CMSGu2013-04

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline On Securing Public and Private Wi-Fi Networks

CERT-MU

National Computer Board
Mauritius

Version 1.0

September 2013

Issue No. 4

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The main objective of this document is to provide users with instructions that they can follow to strengthen their Wi-Fi networks and make their internet experience more secure.

1.2 Audience

The target audience for this document includes everyone who makes use of Wi-Fi networks at home or within an enterprise, and focuses largely on securing their internet connection using secure wireless standards.

1.3 Document Structure

This document is organised into the following sections:

Section 1 gives an outline of the document's content, the targeted audience and the document's structure.

Section 2 gives a background on Wi-Fi Networks.

Section 3 explains how Wi-Fi Networks operate.

Section 4 presents the Wireless Security Standards in use today.

Section 5 depicts some of the major risks of Wi-Fi Networks and their countermeasures.

Section 6 provides some safety tips for Wi-Fi Networks

Section 7 concludes the document.

Section 8 consists of a list of references that have been used in this document.

Appendix A provides a list of acronyms that have been used in the document.

2.0 Background

Wi-Fi stands for Wireless Fidelity. Most modern computers are equipped with Wi-Fi adapters, available as internally-mounted cards, cards that fit in laptop PCMCIA slots or external devices connected through USB ports. These adapters look for signals broadcast by devices called Access Points (APs) that are normally connected to an existing wired network. This gives Wi-Fi devices access to the same resources that wired devices have. In some cases, Wi-Fi devices can also communicate directly with each other. Wi-Fi devices employ different technical standards grouped together, that enable communication with an AP. These standards are typically referred to as the IEEE 802.11 specification.

Wi-Fi networks have revolutionised the way we can use computers and mobile devices, at home, office or when we are out. Home and office Wi-Fi networks make it easier to use the internet both within and outside the building. Public Wi-Fi networks or hotspots allow us to benefit from the same facility at airports, hotels and restaurants. Plug-in mobile broadband devices, or 'dongles' provide even more flexibility, allowing us to work online where a cellular 3G or 4G coverage is available.

Wi-Fi networks indeed provide numerous benefits. However, an unprotected network can result in unauthorised use and potential harm, unless certain security measures are taken. In some cases, unauthorised users may be able to access your private information, view the content of transmissions, download unlawful content using your network or infect computers with viruses or spyware. Unauthorised users may also cause harm beyond your computer or network, such as sending spam, spyware or viruses to others, and the activity, most of the time, will be traced back to your legitimate network.

3.0 How do Wi-Fi Networks Operate?

As a client initiates its Wi-Fi connection, it must find an Access Point (AP) that is reachable and that will approve its membership. The client must settle its membership and security measures in the following sequence:

1. Use an SSID that matches the AP.
2. Authenticate with the AP.
3. Use a packet encryption method (data privacy) *(optional)*.
4. Use a packet authentication method (data integrity) *(optional)*.
5. Build an association with the AP.

3.1 Wireless Signals

There are three wireless technologies, which are not interoperable. The three technologies are Direct Sequence Spread Spectrum, Frequency Hopping Spread Spectrum and Infrared. Wireless technology standards are changing as constant testing involves the verification of the capabilities and features of each product. If two wireless signals are sent at the same time, on the same channel, they may collide and interfere with each other, requiring signals to be resent and eventually slowing down the associated wireless process. Signals are literally floating through the air. They have the ability to bounce and redirect themselves, as well as to absorb themselves into their physical surroundings such as walls, floors, trees or people.

3.2 SSIDs (Service Set Identifier)

In order to set up a wireless network for proper functionality, there are several required components. These will vary depending on the level of security required for the network. There are two types of networks and they are referred to as a Basic Service Set (BSS) or an Independent Basic Service Set (IBSS).

A BSS network consists of an Access Point or Wireless router and some client devices.

