



Safety Wireless

www.aoema.org



Not feeling safe
in the online world?

Use this guide
to secure your
wireless network.



Safety Wireless

Introduction

Work on your laptop or check e-mail from anywhere in your home. Connect to your office network from an airport, restaurant or hotel. Retrieve files, view websites or send instant messages to co-workers from a conference room or the company cafeteria. This is all possible in today's world of wireless communications.

However, convenience and flexibility comes at a price – the security threat level increases with the use of wireless networks and devices. Users must become aware of the issues and learn how to prevent problems before they occur. This booklet is intended to assist you when setting up a wireless network and provides recommendations for how to safely access the Internet from a public wireless hotspot.

Consider this booklet not as a replacement for the manual that comes with your wireless device, but as a complementary resource to help you configure your hardware to achieve the highest level of security possible.

For the most part, this booklet is aimed at all users, regardless of skill level. However, the information on pages 12 and 13 is provided more for the advanced user than the beginner.

Contents

What you need to know to read this book

Page 3

Find the answers to your questions

Page 6

Configuring your Access Point

Page 10

Using Public Hot Spots

Page 14

Using Mobile Phones and PDAs

Page 16

Wireless Security Checklist

Page 26



A glossary of terms is usually found at the back of a book and referred to only as required. However, you will find it much easier to understand this booklet if you take a few minutes now to familiarize yourself with the vocabulary of wireless technologies.

The first nine terms are important for all users to understand and the last four are for more advanced users.

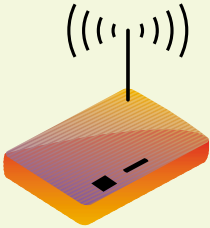


What you need to know to read this book

3

<p>Bluetooth</p>	<p>Bluetooth is the name given to the wireless technology that is used primarily to allow individual devices to communicate with each other over short distances. While Bluetooth is not generally used to network computers, it is very useful for communications between computers, PDAs and mobile phones. It is also possible for your computer to communicate with peripheral devices like printers and scanners via Bluetooth.</p>
<p>MAC Address (Media Access Control)</p>	<p>Every device attached to a network (such as a network card, a wireless card or a wireless access point) needs to have a unique identifier so that information can be addressed to get to that specific adaptor. A MAC address is a series of numbers delimited by colons. For instance, a typical MAC address could be 00:07:40:A2:1A:BB. Often you will see this address printed on a sticker on the network device. In addition, it is possible to send an enquiry to the device to discover its MAC address.</p>
<p>Network Encryption</p>	<ul style="list-style-type: none"> • WEP: Wired Equivalent Privacy Protocol is a basic security feature included in Wi-Fi networks that encrypts information sent over wireless networks. It is available in 40-bit and 128-bit encryption modes. WEP is considered to be fully broken, as fully automated tools that can crack you WEP key from 10 minutes of encrypted messages are freely available for download by anyone. WEP should not be used unless there is no other choice. WEP is much better than nothing at all. • WPA: Wi-Fi Protected Access was developed by the Wi-Fi Alliance and provides improved data encryption and user authentication. Only computers with a matching keys can access your wireless network. The latest versions of computer operating systems (Windows XP, Apple OSX, Linux) offer WPA security.
<p>Rogue Access Point</p>	<p>An unauthorized access point on the network.</p>

<p>SSID</p>	<p>SSID stands for the Service Set Identifier. An SSID is a network name or ID and can be any alphanumeric string, including upper- and lowercase letters, up to 32 characters in length. Wireless Access Point manufacturers set a default SSID at the factory, but you should change this setting to keep intruders out and to make it difficult for a nearby neighbor with the same type of Wireless Access Point to accidentally access your network. The SSID may be referred to by different terms, including Network Name, Preferred Network, ESSID (Extended Service Set Identifier) or Wireless LAN Service Area. Any device that connects to your wireless network must know the SSID.</p>
<p>TCP/IP and IP Addresses</p>	<p>Transmission Control Protocol/Internet Protocol – the language used by computers to talk to each other. The Internet uses this language to allow you to view web pages from next door or the other side of world.</p> <p>TCP/IP networking requires that every machine or device connecting to the network has a unique IP address, and for information to get to its proper destination, data has to contain the IP address of its origin and the IP address of its destination.</p> <p>Similar to a phone number, the format of an IP address is 123.213.154.178, and identifies a given device to the network. Some IP address series have been designated as private, and as such cannot be directly accessed from the public Internet.</p>
<p>Wireless Access Point</p>	<p>At the heart of a wireless home or small office network is the access point (sometimes referred to as a base station), a unit that provides a gateway for your wireless devices. Think of it as a “traffic cop” directing data around your wireless network and if required, managing data traffic between wireless and wired networks. There are many manufacturers of wireless access points, including Netgear, Buffalo, Linksys, D-Link and Cisco, with a price range starting from around \$US75. Your decision will be based on which “802.11” standard best meets your requirements, the features and functionality of different units (including security features) and the price you are prepared to pay.</p>
<p>Wireless Network Modes</p>	<p>The “802.11” standard defines two modes:</p> <ul style="list-style-type: none"> • Infrastructure Mode – wireless devices communicate with each other by first going through an access point, which acts as a conduit to a wired network or operates independently. • Ad-Hoc Mode (also known as Peer-to-Peer or Computer-to-Computer) – wireless devices communicate directly with each other, without the need for an access point. <p>While ad-hoc mode doesn’t require the purchase of additional hardware and provides a wireless network quickly and easily, there are additional security issues that must be addressed before making a final decision about which mode to select.</p>
<p>Wireless Networks</p>	<ul style="list-style-type: none"> • Wi-Fi or Wireless Fidelity: A wireless network enables multiple computers and devices to communicate without being physically connected, thus eliminating the need for unsightly cables. The most common wireless networks in use today are called Wi-Fi, or Wireless Fidelity, networks.



