Wireless Network

Best Practices for General User

In Hong Kong, the number of Wi-Fi access points (hotspots) has reached 31,000 in 2015[1]. Unfortunately, not all of them are well-protected. In fact, wireless broadcasts information in all directions and thus transmission can be received by anyone in the range. This kind of communication is easy to listen, modify and the information can even be stolen from an unprotected system. This newsletter will focus on the best practices to protect data while using wireless network.

Tips for Secure Wi-Fi Access

Public hotspots are not as secure as a home network. Usually, laptop, tablet and smartphone default settings are not secure enough to protect users. There is a list of settings that can be applied on all devices to improve users' security[2].

- **Turn off Wi-Fi when Unused**

When Wi-Fi is not in use, it is better to turn it off. This prevents other people from snooping around. On Windows 7, just right click on the Wi-Fi icon and select Wi-Fi off. On Mac OS X, click on the Wi-Fi icon to turn it off.

- **Turn off Sharing**

When sharing is available, two people connected on the same network can have access and even modify one another's public files. On Windows 7 (*Figure 1*), sharing settings can be found at the control panel under the "Network and Sharing Center" section in "Network and Internet". Finally select "Change Advance Sharing Settings" and disable all the public sharing options. In OS X, ensure that no options are selected in "System Preferences" > "Sharing". To prevent people from searching a machine on the network, "network discovery" option must be disabled.

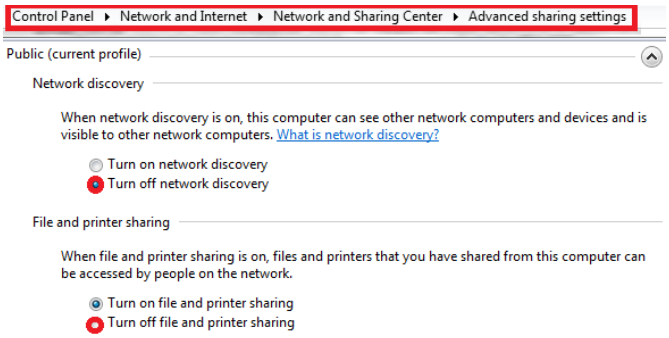

Figure 1 - Sharing settings

- **Disable Auto-connection**

Enabling this setting allows devices to connect to any Wi-Fi without asking permission. To remove this option, the auto-connection setting has to be turned off (on Apple iPhone it is called "Ask to Join Networks", in *Figure 2*). If this option is not available in the Wi-Fi settings, it means that it is already disabled.

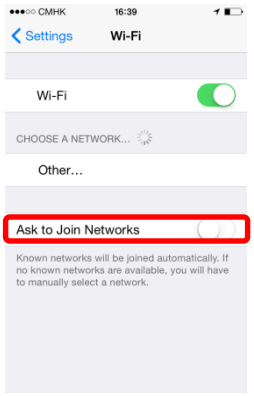

Figure 2 - iPhone auto-connection

- **Enable Firewall**

Firewall should always be enabled to protect devices. For Windows 7, firewall settings are in the control panel under the "System and Security" section in "Windows Firewall". For Mac OS X, it is located in "System Preferences" and then in the "Security & Privacy" part. Turn it on in the Firewall table. If these settings are grayed out, click on the padlock icon in the lower left, confirm the action with a password and start again.

- **Drivers & System Update**

OS and drivers must be updated as soon as they are available. In fact, they will enhance the system productivity and fix security issues. Applications version must also be kept up-to-date.

- **Wi-Fi Setting Automation**

On Windows 7, after connecting to an unknown Wi-Fi network, a pop-up will appear to inquire about the nature of the network: be it Home, Work or Public network. The answer then determines the security settings of this connection.

- **VPN**

A VPN (Virtual Private Network) will encrypt the traffic between computer and the Internet and thus, will offer the security of a private network. This also works on mobile phone which protects mobile applications users. CyberGhost and SurfEasy are two examples of free VPN.

Case study – Intrusion in French universities computer system[3]

In 2010, Nice University decided to complaint for the hacking of its websites. Two years later the hacker was finally arrested. They had difficulty finding him because he used free hotspots and unsecured Wi-Fi to complete his felony. To find these unsecured wireless networks he drove around (wardriving). He succeeded to crash some university servers and to accede to sensitive data. Some other French Universities had been compromised during this period. Even if he gathered a lot of information about people as name, address, he didn't use them. He declared that he did it as an intellectual challenge. He was sentenced to a three-year prison term.