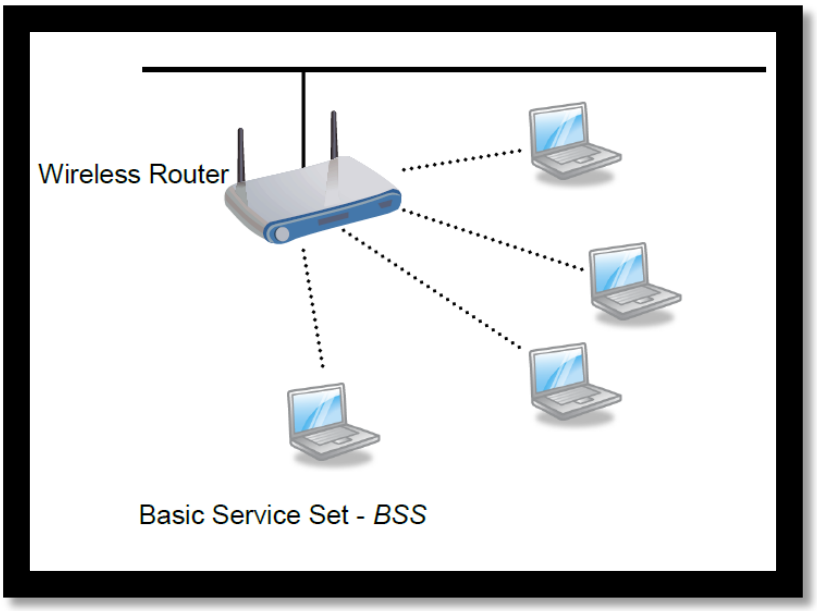

Figure 1 A Basic Service Set

An IBSS network consists of a group of clients connected to one another.

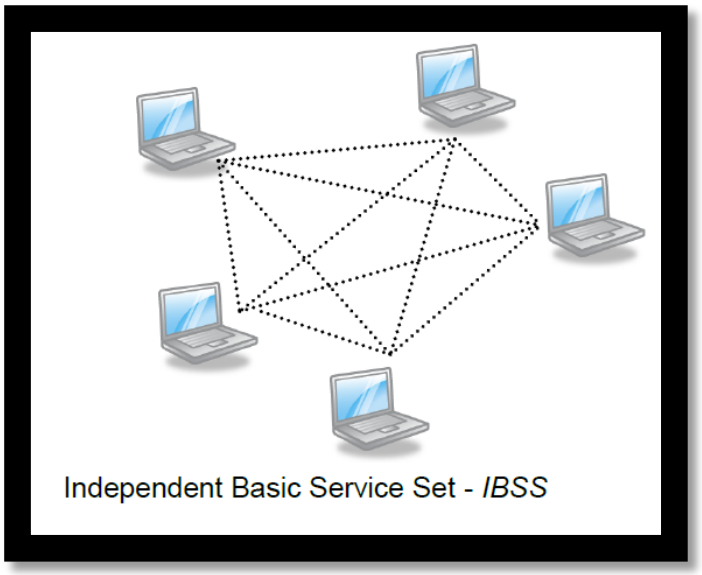

Figure 2 An Independent Basis Service Set

All networks will have an SSID. This ensures that traffic between radios, whether an AP or client device, can be directed to the right destination.

At startup, clients (such as a laptop) usually search for a network with a particular name. Some clients can be configured to look for a network with only one name; some clients such

as the Windows-XP client can be configured to connect to a variety of networks if the appropriate parameters have been configured in the utility.

By default, the SSID is broadcast by the AP in the beacon frame and is visible to almost any client utility or network monitoring tool. Some network administrators restrict the broadcast of the SSID or do not allow a client that does not know the name of the SSID to connect. When enabling this feature, care must be taken to ensure that the clients can tolerate this condition. Not all clients can connect to networks that do not broadcast their SSID, even if it is known and programmed into the client.