- Standards: The Institute of Electrical and Electronic Engineers (IEEE) developed a family of standards to define how devices can communicate using radio waves and gave it the reference “802.11”. There are several variations of the “802.11” standard, and listed below are some of your options when buying a wireless device. Price, performance and compatibility will dictate which one is right for you.
 - o 802.11g – fast data rate, relatively inexpensive, high risk of interference.
 - o 802.11b – compatible with and very similar to 802.11g devices, but transmits data at a slower rate.
 - o 802.11a – lower risk of interference because it doesn’t share the frequency used by cordless phones and microwave ovens (2.4 GHz) as does 802.11b/g. There are also more channels available to 802.11a devices further reducing interference issues.
 - o 802.11n – builds upon previous 802.11 standards by adding multiple-input multiple-output. The additional transmitter and receiver antennas allow for increased data throughput.
 - o 802.11i – A new security standard. The WPA logo certifies that devices are compliant with a subset of the 802.11i protocol. The WPA2 logo certifies full support for 802.11i. You should expect new APs whether 802.11a, b, g, or n to include WPA capability or preferably WPA2.

For a complete list of all “802.11” variations, refer to the website of the Wi-Fi Alliance, a nonprofit industry association responsible for testing and approving all devices using the “802.11” family of standards. www.wi-fi.org

DHCP

Dynamic Host Configuration Protocol assigns IP addresses for a defined period of time to any device that asks for it. DHCP comes pre-installed in some wireless access points and automatically allocates IP addresses for all devices connected to the network. While this can be a time-saving convenience, particularly for laptop users accessing different networks, this service can also be a security risk. If someone gains access, the DHCP server function automatically provides a valid IP address. Therefore, if you can’t limit the addresses allocated by the DHCP, it is best to disable this function.

RADIUS

The Remote Authentication Dial-in User Service Protocol (RADIUS) is a method of authenticating users who want to dial in to their office computers from a remote location. This protocol is useful in authenticating wireless network users in the same way.

SSH

SSH stands for Secure SHell (or Secure Socket sHell) and is a secure replacement to remote terminal access applications such as Telnet.
It is used to get secure command-line access to a remote computer. It can also be used to send other types of data (FTP etc) through a secure “tunnel”.

VPN

Virtual Private Network, a method for having an end to end secure link between two computers over the internet. It can also be used to secure communications over a wireless network.

WHEN SETTING UP A WIRELESS NETWORK, QUESTIONS YOU MIGHT ASK:

Page Reference:

DO I SELECT "COMPUTER-TO-COMPUTER" OR "INFRASTRUCTURE" MODE?

"Computer-to-computer" can be the simplest and least expensive mode, but "Infrastructure" mode is more secure. Make the right decision by learning what the differences are between the two modes.

[Page 8](#)

WHERE SHOULD I PHYSICALLY LOCATE THE ACCESS POINT (AP)?

The physical location of your access point (AP) can affect both performance and security. Follow the ten simple recommendations to achieve both. [Page 9](#)

6

Find Answers to Your Questions

DO I ACCEPT THE DEFAULT SETTINGS ON THE AP OR MAKE CHANGES?

When you take the AP out of the box, it will have default factory settings for a number of features. You will need to decide whether to accept these settings or make changes. Refer to the chart of recommended configuration settings to learn how to securely set up your AP and protect your wireless network. [Page 10](#)

WHAT CAN I DO TO PROTECT MY WIRELESS NETWORK?

Configuring the AP is the first step in setting up a wireless network. There are ten additional recommendations you may need to consider. Learn what they are and if they apply to you. [Page 12](#)

HOW DO I SECURELY INCORPORATE A WIRELESS NETWORK INTO AN EXISTING WIRED NETWORK?

When combining a wireless network with an existing wired network, you will need to address the specific security concerns of wireless technology to protect the entire network. [Page 12](#)



Page Reference:

WHEN USING WIRELESS TECHNOLOGIES, QUESTIONS YOU MIGHT ASK:

Yes, provided you follow six simple recommendations for securing your laptop and the personal data stored on it. While these are simple steps, they must be followed each and every time. Learn what they are so you can take full advantage of public wireless hotspots. [Page 14](#)

Some of the six recommendations require changes to your laptop settings. They are easy to do and take almost no time. However, it is critical that you check these settings each and every time you intend to use a public wireless hotspot. [Page 14](#)

IS IT SAFE TO ACCESS MY E-MAIL AND VIEW WEBSITES FROM A PUBLIC WIRELESS HOTSPOT USING MY LAPTOP?

