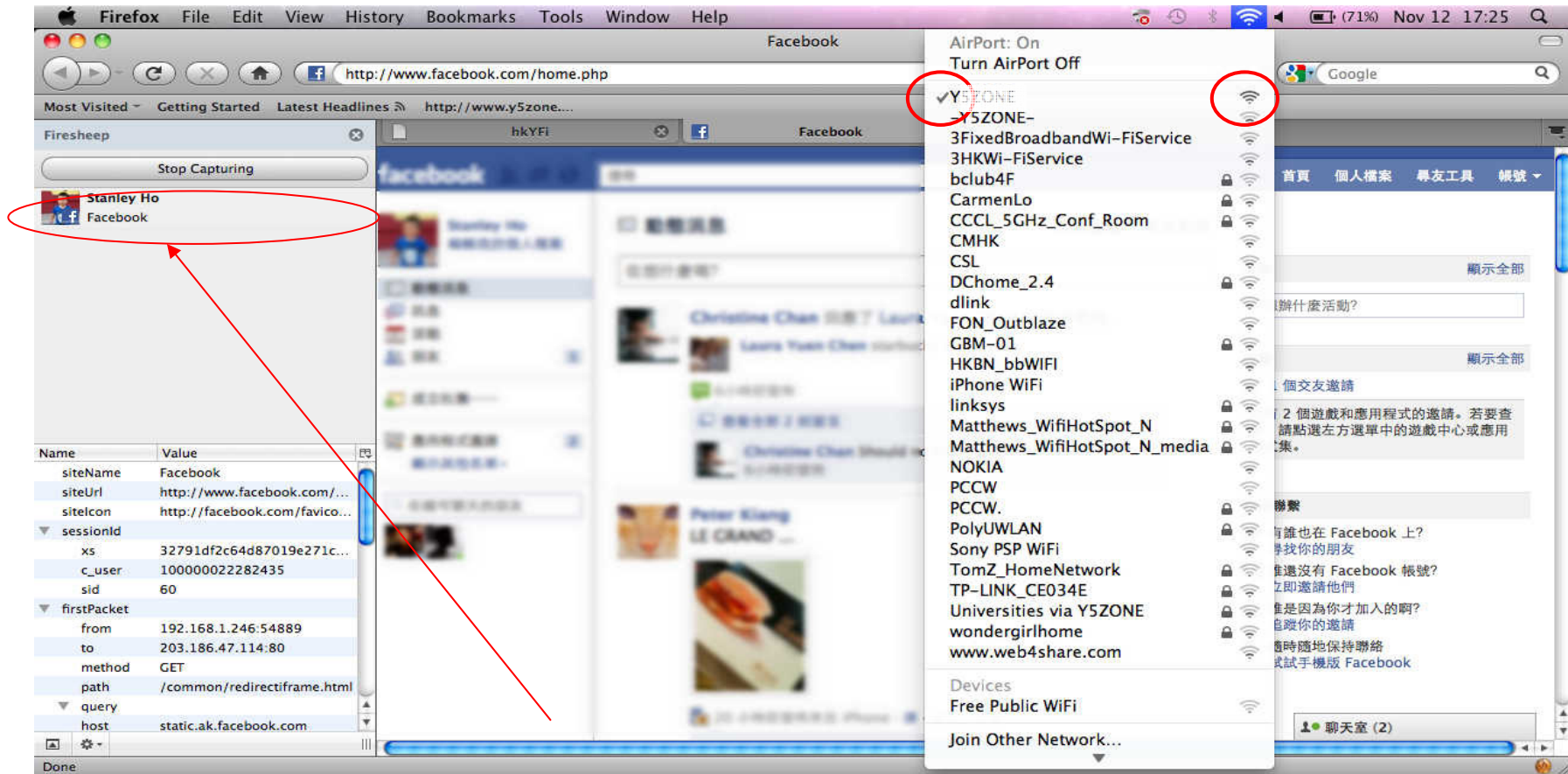
Firesheep Testing procedures:

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

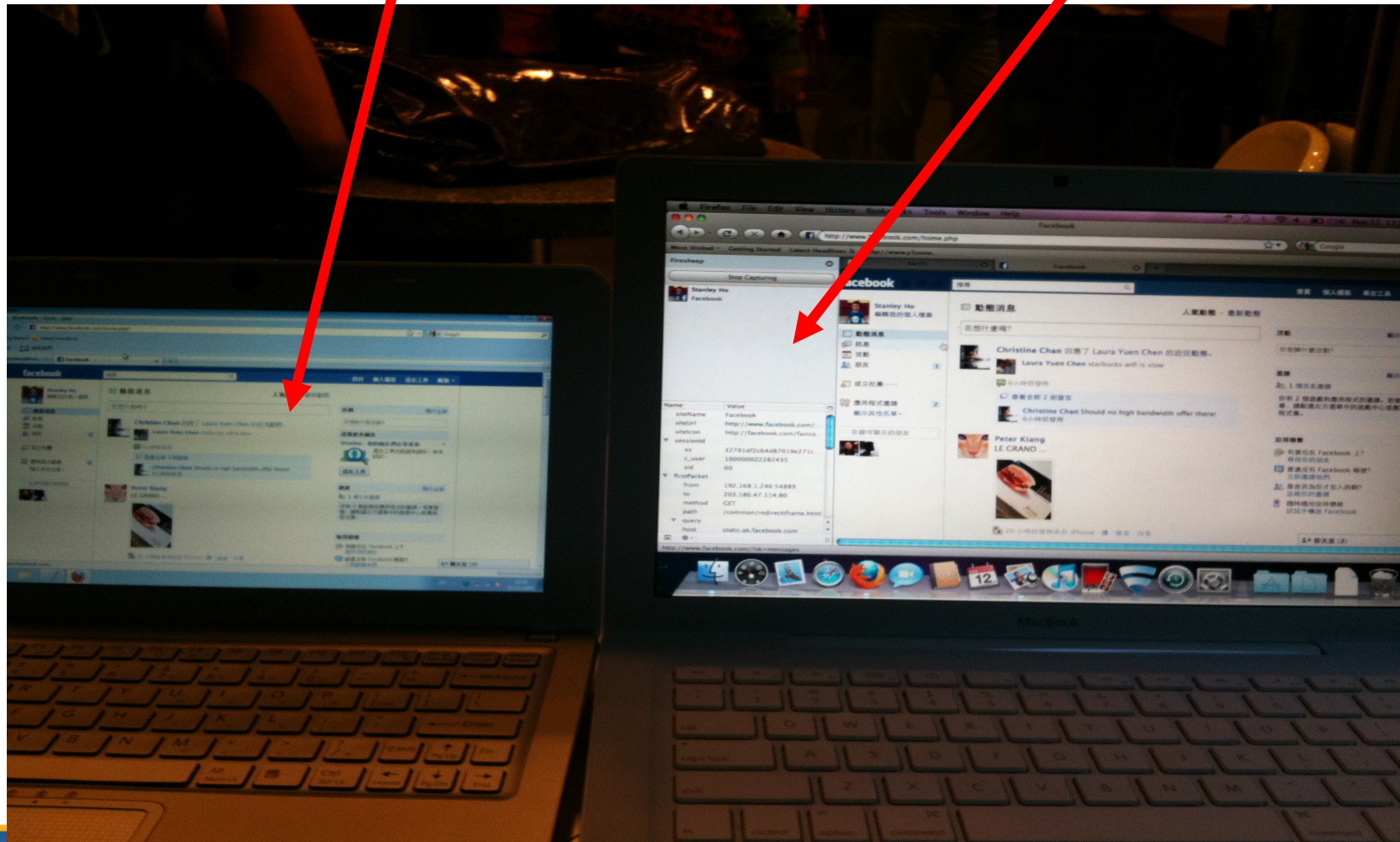


Victim's Facebook session

It does not take a Genius to Perform Wireless Hacking

Victim

Hacker





It does not take a Genius to Perform Wireless Hacking

Using Firesheep to intrude victim's hotmail session

Hotmail - netvigator_product@hotmail.com -
http://sn112w.snt112.mail.live.com/?rru=home&livecom=1

Most Visited - Getting Started Latest Headlines http://www.y5zone...