The AP will also need a channel on which to operate. This channel will be dependent on whether you are operating in the 2.4 or 5.8 GHz band. Some APs have an option to look for the least congested channel, but in most enterprise networks the administrator would plan out the channels for the network. The clients will scan all channels for the SSID and attempt to connect on the channel where the best signal is received.

This scanning can be done in two ways. One is a passive scan where the client simply looks at the Beacon Frames on the channels and the second is by sending Probe Request frames to APs that it sees in the Beacon Frames and analysing the information received in the Probe Response frame. The way in which a client accomplishes this depends on the vendor. Once the client has completed the scan, if it has not yet sent the Probe Request, it will send a Probe Request Frame. Upon receiving a Probe Response from the AP and processing what information it has obtained from the Beacon Frame and the Probe Response frame, it then determines that nothing in these frames would prevent it from joining the network, it will send an Authentication Frame.

4.0 Wireless Security Standards

Wireless network traffic flows in an open medium, the air interface, and therefore is considered insecure. A network administrator must be aware of the types of security risks there are, as well as some of the solutions available to mitigate those risks. Some of the attacks against a wireless network cannot be prevented and only effective monitoring of the network and proper responses will reduce the risk associated with the wireless segment of a network. In most cases, the role of wireless in the network is to create access to a network already in place or the Internet. So some form of authentication and segmentation is required to manage accesses to specific network resources. As wireless technology is introduced into enterprises where security is mandatory, wireless traffic needs to be secure.

First generation 802.11 wireless devices were expensive, limited and users were not particularly concerned with security. Wired Equivalent Privacy (WEP) was integrated into the original standard to provide security.

Security in all networks is included into the security policy of the enterprise.

- How sensitive is the data on the network?
- What are the risks if data is compromised?
- What defines acceptable use?

It is usually combined with an authentication scheme to provide not only authorised use but effective encryption. Most of the existing wired network user authentication methods can be leveraged over a wireless network.

4.1 Packet Encryption and Authentication

Two basic concerns that 802.11 clients and APs must work out are authentication and encryption. These are the basic two elements of wireless security. Authentication verifies the content of the packets of information travelling between two trusted wireless devices, such as a laptop and an AP. Next, encryption ensures that only the two trusted, wireless devices can read the information. Many different methods are available for authentication, encryption and a combination of the two.

4.2 Extensible Authentication Protocol (EAP) and 802.1X Authentication Protocols

Wireless security has advanced to use further, more robust methods. APs can use a variety of authentication methods that leverage external authentication and authorization servers and their user databases. EAP forms the basis for many wireless security methods, most of which have similar acronyms, such as EAP, PEAP, and LEAP. Because EAP is extensible, it is well suited for a variety of secure environments. EAP has its history in Point-to-Point-Protocol (PPP, also known as *dial up*) communication, not in wireless authentication.

Through 802.1X, users can authenticate even at Layer 2, before gaining further network connectivity. WLANs can leverage 802.1X as the means to implement EAP at Layer 2 for wireless clients. In a wireless LAN, you can find some of the following security method names: LEAP, PEAP, EAP-TLS, and EAP-FAST. Many different methods exist, but each one is based on EAP and uses a different type of credentials to authenticate wireless users. Some of the EAP-based methods go beyond authentication by adding extra security features.

4.2.1 Extensible Authentication Protocol – Transport Layer Security (EAP-TLS)

The EAP-TLS method uses the Transport Layer Security (TLS) protocol to secure client authentication. TLS is based on Secure Socket Layer (SSL), which is frequently used in secure web browser sessions. EAP-TLS uses digital certificates as authentication credentials, which means that every AP and wireless client must have a certificate generated and signed by a common Certificate Authority (CA). EAP-TLS also addresses wireless data privacy by generating WEP keys automatically, each time the authentication server forces the client to re-authenticate. The TLS session key, unique to each wireless client that is authenticating, is used to derive a unique WEP key. The WEP key is then used to encrypt the wireless data.