WILL I NEED TO CHANGE THE SETTINGS ON MY LAPTOP?



Many mobile phones and PDAs today have Internet capabilities, making them vulnerable to the same security risks as laptop computers.

For example, did you know that anti-virus software and a firewall should be installed on all mobile devices? [Page 16](#)

There are potential risks with Bluetooth devices since they communicate over open radio waves. Learn what the risks are and how to take preventive measures. [Page 18](#)

There are intentional acts that can be illegal and subject to the laws of individual jurisdictions. What is worrying are the unintentional acts that innocent, law-abiding, individuals are committing by not being aware of how the use of wireless technologies is governed by law. [Page 20](#)

Wired or wireless, network or standalone, there are some standard practices that should be followed when connected to the Internet. [Page 22](#)

WHAT ABOUT USING MY MOBILE PHONE OR PDA TO ACCESS THE INTERNET FROM A PUBLIC LOCATION?

IS BLUETOOTH TECHNOLOGY SAFE?

ARE THERE LEGAL CONSIDERATIONS ASSOCIATED WITH USING WIRELESS CONNECTIONS?

IN GENERAL, HOW DO I SECURE MY COMPUTER AND PROTECT MY DATA?



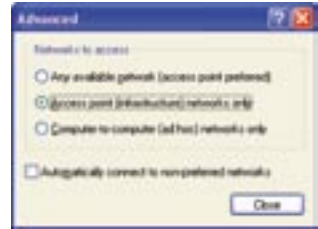
WiFi devices have two modes in which they can be used:

- Infrastructure mode - using wireless access points (APs) as base stations that wireless devices connect to.
- Ad-hoc or Computer-to-Computer mode - in which each wireless device connects to other wireless devices directly, not requiring the use of an AP.

Ad-hoc mode is often used to exchange data between two or more computers in an “ad-hoc” (or one time only) situation. Some users select ad-

pass-phrase that is at least 15 to 20 characters. This way, anyone seeking to connect to your computer must know the precise pass-phrase you have assigned.

The best advice is to not use ad-hoc networking mode at any time or if you must use it, turn it off whenever possible. This can be done in the “Advanced” screen of your “Wireless Networks” setup screen in Windows XP. Always de-select “Automatically connect to non-preferred networks”.



8

Selecting your Wireless Mode



hoc mode as an inexpensive and simple way to set up a wireless network, saving the cost of an AP. However, when using ad-hoc mode, some of the protections afforded through APs are not available. Most large corporations prohibit the use of ad-hoc mode for all network devices as they consider it a security risk to their network and stored data.

Since ad-hoc networks don't employ measures to authenticate users, “outside” devices within range can connect to any “inside” device configured to allow ad-hoc networking. Admittedly, each device must be on the same channel, using the same SSID and IP subnet, but these are relatively trivial issues for the experienced “cracker” to resolve.

If you still have reasons to allow ad-hoc networking, ensure that you use WPA encryption with a

RECOMMENDATIONS

- Always disable ad-hoc networking when not in use
- Always use WPA encryption when using ad-hoc networks
- If WPA encryption is not available, use WEP encryption
- Use strong passwords (a pass-phrase of 15 to 20 characters is recommended)
- Use properly configured wireless access points in preference to ad-hoc networks



One of the first things to consider is the physical location of your AP. While there are performance issues involved in the location of your access point, there are

RECOMMENDATIONS

- Place the AP near the center of your wireless network.
- As far as possible ensure line-of-sight access to all computers.
- Minimize the number of walls or ceilings between the access point and computers.
- Set the AP in an elevated location such as a high shelf to enhance receiving sensitivity.
- Keep the AP away from large metal surfaces, including solid metal doors, metal desks and filing cabinets. Water can also degrade performance, such as aquariums and large potted plants.



Locating your Access Point

9

also security issues. APs are radio transmitters and receivers. In order to protect the data flowing around your network, you should strive to minimize the leakage of radio waves outside the area that you want to service.

In addition to the leakage consideration, you will also want to protect your access point from tampering by unauthorized people. They could hit the reset button and cause all settings to revert to factory defaults undoing all your hard work to secure the device. This can also prevent access to the AP from computers configured with the "old" settings.

- To prevent interference, keep away from microwaves and 2.4 GHz cordless phones.
- To minimize leakage outside the area it is meant to service, turn down the power of the broadcast as required, if possible.
- Avoid outside walls/windows and common walls with adjacent homes/offices to ensure that the signal doesn't extend beyond the required area.
- To ensure that unauthorized people don't tamper with your AP try to have it in a secure location
- Some AP's allow you to reduce the output power of the device. This is one way to prevent too strong a signal from extending beyond the desired wireless broadcast area(through doorways and windows), and being accessible to the "outside" world.

Feature	Factory default settings	Setting for improved security
User name and Password	Vary according to manufacturer, but two common examples of user name are "admin" and "root" Common examples of default passwords include "admin" "password" and blank fields without any words	Change User Name and Password All APs allow you to change the default password and encourage you to do so. There are, however, some APs that do not allow changes to the user name.
Broadcast Network Name (SSID)	Enabled	Disabled Do not allow the name or SSID of the AP to be broadcast If SSID broadcasting cannot be turned off, the "Beacon Interval" should be increased to its maximum.
Wireless Network Name or SSID	Some examples of defaults include: NETGEAR DWL-2100AP AP+(MAC address)	Change name or SSID Many APs come pre-configured with a standard name or SSID. These names are readily identifiable from the manufacturers web site.