Firesheep

Stop Capturing

Stanley Ho
Facebook

Alice, or perhaps Bob
Windows Live

Name	Value
siteName	Windows Live
siteUrl	http://live.com
siteIcon	http://live.com/favicon.ico
sessionId	
MSPProf	2pZc*4yx2GSkUFq7lgg2LOO...
MSPAAuth	2TEveWEuZD9Uu0EEWTTs4y...
RPSTAuth	EwDgARAnAAAUWkziSC7Rb...
NAP	V=1.9&E=a22&C=yU0OXmr...
firstPacket	
from	192.168.1.246:54972
to	203.186.47.65:80
method	GET
path	/default.aspx
query	

Hotmail

收件匣 (24)

Microsoft Office 2010 Be
Kan Wing Yan
office2010.uk@trymicrosoft
office2010.uk@trymicro
Apple
Microsoft Office 2010 Be
Apple
HuAfie
Windows Phone
Apple
Microsoft Office 2010 Be
VMware Hong Kong
Windows Live 團隊
Microsoft
Microsoft
VMware Hong Kong

Hotmail

收件匣

Microsoft Office 2010 Be
Kan Wing Yan
office2010.uk@trymicrosoft
office2010.uk@trymicro
Apple
Microsoft Office 2010 Be
Apple
HuAfie
Windows Phone
Apple
Microsoft Office 2010 Be
VMware Hong Kong
Windows Live 團隊
Microsoft
Microsoft
VMware Hong Kong

AirPort: On
Turn AirPort Off

✓
Y
- YZONE-
3FixedBroadbandWi-FiService
3HKWi-FiService
bclub4F
CarmenLo
CCCL_5GHz_Conf_Room
CMHK
CSL
DHome_2.4
dlink
DM_Plus
Enterprise
FON_Outblaze
GBM-01
Guest_WiFi-1x
HKBN_bbWIFI
iPhone WiFi
linksys
Matthews_WifiHotSpot_N
Matthews_WifiHotSpot_N_media
negrozz
NOKIA
PCCW
PCCW1x
PolyUWLAN
Rex's Network
Sony PSP WiFi
TP-LINK_CEO34E
Universities via PCCW
Universities via Y5ZONE
winniesy

Google

Netvigator Product
個人檔案 | 登出
選項

Windows Live™
Messenger

IT'S OFFICIAL.
The Messenger app for iPhone® is here.

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

- Secured connection option on Forced Portal

Internet Explorer

http://www.pccw.com/wifi.com/WL/chi/login2.jsp

Help

歡迎使用PCCW Wi-Fi 寬頻 請選擇你的帳戶類別，然後登入

計劃 | Wi-Fi 通行證/Wi-Fi 通行証 | 按用量收費用戶 | 商業網上行用戶 | 漫遊/Roaming, 儲值咭及其他用戶

名稱 @ netvigator.com 密碼 登入

忘記密碼?