4.2.2 Protected Extensible Authentication Protocol (PEAP or EAP-PEAP)

PEAP or EAP-PEAP is similar to EAP-TLS in that a TLS session is used to secure the authentication. PEAP requires a digital certificate only on the authentication server so that the server itself can be authenticated to the client. The wireless clients are authenticated using Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2). As with EAP-TLS, the TLS session key is used to generate a WEP key for encrypting the wireless data stream. The keys change periodically as the authentication server forces the client to re-authenticate.

4.2.3 Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling (EAP-FAST)

EAP-FAST is a wireless security method developed by Cisco. EAP-FAST is not named for its speed; rather, it is named for its flexibility to lessen the administrative complexity. Clients are not required to use digital certificates, and they are not required to follow strict or strong password policies. EAP-FAST works by building a secure tunnel between the client and the authentication server. A Protected Access Credential (PAC) is used as the only client credential to build the tunnel. The PAC can be assigned from a PAC server or it can be created dynamically during an EAP-FAST negotiation process. Once the tunnel is built, the client is authenticated using familiar username and password credentials. EAP-FAST can generate a WEP key dynamically so that the wireless data stream can be encrypted.

Authentication Protocol -->	EAP-MD5	EAP - LEAP	EAP- TLS	TTLS (EAP-MSCHAPv 2)	PEAP (EAP-MSCHAPv 2)	PEAP (EAP-TLS)	PEAP (EAP-GTC)	EAP-FAST
802.1X Authentication Characteristics								
Client certificates	No	No	Yes	No	No	Yes	No	No
Server certificates	No	No	Yes	Yes	Yes	Yes	Yes	No
Client Password	No	Yes	N/A	Yes	Yes	No	Yes	Yes
Security Level	Weak	Weak (depends on password strength)	Strong	Strong	Strong	Strong	Strong	Strong (if Phase 0 is secure)
Mutual Authentication	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Compatible with WPA	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tunnelled Authentication	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Encryption key management	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 1 Comparison of EAP Methods

Upon detection of the new wireless client, the “requester”, the port on the switch, the “authenticator”, is enabled and set to the “unauthorised” state. In this state, only 802.1X authentication traffic will be allowed. Other traffic, such as DHCP and HTTP, will be blocked at the data link layer. The authenticator will send out the EAP-Request identity to the requester. The requestor will then send out the EAP-response packet that the authenticator will forward to the authenticating server, usually a RADIUS server (Remote Authentication Dial In User Service). The authenticating server can accept or reject the EAP-Request. If it accepts the request, the authenticator will set the port to the “authorised” mode and normal traffic such as HTTP will be allowed. When the requester logs off, an EAP-logoff message is

sent to the authenticator. The authenticator then sets the port to the "unauthorised" state, once again blocking all non-EAP traffic. In the WLAN world, 802.1X by itself is a Port-based Access Control, a flexible authorization scheme that can work with WPA, WPA2 or 802.11i technologies. It is typically combined with an authentication protocol, and as a pair they provide a secure authentication and encryption key rotation mechanism.

4.3 WLAN Authentication and Encryption

In 802.11 networks, clients can authenticate with an AP using many methods. The following are some of the most common means of connecting to a WLAN. It is worth noting that the level of security provided varies under the different methods. These methods are listed in order of the level of security which they provide, starting with the oldest and generally accepted as least secure.

4.3.1 Pre-shared key (PSK)

The same secret key is statically defined on the client and the AP. If the keys match, the client is permitted to have access. Notice that the authentication process in these two methods stops at the AP. In other words, the AP has enough information on its own to independently determine which clients can or cannot have access. Open authentication and PSK are considered to be legacy methods because they are not scalable and are not necessarily secure.

Open authentication is usually the default, and offers no client screening at all. Any client is allowed to join the network without providing any credentials. In fact, the SSID is the only credential that is required. Although this facilitates our task, it does not really control access to the WLAN. In addition, open authentication does not provide a means to encrypt data sent over the WLAN.