10

Configuring your Wireless Access Point

Encryption (WEP/WPA)	Disabled	Enabled There are two methods of encryption: WEP (Wired Equivalent Privacy Protocol) and WPA (Wireless Protected Access). WEP is the older method and considered to be inadequate by today's standards. Nearly all APs sold today provide WPA with 128-bit encryption and is the recommended setting.
Authentication Type	Auto	Open Authentication
MAC Address Filtering	Disabled	Enabled The MAC address is the unique identifier assigned to the network card in each computer. Many APs have the ability to automatically establish a list of MAC addresses that will be allowed to access the wireless network.
DHCP	Enabled For networked computers to be able to communicate with one another, each one must have IP addresses on the same "subnet" - this is the equivalent of having house addresses in the same Zip code or phone numbers in the same area code.	Disabled Some APs provide a DHCP facility but others do not. If it is there, you should disable it.

Why this is important	Be Aware !
<p>Most APs come pre-set with the same user name and password (factory default settings) and that means anyone could access your network to change the settings on your AP.</p>	<p>If you forget the password you will have to reset the AP to gain access to it. This means that you will need to configure the AP again.</p>
<p>The name or SSID of the APs wireless network. By broadcasting your SSID you are telling everyone that your wireless network exists and anyone with compatible equipment could possibly tune into your wireless network.</p>	<p>Anyone wishing to connect to your wireless network will need to manually enter the SSID to gain access. Software on your computer will not be able to automatically discover the access point.</p>
<p>Even if you disable the broadcast of the SSID, someone could guess it if left as the factory default. You must change the SSID to avoid this.</p>	<p>The new name should not identify anything about you, your company or home environment, or your geographic location.</p>

There are two ways to change the settings on your AP: from the wireless network or only when the AP is physically connected to a computer via a USB or network cable. A physical connection provides additional security and is therefore the best way to make changes. In the AP, you should definitely disable the ability to make changes from the wireless network.



<p>You can protect your AP and wireless network, but it is still possible for dishonest people to actually read the data transmitted across a wireless network since it is over radio waves. This is why it is critical that you enable encryption and use the stronger WPA format.</p>	<p>All devices on the wireless network must be able to use WPA encryption. It is not possible to mix WEP and WPA through the same AP When using WPA a pass-phrase of 20 characters or more is recommended. This can be hard to remember but there are software packages available that can securely store your passwords</p>
<p>The shared key mechanism should never be used. It could allow the key to be compromised in a matter of seconds. Open authentication (null/no authentication) is always better than shared key.</p>	<p>Remember, WEP encryption is no longer recommended, but you may have to use it if your device is not configured with WPA or WPA2 encryption.</p>
<p>The result of manually specifying a list of MAC addresses will be to restrict access to your network by only known devices. By using MAC address filtering you can greatly minimize the chance of this being possible.</p>	<p>Include your own computer's MAC address or you won't have access. MAC addresses are not encrypted, making it possible for dishonest individuals to discover the MAC addresses on your network and then change their own MAC address to match one of yours and gain access. You can, however, greatly minimize the chance of this happening by following the recommendations in this booklet.</p>
<p>DHCP automatically assigns each network computer a unique network address, thus making it easier to add computers and other devices to the wireless network. However, this automated feature can also make it easier for unauthorized parties to access your network and therefore it is best to disable it.</p>	<p>By disabling this feature, you will need to manually enter IP addresses for all computers and PDAs on the network. While this is somewhat inconvenient, it adds to the overall security of a wireless network.</p>



In addition to the things that need to be set up within your wireless access point, there are many other things that can be done to protect your overall network environment. Listed below are some of the key recommendations that you can use that will help to further enhance your security.

Protecting your Network



RECOMMENDATIONS	WHY THIS IS IMPORTANT
<p>Use software to detect snoopers on the network</p>	<p>There is software available today that will allow you to see all of the devices connected to your network. Some popular anti-virus programs have this facility. Using this software will allow you to notice when an unknown computer is connected to your network. "Rogue Access points" or APs that have been unofficially installed on your network can also be detected in this way They can also be detected by walking around your premises with AP detection software and identifying all of the APs discovered. These "Rogue APs" may be innocently installed by someone in your home or office who does not understand the security risks involved in doing this. This is why education is always an important tool in protecting your network</p> <p>.....</p>
<p>Turn off all APs when they are not in use (e.g., after hours and weekends in an office)</p>	<p>Just as you should turn off your broadband connection when not in use you should also turn off wireless access point when not in use such as at night or during weekends.</p> <p>.....</p>
<p>Develop and manage a security policy for the use of a wireless network in your enterprise</p>	<p>In an office environment ensure your staff understands that there is a security issue with using wireless devices and networks, otherwise they will not appreciate the threat. Writing a comprehensive policy document for wireless security will enhance your internal security. This policy should be integrated into your overall communications and network policy. Unless people read and understand the policy it is not worth the paper it is written on. Be sure to educate your staff on the policy issues.</p> <p>.....</p>
<p>If possible, change the default "subnet" range of addresses</p>	<p>The trick to securing a wireless network is to put as many obstacles in the way of the potential of unauthorized access. By selecting a different range of network addresses than the standard, it makes it more difficult for an unauthorized person to guess a correct network address to use.</p> <p>WARNING: If you are using Microsoft's "Internet Connection Sharing" facility, you cannot change the address range that is used.</p>