Unsafe Networks & Websites Banned

- **Never Connect to Wi-Fi Access Point without Authentication Key**

A Wi-Fi access point without authentication process is not protected. In fact, anyone connected on this kind of network can probably mouse around all data, as e-mail content, login, password, are transferred within the network.

- **Beware of Fake Hotspot**

Logging into an unknown or untrusted hotspot should be avoided. In a café better ask the staff before connecting to their network. Logging into an unsecured hotspot must be prohibited. To check the security level of a hotspot, on Windows, let the cursor hover over the selected access point and a window will appear showing the security information. WPA2 is the most secure one; try always to log into well-encrypted networks (*Figure 3*).

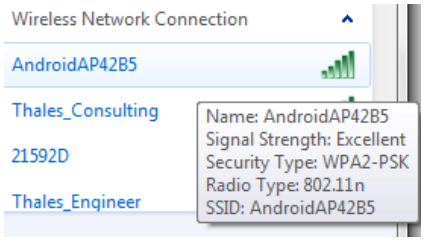

Figure 3 – Wi-Fi Security Type

- **HTTPS and SSL with trusted Certificates**

Logging into encrypted websites (URL address that starts with HTTPS instead of HTTP, in *Figure 4*) will increase users' security level. For a safe access to mail on desktop client (e.g. Microsoft Outlook), SSL encryption has to be activated. This will prevent intruders from reading emails but also stealing login and password. This can be enabled in the setting accounts section. In Microsoft Outlook, accounts have to be encrypted one by one. To do it, select the following path: tools > accounts the Select the right account, properties > Advanced. Finally, tick the SSL box.

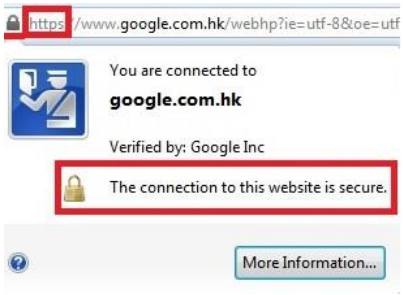

Figure 4 – Well-encrypted website

Besides HTTPS, certificates also provide indications on website security. A click on the little icon just at the beginning of the URL address will give precise information about it. As certificates are approved by different browsers, each one uses its own icons to define the level of security from the untrusted to the most secure websites (*Figure 5*).

Figure 5 – Mozilla Certificates Icon

- **Never Use Communication Mobile Apps at Untrusted Network**

Case study – A student hacked his university network[4]

A student at Florida State University Panama City hacked the university wireless network and had redirected users to a porn site for about thirty minutes. He declared that he did it to expose the lack of security in its university wireless network. As a result, Florida State University Panama City improved its wireless network security and now authentication is required to log into the network.
The student has been suspended and is facing felony charges for "offenses against computer users".

Home Wireless Configuration

It is also important to secure the Wi-Fi connection at home. Otherwise it would be as dangerous as a hotspot. To well secure a router some easy rules must be followed[5].

- **Secure Home Router**

Firstly, the router default administrator SSID and password must be modified. The SSID is the router name. In fact, hackers have precomputed breaking functions for the top 1000 most popular SSID. Selecting a name that is easy to remember is a good idea. However, the SSID should not be a dictionary name and it should not involve and give out any personal information. To reduce risk, the default password must be changed to a stronger one.

Hiding the SSID will prevent people from finding a Wi-Fi. To connect to a hidden Wi-Fi, the SSID has to be entered manually in the following path: "Control Panel" > "Network and Sharing Center" > "Set up a new connection or network" > "manually connect to a wireless network".

Regular update of the Wi-Fi router firmware and enabling its firewall will also shield users from some attacks, as updates will fix all the vulnerabilities detected by the router's firmware.

- **Use Encryption**

High encryption is also important to enhance the security level. Several choices of security level are available during the router settings. The most secure choice among WEP, WPA and WPA2 is WPA2. If it is not available, choose WPA and then WEP as the last resort. For the encryption type, AES algorithms should be preferably used for WPA2 (*Figure 6*). Other options, such as TKIP, are older and less secure.