Pre-shared key authentication uses a long Wireless Equivalence Protocol (WEP) key that is stored on the client and the AP. When a client wants to join the WLAN, the AP presents it with a challenge phrase. The client must use the challenge phrase and the WEP key to compute a value that can be shared publicly. That value is sent back to the AP. The AP uses its own WEP key to compute a similar value. If the two values are identical, the client is authenticated. When pre-shared key authentication (commonly called *static WEP keys*) is used, the WEP key also serves as an encryption key. As each packet is sent over the WLAN, its contents and the WEP key are fed into a cryptographic process. When the packet is received at the far end, the contents are unencrypted using the same WEP key.

Pre-shared key authentication is more secure than open authentication, but it has two shortcomings:

- It does not scale well because a long key string must be configured into every device
- It is not very secure.

A static key persists for a very long time, until someone manually reconfigures a new key. The longer a particular key is in use, the more malicious users can gather data derived from it and eventually reverse-engineer the key. It is commonly known that static WEP keys can be broken.

4.3.2 Wired Equivalent Privacy (WEP)

WEP was introduced into the original standard as a means to encrypt the traffic on the network. From the wireless vendors' perspective, it was easy to implement, did not require much CPU power to encrypt and decrypt traffic, exportable, self-synchronising and used a relatively strong cipher. The weakness that has been exploited is related to the fact that a static key entered in both the AP and the client is required. This key is only changed manually, typically by an administrator of the devices, and must match on both devices. With these static keys being used to encrypt traffic on the network, an intruder can capture encrypted traffic and then run the traffic against an encryption cracking software or now even plan a live encryption key cracking event on a network that uses this security mechanism.

4.3.3 Wi-Fi Protected Access (WPA)

WPA was initially a temporary solution implemented by the Wi-Fi Alliance to provide an short-term security option during the time that 802.11i was under development. It actually repairs the primary weakness in WEP with a mechanism to rotate the encryption keys periodically and removes any requirements from the administrator or user to manually enter an encryption key. It also allows for each device to use a unique encryption key rather than sharing the same key with all the other users on the AP in use. The two methods of creating the key to be used for encryption are a passphrase method and a four-way handshake.

The passphrase method once again requires a manual entering of an 8 to 63 character passphrase in both the AP and the client. The passphrase must match in all devices using this AP. As a client connects to the AP, the client and AP go through a four-way handshake to derive the encryption key for that client. The passphrase then is the weak link in this method

and there is software that can be used to derive the passphrase from a captured four-way handshake. This can be mitigated to some degree by a strong passphrase. WPA offers the following wireless LAN security measures:

- Client authentication using 802.1X or a pre-shared key
- Mutual client-server authentication
- Data privacy using Temporal Key Integrity Protocol (TKIP)
- Data integrity using Message Integrity Check (MIC)

4.3.4 Temporal Key Integrity Protocol (TKIP)

TKIP leverages existing WEP encryption hardware that is embedded in wireless clients and APs. The WEP encryption process remains the same, but the WEP keys are generated much more frequently than the periodic re-authentications that occur with EAP based authentication methods. In fact, TKIP generates new WEP keys on a per-packet basis. An initial key is built as a client authenticates (or re-authenticates) with the EAP-based method. That key is formed by mixing the MAC address of the transmitter (the client or the AP) with a sequence number. Each time a packet is sent, the WEP key is incrementally updated. Once the client is forced to re-authenticate, an entirely new WEP key is built and the per-packet process repeats. WPA can use a pre-shared key for authentication if external authentication servers are not used or required. In that case, the pre-shared key is used only during the mutual authentication between the client and the AP.