RECOMMENDATIONS

WHY THIS IS IMPORTANT

Enable logging and check log files regularly

Most Wireless Access Points have the facility to log activity on the wireless network. It is good practice to keep these logs and analyze them frequently to uncover any unauthorized activity.

WARNING: You may need to obtain extra software to collect, maintain and analyze the data.

.....

Test your wireless security with the many tools available today

Unless you test your set up, you can never be sure if it is working correctly. Testing it on a regular basis can set your mind at rest. In a small home or office network, this need only take a few minutes on a regular basis.

WARNING: Sometimes testing can actually create vulnerabilities in your own network so test with care and forethought.

.....

Authenticate the incoming wireless users with an external server

Even if you secure all of the data on your network using the various encryption protocols, it is good practice to actively identify all users on the network. This can be done using a RADIUS server. However, unless you or your technology person has adequate experience in setting up such a protocol, you can actually degrade your security. Be aware that setting up an effective RADIUS server environment is not a trivial exercise.

WARNING: You will need to ensure that the hardware you have purchased supports the use of a RADIUS server.

.....

When adding a wireless network to a wired network, ensure there is a firewall between the two

Most wired networks have a secure firewall interface to the internet. This is to ensure that your network cannot be accessed from the internet. If employees dial in to your network from home, they expect that they will have to go through the firewall. Treat employees using wireless networks in the same way that you would treat employees dialing in from home. Due to the insecure nature of wireless networks the safest method is to separate the two networks with a firewall.

WARNING: In a small office or home office environment this will add cost. It may not be required if you are using WPA/WPA2

.....

Encrypt your wireless traffic using a VPN

While using WEP/WPA to secure your wireless communications, is good practice, you can make it even more difficult for anyone to eavesdrop on your network communications by using a Virtual Private Network(VPN) on devices attached to the wireless network.

WARNING: Using VPN on top of WEP/WPA can dramatically reduce network performance due to increased overhead. Using a VPN can also make it difficult to roam between access points and maintain data sessions. You may not need VPN if you are using WPA/WPA2.

.....

Use encryption protocols for applications where possible

Applications run over a network can also be made secure using encryption protocols. Doing this should be standard practice on both wired and wireless networks. Encrypting application data that is being run over a wireless network will help to keep the information secure.





Today, there are a growing number of public wireless hotspots available for use. Some are free while others are commercially operated. The commercial operations are recognising the need to provide secure access and offer software on their site to enhance security while access their hotspots. The free and private hotspots usually do not provide any security at all.

Under either circumstance, you need to ensure that your computer is not vulnerable to attack and that your data is not exposed. Following the recommendations shown here will help to ensure that you are protected when using public wireless hotspots.

Using public hotspots



RECOMMENDATIONS	WHY THIS IS IMPORTANT
<p>Before going to a public hotspot, turn off “file and printer sharing” protocols for your wireless network card</p> <p>(Windows XP users): Prior to using a public hotspot, you should clear your list of “preferred networks.”</p> <p>(Windows XP users): Select “Access point (infrastructure) networks only” in the “Wireless Network Configuration” screen</p>	<p>While working in your office or at home and accessing your own network, the “file and printer sharing” protocol can improve productivity. It allows you to seamlessly share files or access printers associated with other computers in your network. However, in a public hotspot, this protocol becomes a major security risk. You obviously do not want the general public to have access to the files on your computer, so it is critically important that you turn this feature off when working in all public locations, including restaurants, hotels, airports and open wireless zones.</p> <p>WARNING: You will need to remember to turn this facility back on when you want to access your own network. Otherwise, you will not be able to print on local printers or share files.</p> <p>.....</p> <p>Windows XP actively probes and broadcasts all SSIDs you access. If someone can identify your preferred networks, a rogue access point can be made to look like one of your own access points.</p> <p>WARNING: Upon returning to your home or office environment, you will need to re-associate your laptop with the network, however, this is a trivial exercise as long as you remember all the encryption keys, SSIDs, and authentication settings for the deleted networks.</p> <p>.....</p> <p>If you switch between “ad-hoc” and “infrastructure” network modes, you will need to check your “Wireless Network Configuration” screen prior to any session from a public hotspot. This is extremely important because if you don’t disable the “ad-hoc networking” option, other users within close proximity could access your computer without your knowledge. Most users connect to a network through a wireless access point, making it</p>

RECOMMENDATIONS

When accessing a public wireless network, (1) use the software provided by the hotspot provider (downloadable from their website) and (2) check website certificates for their authenticity.

Make sure all data to be transmitted over a public hotspot is encrypted.

Avoid transmitting personal information when using a wireless network hotspot.

