CyberSecurity MALAYSIA

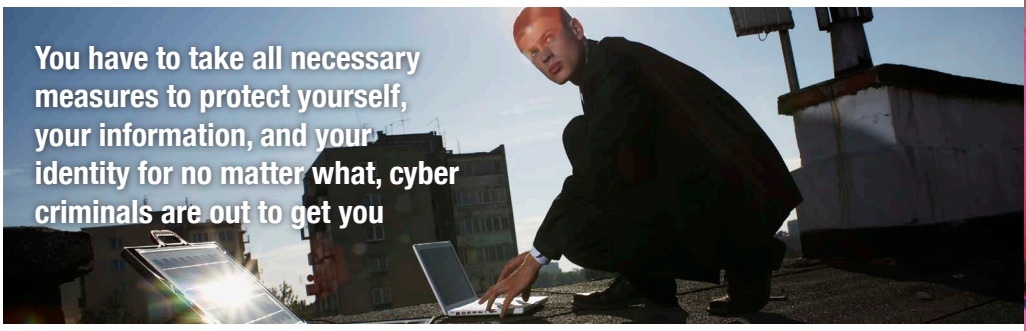
An agency under MOSTI

Wi-Fi

NOTHING IS PRIVATE WHEN DONE IN PUBLIC

Securing Our Cyberspace

WI-FI: NOTHING IS PRIVATE WHEN DONE IN PUBLIC



Wi-Fi is a popular technology that allows Internet-enabled devices (notebooks, smartphones, tablets, etc.) to exchange data or to connect to the Internet wirelessly, using radio waves. Wi-Fi is a service that is available at home, work, cafes, restaurants, airports, hotels and other public places.

The list of activities that can be performed, when connected to Wi-Fi, are endless. Office work can be completed and emailed to bosses with ease, from anywhere and at any time. In some public places, businesses provide public Wi-Fi to attract patrons. Patrons can leisurely enjoy the flexibility of surfing the Internet while enjoying a cup of coffee. This service is usually available for free but at certain places, payment for access is required.

However, this flexibility and mobility of Wi-Fi, has also brought about new threats in the physical world, and more dangerously in the cyber world. Unlike Wi-Fi that is used at home whereby only those who are known to us have access, public Wi-Fi connections are shared and accessible by anybody and everybody. Public Wi-Fi users do not have the privilege of managing the security settings of the network i.e. changing network name and changing the encryption to suit their needs.

The evolution of Wi-Fi technology offers innumerable benefits which unfortunately comes alongside risks as well. However, the risks exposed to each individual is largely based upon the attitude they possess. These risks can be minimised, if good habits are practiced as the weakest point in any security-strengthened system is usually the human element. Here are some essential safety tips that can help you enjoy a safer online presence.

BEFORE CONNECTING TO PUBLIC WI-FI

These are several essential safety tips that you can adopt in order to increase the security of your Internet-enabled device before connecting to public Wi-Fi. Before you go online, ensure that your Internet-enabled device fulfils the following:

1. Set Strong Passwords

Setting a strong password will minimise the possibility of a perpetrator cracking your password and subsequently accessing your accounts and exploiting available information. It is recommended that a password should be more than eight characters and should consist of a combination of upper and lowercase letters, numbers and symbols. Have a different password for different accounts. How do you check the strength of your passwords? Try using Password Meter at *http://www.passwordmeter.com/.*

2. Enable Password Protected Screen Saver

Regardless of the type of device you use to surf the Internet when you are in public places, ensure that the device is screen saver protected.

3. Encrypt File and Folders

Encrypt all the important files to protect the confidentiality of the information in the Internet enabled device.

4. Secure Operating System (OS)

Install genuine operating systems for your notebook and devices. This is to ensure that you will receive support and regular updates from the developers. Vulnerabilities increase by the day. Therefore, these updates are crucial for continuous security and enhancement of your operating system and to maintain and ensure optimal performance of your notebook or device.

5. Secure Browser

Ensure that your Internet browser is updated and is the latest version. Devices usually come with a feature that prompts a request to automatically save your passwords and another feature that automatically fills fields entered. These features should be disabled as these features will store your passwords and entries in the cache.

6. Disable Network Discovery

Network discovery enables you to view other computers or devices that are within the same network. It also enables others to view your computer or device

too. This visibility will expose you to threats. Some operating system have by default, disabled the network discovery feature. Before connecting to public Wi-Fi, disable the network discovery feature. The *network discovery setting* is applicable to notebooks regardless of operating system.

7. Turn Off File Sharing

Enabling file sharing when not required exposes and increases the probability of remote logins and also the transfer of malicious data to your device. It also enables others to have access to your files and folders. Disable file sharing by default and enable it only when required. Ensure that this feature is disabled before you connect to a public Wi-Fi network. The file sharing setting is applicable to notebooks regardless of operating system.