Data privacy or encryption does not use that pre-shared key at all. Instead, TKIP takes care of the rapid encryption key rotation for WEP encryption. The MIC process is used to generate a fingerprint for each packet sent over the wireless network. If the fingerprint is made just before the packet is sent, the same fingerprint should match the packet contents once the packet is received. When packets are sent over the air, they can be intercepted, modified, and sent again.

Fingerprinting is a way to protect the integrity of the data as it travels across a network. For each packet, MIC generates a hash code (key), or a complex calculation that can only be generated in one direction. The MIC key uses the original unencrypted packet contents and the source and destination MAC addresses in its calculation, so that these values cannot be tampered with along the way.

4.3.5 Wi-Fi Protected Access Version 2 (WPA2)

WPA2 is based on the final 802.11i standard. WPA2 goes several steps beyond WPA with its security measures. For data encryption, the Advanced Encryption Standard (AES) is used.

AES is a robust and scalable method that has been adopted by the National Institute of Standards and Technology (NIST) for use in the U.S. government organizations. TKIP is still supported for data encryption, for backward compatibility with WPA. With WPA and other EAP-based authentication methods, a wireless client has to authenticate at each AP it visits. If a client is mobile, moving from AP to AP, such as a student with a tablet PC walking throughout the school requiring constant connectivity to the WLAN, the continuing authentication process can become burdensome. WPA2 solves this problem by using Proactive Key Caching (PKC). A client authenticates just once, at the first AP it encounters. As long as other APs visited support WPA2 and are configured as one logical group, the cached authentication and keys are passed automatically.

4.3.6 WPA/WPA2 Personal vs. Enterprise

Within the above described WPA and WPA2 authentication/encryption methods, there are two further types. The first type is known as personal and the other is referred to as enterprise. The primary difference between these two types is that Personal does not use EAP or a server such as RADIUS to authenticate users. Personal stores all security settings within the APs themselves. Enterprise uses EAP to facilitate authentication with an authentication server such as RADIUS.

WPA Personal mode and WPA2 Personal mode do not use an EAP type and a managed authentication server such as RADIUS. Instead, they work from a static list of keys stored in the access point. Their use on company networks should be avoided because vulnerabilities have been published about them and cracking tools are available.

If PSK has to be used, passwords must have a high degree of entropy. In an enterprise environment, some form of authentication is essential whereby users are required to authenticate to a Server, an Active directory, RADIUS, LDAP database or some other type of resource that maintains the users and their credentials. This eliminates the weakness of the passphrase in WPA-PSK. There are three elements of this process - Requester (Client), Authenticator (AP) and the Authentication Server (AS). In some enterprise APs, the Authentication Server may reside within the AP. Typically, once that process is complete the

server and the client determine the encryption key for that user and that specific session. The AS then sends the encryption key to the Authenticator for use in that specific session. WPA still uses a WEP key, but each client has their own encryption key. WPA2 assigns a unique key for each client. However, it uses the AES encryption mechanism. Both WPA/WPA2 Personal and Enterprise are among the strongest level of security available today.

4.3.6.1 WPA Enterprise Mode with EAP-TLS or PEAP for Authentication and TKIP for Encryption

If using WPA, this is amongst the strongest level of protection currently available. WPA with TKIP is a suitable alternative to WPA2 while waiting to migrate to new equipment. EAP-TLS is the most thoroughly tested authentication protocol for interoperable security. Some forms of PEAP may be easier to implement because client-side certificates are optional. However, variations exist between implementations by Cisco, Microsoft and other vendors. TKIP resolves the encryption vulnerability found in WEP.

4.3.6.2 WPA2 Enterprise Mode with EAP-TLS or PEAP for Authentication and TKIP for Encryption

This is amongst the strongest level of protection currently available. Alternative to WPA2, with TKIP for encryption to accommodate small devices, TKIP resolves the encryption vulnerability found in Wired Equivalent Privacy (WEP). This option must be considered for smaller devices that can support WPA2 authentication, but lack the processing power for AES.