WHY THIS IS IMPORTANT

highly unlikely that “ad-hoc” networking mode would ever have to be enabled in the first place. This important setting is easily missed, potentially causing a huge security breach that would likely go undetected.

(1) While most public hotspots are legitimate, it is possible for a dishonest person to create a bogus hotspot that looks exactly like a known hotspot (e.g. T-Mobile, Boingo, Wayport). One way to guard against this type of fraud is to download software from the provider’s website and only access their hotspot using that software.

Be sure to virus check their software before installing it.

(2) Another way to guard against rogue access points is to review a website’s certificate for authenticity. Simply click on the lock or key icon of the website page and check to make sure that the certificate was issued to the actual service provider (e.g. T-Mobile, Boingo, Wayport), by a legitimate authentication service (e.g. VeriSign, Thawte), and that the certificate is not expired.

While it is not a good idea to transmit personal information like credit card details, bank account numbers, and user names and passwords over a public hotspot, you can’t escape the need to establish an account with the hotspot service provider at the time of initiating a connection. By following recommendations 1 and 2 above, you can significantly limit your exposure to risk. Should you still have concerns, you might want to consider a credit card account with a very low charging limit (such as less than \$100) and reserve that card for online transactions of this type.

Most public hotspots don’t use encryption techniques to protect the data being transmitted over their network. It is up to individual users to encrypt their files. Remember, with the right software tools, wireless traffic can actually be read.

Methodologies you could deploy include VPH, SSH or SSH tunnel to securely connect to your “home” network. Check with your hardware supplier and/or Internet Service Provider (ISP) for more details on how to use and set up these tools. There are also public services that offer VPN connections to individuals and small businesses.

An additional security measure to consider is web-based e-mail that employs secure data transmission. This service is provided by your e-mail service provider and is an excellent option for anyone who travels with a laptop and regularly accesses their e-mail.

If you are not able to ensure that the data being sent is encrypted over the wireless network hotspot, then you can assume that it is able to be read by anyone using wireless surveillance software. Therefore, it would not be prudent to send information of a private, personal or sensitive nature to a non-secure website or via an e-mail message.



Using mobile phones and PDAs



A number of mobile phones and PDAs today have Internet capabilities, making it possible to access email and view websites at any time, from any location. These highly portable devices are moving closer to computers in terms of functionality, but few users recognize the security issues associated with these advancements. Most of us have come to accept the fact that a personal firewall and anti-virus software are minimum requirements for protecting our information assets. It is now clear that just like our computer systems, mobile devices that access the Internet are susceptible to viruses, Trojan horses, worms, spyware and other forms of unauthorized access.

RECOMMENDATIONS	WHY THIS IS IMPORTANT
<p>Regularly backup your mobile device</p>	<p>When you synchronize your mobile device to a computer, a lot of data is ultimately stored on the computer's hard disk. However, you typically don't synchronize program files and other large data files. Periodic full backups are recommended in the event you need to fully restore a mobile device.</p> <p>WARNING: Ensure that backup files are stored on reliable media and in a safe location</p>

RECOMMENDATIONS	WHY THIS IS IMPORTANT
<p>Install a firewall</p>	<p>Firewalls strengthen the security protection for devices connecting to the internet.</p> <p>WARNING: This is an emerging area, with security software for mobile phones and PDAs slow to become available to the general user. Your choices may be somewhat limited but you shouldn't put your information assets at risk by not taking action. Install a product that best meets your needs today and monitor future developments with the idea of migrating to a more comprehensive software program when it becomes available.</p> <p>.....</p>
<p>Install anti-virus software</p>	<p>All devices that connect to the Internet require anti-virus software. This is particularly important when sending and receiving email and SMS messages. Your mobile device could further infect your desktop computer or laptop when synchronizing files.</p> <p>WARNING: This is an emerging area, with security software for mobile phones and PDAs slow to become available to the general user. Your choices may be somewhat limited but you shouldn't put your information assets at risk by not taking action. Install a product that best meets your needs today and monitor future developments with the idea of migrating to a more comprehensive software program when it becomes available.</p> <p>.....</p>
<p>Use the password protection feature of your mobile device</p>	<p>As the name implies, a "personal device" often contains personal or sensitive data that you wouldn't want others to have access to. From appointments to account numbers, you wouldn't want these personal details to be available to either the honest person who finds your lost device or the thief who actually stole it from you. It is easy to enable the password protection feature and it will protect the data on both your mobile device and network computers accessible by that device. Refer to page 22 for tips on how to create passwords.</p> <p>WARNING: If you forget your password, your data will no longer be accessible. To continue using your device, you will need to reinitialize and that wipes all data from the file storage area.</p> <p>.....</p>
<p>You may need to install encryption software</p>	<p>If you store sensitive personal data or company information on your mobile device, it should be encrypted in the same way files are on your computer.</p> <p>WARNING: If you forget your password, you will not have access to your data.</p>

Bluetooth-equipped devices use radio waves for communications in much the same way as WiFi. WiFi enables a group of computers, mobile devices and peripherals to communicate without being physically connected by wires, while Bluetooth is used primarily to allow individual devices to communicate with each other over short distances and without the need for wires. Bluetooth operates at a lower power level and covers a much smaller area, making it difficult for someone to intercept your signals unless they are within 30 feet of you. There are, however, some vulnerabilities you need to be aware of. The list that follows identifies the major types of attacks known today. While the

names may cause you to laugh, this is no laughing matter and should be taken seriously.