Figure 6 – Choice of Home Security Level

- **Network Access Control**

Once all the main settings are done, network security can still be improved by limiting its access.

Devices allowed to connect to a network can be limited by filtering their Mac addresses. The easiest way to do that is to connect all devices to the network; then open the DHCP client table in Status or Local Network section, copy their Mac address and paste them into the Wireless MAC filter section of the router.

Router should be disabled if there is no occupant in the room for extended periods (a few days, for example). Otherwise, in the case of regular planning, some routers provide the option of controlling Wi-Fi availability time according to pre-set schedule.

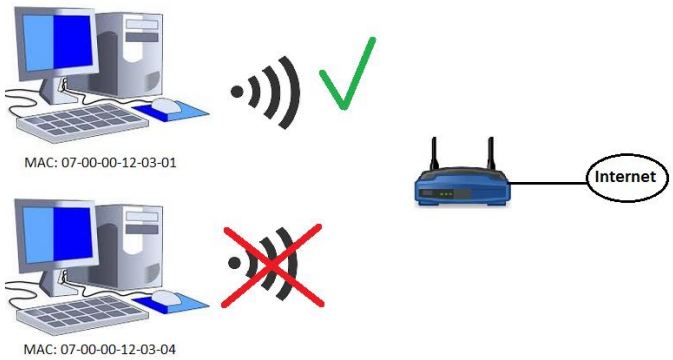

Figure 7 – Network access control by MAC address filtering

In *Figure 7*, the first computer can access the network because its MAC address belongs to Wireless MAC filter section of the router. The second computer MAC address is not registered. Therefore it is denied the connection to this wireless network.

Eduroam

Eduroam which means Education Roaming is a world-wide wireless access for the international education community[6]. In fact, if a university belongs to this consortium its students will be able to access Wi-Fi on campuses around the world. Even their guests, who belong to another participating university, will also be able to connect to the campus network. Regardless of their physical location, they can simply select the Wi-Fi network untitled Eduroam and enter their university account credentials (for example UID@hku.hk and the corresponding password) and gain access to Internet as they wish.

For a connection abroad, the authentication is done by the user's university but the authorization to accede to the network is given by the host. This wireless network is secured by WPA2. As discussed, this is the most secure setting.

Security measures vary among universities – there is no global standard. For instance, the frequency of password renewal can be every 3 months for a university and every year for another one. But students from both universities will have access to Eduroam network. Eduroam is available in 71 countries, indicated by dark blue on the map in *Figure 8*. Eduroam is available in 15 higher education institutions in Hong Kong, including Hang Seng Management College and Hong Kong Academy for Performing Art since January 2015.

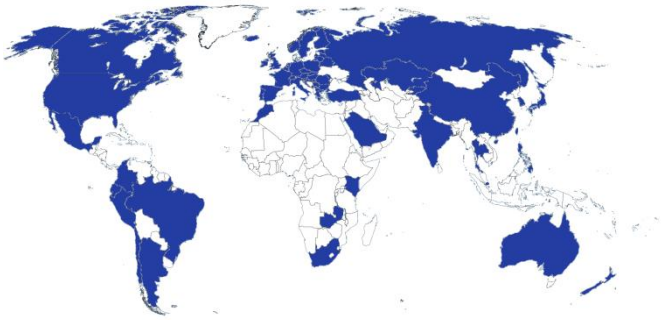

Figure 8 – Countries in which Eduroam is available

Conclusion

Wireless network allows people to access the Internet from almost everywhere. Nevertheless, security threats should not be ignored. Logging into unsecured hotspots should be avoided and sensitive data transmission must only be done at home or through networks that are encrypted and reliable. Follow the best practices and keep the network away from probing eyes.

References

1. "Location Information of WiFi Access Points" OFCA, WEB, 8 MARCH 2015. Web. 16 June 2015
2. "14 tips using public Wi-Fi- networks" March 2014. Web. 9 June 2015
3. "Three years of jail for a hacker" Le Journal de Soane et Loire. 7 March 2015. Web. 11 June 2015
4. "Student hacks Florida university's wireless network", NY Daily News, 12 March 2013. Web. 10 June 2015
5. "How to secure your home wireless network router" 16 March 2015. Web. 10 June 2015
6. "Eduroam.org" 9 June 2015. Web. 10 June 2015

Copyright Statement