4.3.6.3 WPA2 Enterprise Mode with EAP-TLS or PEAP for Authentication and AES for Encryption

This is actually the strongest level of protection currently available. WPA Enterprise mode uses an EAP type in conjunction with an authentication server. EAP-TLS, one of several EAP types, is the most thoroughly tested authentication protocol for interoperable security. Some forms of PEAP, a newer EAP type, may be easier to implement because client-side certificates are optional. However, variations exist between implementations by Cisco, Microsoft and other vendors.

4.4 Virtual Private Network (VPN)

In addition to the previously described authentication and encryption methods, it is now very common to add VPN technology as an additional layer of security for mobile devices.

VPN technology has existed since the days of Remote Access for dial-in modem connections to the corporate network. This technology can be implemented in Wireless Networks as well. It can provide encryption, tunneling and security when a wireless client gains access to an unsecured network such as a local hotspot. Prior to the client gaining access back to his corporate network, he is required to authenticate against a VPN endpoint at the head office. A tunnel and encryption can then be setup between the endpoint and the client to secure the transport of packets between them over an un-secure network such as a wireless connection. Some wireless routers are also capable of acting as the VPN endpoint. This allows clients to establish a secure tunnel between itself and the wireless router.

5.0 The Risks of Wi-Fi Networks And The Countermeasures

Home, office, mobile and public Wi-Fi, all use the same technology (802.11). There are some common potential issues, whilst each has its own particular risks. You can protect yourself easily with a few simple precautions.

5.1 Home/Office Wireless Networks

5.1.1 The Risks

If your wireless hub/router/dongle is not secured other people can easily access it if they are within range. This can result in unauthorised people doing the following malicious activities:

- Taking up your bandwidth, thus affecting the online speed of your own computers and other devices.
- Using your download allowance, for which you have paid your Internet Service Provider (ISP).
- Downloading inappropriate material which would be traced back to your address and not to their computer.
- Accessing sensitive information that you may be sending or receiving online.

5.1.2 Safe Wireless Networking

All of the above risks can be avoided simply by ensuring that the wireless hub/router/dongle that you wish to connect to is secured. To check that this is the case, simply search for available wireless networks, and those that are secured will be indicated with a padlock symbol.

When you first connect a computer, smartphone, tablet, printer or any other wireless-enabled device to any wireless hub/router/dongle, you will be prompted to enter a password/key, provided the network is in secure mode. This will enable the device to connect on this occasion and normally, for future use. The password/key will be supplied with the hub/router/dongle, but you may be given the opportunity to change it to one of your own choice.

If you are setting up a new hub/router/dongle, it will probably have been supplied with security turned on as the default. There are three main encryption levels available (WEP, WPA and WPA2), WPA2 being the highest. Most hubs/routers give you the option of

selecting a higher level, but remember that some older devices may not be compatible with higher levels.

If for any reason a home/office/mobile wireless hub/router/dongle you wish to connect to is not secured, consult the user manual. You should also ensure that you have effective and updated antivirus/antispyware software and firewall running, before you connect to a wireless network. Wi-Fi codes should be kept safe at all times so that others cannot access or use them.

5.2 Public Wi-Fi

5.2.1 The Risks

The security risk associated with using public Wi-Fi is that unauthorised people can intercept anything you are doing online. This could include capturing your passwords and reading private emails. This can happen if the connection between your device and the Wi-Fi is not encrypted, or if someone creates a spoof hotspot which makes you believe that it is the legitimate one.

With an encrypted connection, you will be required to enter a 'key' or a network code. Alternatively, you may only be prompted to log in to have internet access. This will tell the operator that you are online in their hotel, restaurant or airport. There is almost certainly no security through encryption.

5.2.2 Safe Public Wi-Fi

Unless you are using a secure web page, do not send or receive private information when using public Wi-Fi. Business people wishing to access their corporate network should use a secure, encrypted Virtual Private Network (VPN).

You should ensure you have effective and updated antivirus/antispyware software and firewall running before you use public Wi-Fi.