8. Install Security Software

Install security softwares such as firewall and antivirus. Make sure it is activated and always turned on. Personal firewalls can detect abnormal activities like attempts to intrude, for instance. While, antivirus softwares can detect and remove viruses.

WHEN CONNECTED TO PUBLIC WI-FI

Once you are about to connect to the public Wi-Fi, the following tips are recommended:

1. Verify the Network Name

There may be two or more similar network names of one place. One of them could be a false network name set up by the perpetrator. Therefore, always verify the network name with perhaps an employee of the location or place, providing the said network.

2. Use HTTPS

Data transferred is usually in plain/clear text, which is easily legible by others. HTTPS wraps the data with an encapsulation technology to secure data from unauthenticated users. Download and enable HTTPS extensions on your browser.

3. Avoid Sensitive Transactions

Avoid performing any sensitive transactions when connected to public Wi-Fi, more so, financial or private transactions. It would be best to avoid performing financial transactions completely, over public Wi-Fi connections.

4. Avoid Leaving Device Unattended

Never leave your Internet-enabled device unattended in public places. A stolen device with confidential and valuable data would be a very high price to pay. The device can be replaced but the loss of confidential and valuable data are irreplaceable.

5. Get Paranoid

Practice healthy paranoia. Be alert of your surroundings in public areas as sensitive or private information on the screen of your device is exposed and vulnerable. You could also minimise the brightness of the screen or purchase a privacy filter or screen which limits and reduces the visibility of your screen to others around you. Someone might literally look over your shoulder with the hope of sighting your username, password or credit card number. This is known as shoulder surfing.

BEFORE DISCONNECTING FROM PUBLIC WI-FI

The following are steps to be taken when you decide to disconnect from a public Wi-Fi connection.

1. Clear Cache

Unscrupulous individuals may hack your device and capture your passwords or entries, as it is stored in the cache. Clearing your cache simply means clearing the history stored in the cache. How to clear your cache would depend largely upon the browser you are using, as the steps to do so, would differ from browser to browser. The clear cache option can be found under *Tools* → *Internet Options* or *History Tab* at the menu bar of your browser. Some browsers provide you with an option to select what it is that you would like to clear.

2. Disconnect from public Wi-Fi

Do not forget to disconnect the Wi-Fi connection by disabling Wi-Fi, when you are done. The longer you are connected to a network, the more exposed you are to an attack. It is a good practice to regularly check the connection status of the Internet-enabled device.

3. Manage Wireless Network

If you are a regular user of public Wi-Fi networks, always disable auto connect and delete ID's of previously connected public Wi-Fi networks stored on your device.

REFERENCES

1. Brian Burgess, “Wi-Fi”, 21 August 2013
   http://www.gizmag.com/how-to-stay-secure-on-public-wireless-hotspots/28694/

2. John Spaulding, Alyssa Krauss, and Avinash Srinivasan, “Exploring an Open Wi-Fi Detection Vulnerability as a Malware Attack Vector on iOS Devices”, 2012, IEEE

3. Matthias Korn, Clemens Nylandsted Klokmose, “Putting ‘Local’ Back into Public Wi-Fi Hotspots”, UbiComp 12, September 2012

4. Syahrul Fahmy, Akhyari Nasir and Nooraida Shamsuddin, “Wireless Network Attack : Raising Awareness of Kampung Wi-Fi Residents”, 2012

5. Samara Lynn, “Ten Tips for Public Wi-Fi Hotspot Security“, 7 September 2010
   http://www.pcmag.com/article2/0,2817,2368802,00.asp

6. Steven Andres, “How to Stay Safe on Public Wi-Fi”, PCWorld, 12 April 2010
   http://www.pcworld.com/article/194062/how_to_stay_safe_on_public_wifi.html

7. “Dependability in Wireless Networks – Can We Rely on Wi-Fi”, Jan/Feb 2007, IEEE Security & Privacy

8. Microsoft Safety and Security Centre, “Four Safety Tips for Using Wi-Fi”, http://www.microsoft.com/security/online-privacy/public-wireless.aspx

Corporate Office:
CyberSecurity Malaysia
Level 5, Sapura@Mines
No 7, Jalan Tasik, The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia

Tel : +603 8992 6888
Fax : +603 8992 6841
Email : info@cybersecurity.my
Customer Service Hotline : 1300-88-2999
www.cybersecurity.my

People First, Performance Now

Ministry of Science, Technology and Innovation

Best Brand Internet Security 2008 & 2009

CERTIFIED TO ISO/IEC 27001:2005 CERT NO. : AR4656

MS ISO/IEC 17025 TESTING SAMM NO. 456 (MyEF LABORATORY)

Status Company

Best Child Online Protection Website