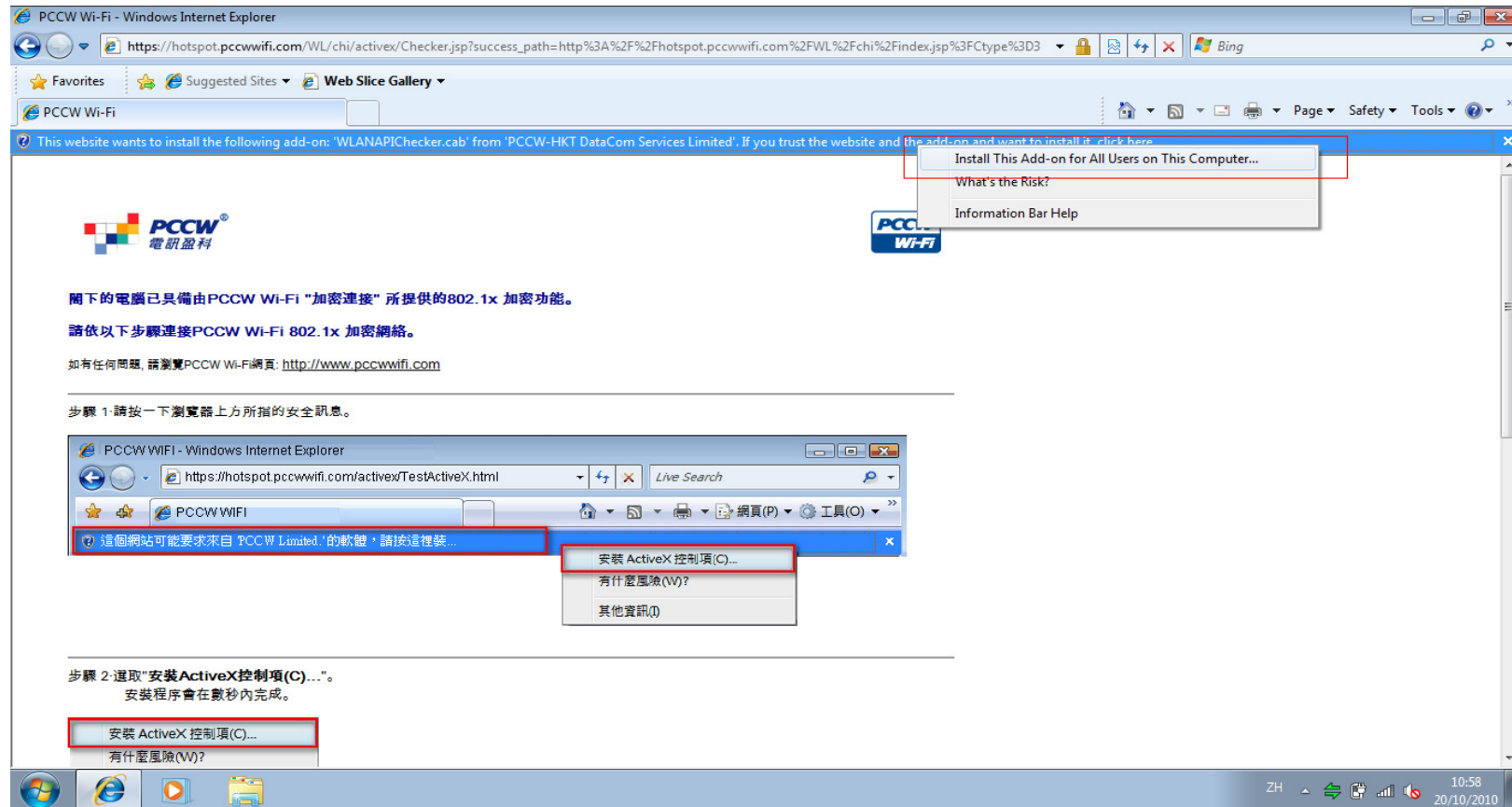
加密連接 登入 加密連接使用方法

PCCW 電訊盈科



PC Set-up

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

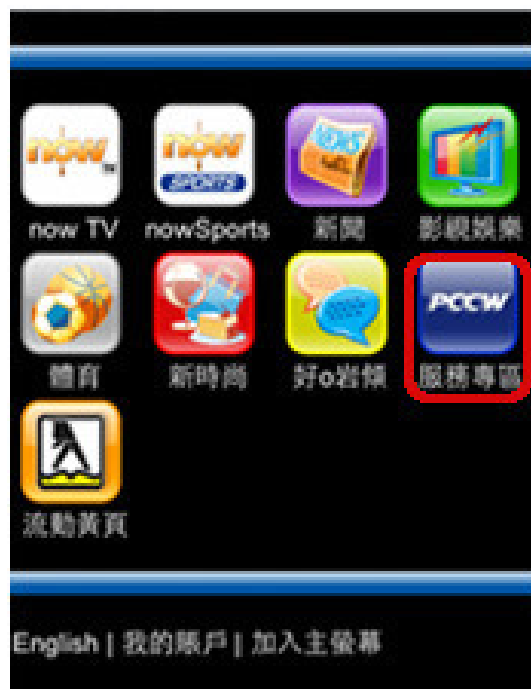


Auto redirect to "PCCW1x" SSID after set-up





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.



保護個人資料 上網安全可靠
 選擇“PCCW1x”登入網絡
 即可享用802.1x加密模式* 防止私隱被盜

POWER UP WITH PCCW WI-FI
 即時以手機免費試用2個月

保障全面	8000+熱點	100M* 極速光纖	AUTO Click登入
------	---------	------------	-----------------

*有關 802.1x 加密連接使用方法，請瀏覽www.pccwwifi.com。*PCCW Wi-Fi 100M 為網絡服務並需同時指定PCCW Wi-Fi熱點。網絡速度並不與個別客戶於熱點所連接的網絡相同。而客戶之網絡速度受使用者的設備、網絡技術、個別網絡及軟件之使用、網絡設定及實際需要、使用量及其他外在因素尚有所影響。優惠受有關條款及細則約束。

申請專線 **2888 1888** 後按8 或親臨 **電訊盈科專門店** 盡情體驗 www.pccwwifi.com

ONLY PCCW



THANK YOU