Be aware that not all devices are susceptible to any or all attacks included on this list. You should refer to the manufacturer's manual and website for more information and possible warnings. As a matter of precaution, it is always best to turn Bluetooth off when it is not being used.

Using Bluetooth Devices



SNARF attack

An unscrupulous person gains access to your phone and changes your settings. This is most likely to occur when in close proximity, such as attending a conference, eating in a restaurant, travelling on public transport, etc.

BACKDOOR attack

Bluetooth devices communicate with each other through a mechanism called "pairing". Some phones have a flaw that will allow them to pair with a previously authorised device even if that device has been removed from the list of authorised devices. The device can then make a connection to your phone and will have access to all capabilities of your

phone. How could this happen? Someone borrows your phone and pairs it with their own device (e.g. headphone), then deletes that pairing from your phone. Not all phones have this vulnerability and many have been updated to overcome this problem.

BLUEBUG attack

This attack allows someone to connect to the basic “command set” of your phone, making it possible to divert your phone, listen in on conversations and other forms of surveillance that you do not want.

Bluejacking

Bluejacking is mostly harmless, with people in close proximity sending annoying messages to your phone. It is akin to spam in some instances.



It can, however, quickly change from being a minor nuisance to something far more dangerous. For instance, a text message could be sent that asks you to enter four numbers and by doing so you have actually paired your phone with the perpetrator’s device, giving them full access to your phone, including stored data. Never respond to messages of this type.

RECOMMENDATIONS

Choose Bluetooth phones and devices that are not susceptible to the types of attacks noted above.

Keep your phone in “hidden” mode.

When Bluetooth mode isn’t being used, disable the facility.

WHY THIS IS IMPORTANT

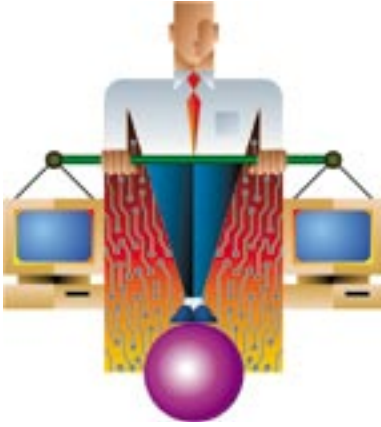
As issues are identified with Bluetooth technologies, the device manufacturers are usually very responsive and the problems are fixed in future devices. In addition they will often release a “patch” to fix existing phones. People without some technical ability may find it difficult to apply the patch to their phone and so it is much easier to buy a phone that is not vulnerable.

.....

By keeping your device in hidden mode you will ensure that unauthorised people do not stumble upon the existence of your Bluetooth enabled device and try to explore the device for vulnerabilities.

.....

While it may be inconvenient to continually turn Bluetooth on and off depending upon whether you are using it or not, it is the best defence against any vulnerabilities in the protocol. This tactic of turning off un-used or un-needed facilities is a common security recommendation in all environments.



for rogue access points, as you could be accused of the very wrongdoing you are trying to guard against. The best way to guard against this kind of unintentional act is to remember this advice: Don't connect to any device that doesn't belong to you.

STEALING BANDWIDTH

With the growing use of wireless networks by business and home users, it is becoming easier to naively stumble across an open wireless network that affords you Internet access. To

Understanding legal issues



While the legal systems in APEC economies and countries around the world differ markedly on their definitions and treatment of computer-related crime, all wireless network users need to be aware of the types of crimes being facilitated through wireless networks today and how to protect personal and company assets.

ROGUE ACCESS POINTS

Even if you implement all recommended security measures, the possible connection of a rogue access point is a significant threat. This is when an unauthorized access point is attached to the network, generally without the knowledge of the network administrator. This could be the innocent act of an employee who purchased an access point and installed it in his office without understanding the security implications. On the other hand, this could be the malicious act of someone intent on doing harm or committing a crime using your network. This can cause obvious legal problems for a company and for that reason it is important to continually monitor for the presence of rogue access points.

There is one caveat to this recommendation, however. Care must be taken when monitoring

actually use one of these open wireless networks without first obtaining permission from the Internet account holder could be considered theft in most jurisdictions. Even if it is not actually breaking the law in a given jurisdiction, it certainly isn't honorable or moral. Many Internet accounts have download limits and impose strict penalties for exceeding monthly allotments. To use someone else's Internet connection without their knowledge and permission is potentially the same as stealing from them.

EAVESDROPPING

Tools are readily available today that make it possible to view data flowing across a wireless network. Observing data across a network that does not belong to you or your organization is the same as covertly tapping into a

phone conversation and in most jurisdictions could be considered an illegal act. Be aware that if an unauthorized person is using your network because you haven't taken proper measures and you are looking at their data, you could be accused of eavesdropping on them.