5.2.3 Other Advice

- Never leave your computer, smartphone or tablet unattended.
- Always be aware of who is around you and may be watching what you are doing online.

6.0 Safety Tips For Your Wi-Fi Network

The following tips will help you to use your Wi-Fi more securely and protect your personal information against unauthorised access. Consult the owner's manual that came with your wireless router for specific instructions on performing the following steps. Manuals are often available on the manufacturer's website.

1. Turn Encryption On

Turning on your wireless router's encryption setting can help secure your network. Wireless routers often come out of the box with the encryption feature disabled, so be sure to check that encryption is turned on shortly after you or your broadband provider installs the router. Note that there are different types of encryption. "WPA2" currently is the most effective standard. Another common standard, "WEP", is less secure, and therefore is not recommended. To turn on encryption, you will need to choose a wireless network password. Longer passwords that are made up of a combination of letters, numbers and symbols are more secure.

2. Turn the Firewall On

A "firewall" is configured to protect computers from harmful intrusions and can be hardware-based or software-based. Wireless routers generally contain built-in firewalls, but are sometimes shipped with the firewall turned off. Be sure to check that the wireless router's firewall is turned on.

3. Change Default Passwords

Most wireless routers come with default passwords for administering the devices settings (this is different from the password used to access the wireless network itself). Unauthorised users may be familiar with the default passwords, so it is important to change the router device's password as soon as it is installed. Make sure you use a password which is easy for you to remember but would be difficult for a stranger to guess, and preferably something with a combination of letters, numbers and special characters. Avoid using obvious words such as the name of your street.

4. Change the Default Name of the Network

When a computer with a wireless connection searches for and displays the wireless networks nearby, it lists each network that publicly broadcasts its SSID. Manufacturers usually give all

of their wireless routers a default SSID, which is often the company's name. It is a good practice to change your network's SSID. However, to protect your privacy do not use personal information such as the names of family members.

5. Turn Network Name Broadcasting Off

Wireless routers may broadcast the name of the network (the "SSID") to the general public. This feature is often useful for businesses, libraries, hotels and restaurants that want to offer wireless Internet access to customers, but it is usually unnecessary for a private wireless network. It is recommended that owners of home Wi-Fi networks turn this feature off.

6. Check that your device does not auto-connect to Wi-Fi signals

If your device is set to automatically connect to available Wi-Fi networks, then you run the risk of automatically connecting to unknown and potentially dangerous networks. You should switch off auto-connect on your device settings page. You can refer to the manufacturer's instructions if you do not know how to do this.

7. Use the MAC Address Filter

Every device that can connect to a Wi-Fi network has a unique ID called the "physical address" or "MAC" (Media Access Control) address. Wireless routers can screen the MAC addresses of all devices that connect to them, and users can set their wireless network to accept connections only from devices with MAC addresses that the router is set to recognise. In order to prevent unauthorised access, change your router's settings to activate its MAC address filter to include only your devices.

7. Additional Wi-Fi Safety Tips

- Turn off your Wi-Fi network when not be in use for extended periods of time
- Use anti-virus and anti-spyware software on the computers that access your wireless network
- Do not assume that public Wi-Fi networks are secure and free from threats

7.0 Conclusion

Computers and many other devices, including smart phones and tablets, can connect to the internet wirelessly using Wi-Fi. An unsecured Wi-Fi connection makes it easier for hackers to access your private files and information, and it allows strangers to use your internet connection fraudulently. Therefore, wireless security standards should be used for authenticity and privacy. Additional measures such as turning the firewall and the MAC address filter on should be used for enhanced security.

8.0 References

- Protecting your wireless network, http://www.fcc.gov/
- Wireless networks and hotspots, http://www.getsafeonline.org/
- Wireless Local Area Network Best Practices Guide, http://education.alberta.ca
- Wi-Fi Security, http://www.ico.org.uk