STEALING DATA

When you are working at home or in your office, you will have "printer and file sharing" enabled on your laptop to facilitate the exchange of files and for purposes of sharing resources like a printer, scanner or Internet connection. However, if you access either a wired or wireless network from a public hotspot (Internet café, airport lounge, hotel room, etc.), you must make sure that "printer and file sharing" is disabled. If you don't make this change, the data on your computer is potentially exposed to others accessing the same hotspot and a dishonest person could easily steal whatever they are interested in. An act of this kind is illegal, but prevention is extremely important to protect personal and company assets.

COMPUTER VANDALISM

Destroying or altering data on a computer that doesn't belong to you is a case of vandalism and in most jurisdictions will be prosecuted as such. The issue for home and business users is to understand the critical importance of protecting their wireless network from intruders. There are computer crime laws that make it illegal to access a computer without authorization

to destroy modify or alter data. (explain how you could violate these laws by accessing someone else's computer)

INADEQUATE SECURITY - RAMIFICATIONS FOR BUSINESSES

This is not an issue related only to wireless.

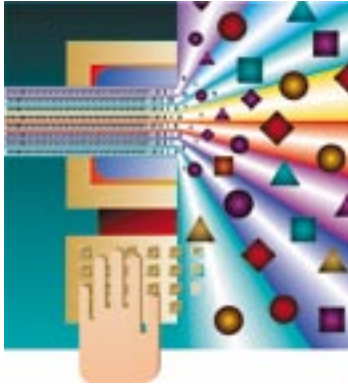
Business owners and managers today have significant corporate responsibilities for the protection and continuation of their businesses. If a business loses significant amounts of money or is forced to close due to a lack of appropriate security measures, owners and managers may find themselves at risk of being prosecuted by government regulatory bodies. APEC Privacy principles indicate that individuals who entrust their information to another are entitled to expect that their information be protected with reasonable security safeguards.

JAMMING SIGNALS

Jamming, also known as "interference," involves using a transmitter to broadcast signals to a device(s) of a wireless network from a nearby location in an attempt to overload the wireless network and cause it to fail. Jamming is a crime in many jurisdictions. The only real defense against jamming attacks is to physically protect the wireless broadcast area from unauthorized individuals.

USING WIRELESS EQUIPMENT THAT HAS NOT BEEN APPROVED

In most APEC economies and countries around the world, government regulators approve the types of wireless equipment that may be used. Make sure that the equipment you are using or plan to use has been approved by your government. You may hear of ways to enhance the performance of your wireless network through the "creative" use of non-standard equipment. You could be in violation of the law if you use any type of equipment that is not sanctioned by your government. For example, if a device outputs too strong a signal, you could unintentionally interfere with or jam other signals and thus be in violation of the law. Another problem is grey market equipment: while it might be considerably cheaper, there is a good chance it is not configured for proper use in your area.



Wired or wireless, network or standalone, there are some standard practices that should be followed when connected to the Internet. The following general security recommendations will help to secure your computer and protect the information stored on it:

Computer Security Essentials



Upgrade to latest version of your operating system

For security reasons, it is extremely important to update your operating system to the most current version. All users of Windows, Apple Mac and Linux should check the appropriate website regularly for software upgrades. By using the latest version, you get the benefit of “patches” for known security problems, protecting both your computer and your data from becoming a target.

For Windows 95 and 98 users, your operating system software is no longer supported by Microsoft, thus making you particularly vulnerable to attack. You should immediately upgrade to a current (and supported) version of Windows or, alternatively, migrate to Linux. In addition to upgrading your operating system, you need to engage in secure computing

practices as outlined in this section. Regardless of which operating system you are using, you will still have a security risk if you don't follow the recommendations below.

WARNING: Prior to upgrading to the latest version of your operating system, ensure that (a) your computer is sufficiently powerful to run the new operating system, and (b) your application programs are compatible with the new platform.

Create strong passwords

Follow best practice recommendations when creating passwords. Hackers are able to discover a simple password in a matter of minutes. However, a strong password that follows these best practice “do’s and don’ts” will need much longer to “crack”.

- Don't use any word that can be found in

any dictionary (any language) including scientific terms.

- Don't use any word in reverse that can be found in any dictionary (any language).
- Don't use any word that can be associated with you, i.e. address, phone number, birth date, pet's name, nicknames, favourite sports activity or hobby.
- Don't use consecutive letters or numbers like "abcdefg" or "234567".
- Don't use adjacent keys on your keyboard like "qwerty".
- Do make it simple enough that you can remember it without writing it down.
- Do use a combination of letters, numbers and special characters in random order.
- Do use upper and lower case and include special characters (* @ #).
- Do use at least 6 characters and the longer the better.
- Don't give your password to anyone for any reason.
- Don't select the "remember my password" feature associated with some websites and disable this feature in your browser software.
- Don't use the same password for everything - have one for non-critical activities and another for sensitive or critical activities.
- Do change your passwords every month for extra security.

An example of a good password could be V-pfC~6M



WARNING: Do not write passwords down. This is the one big mistake users often make. Software is available to securely manage your passwords and you will only have to remember one password. All password should be changed regularly, about every six weeks.



Install a "personal firewall" on your computer

Through the use of a "personal firewall" you can protect your computer from hackers and prevent unwanted programs from entering your system in the first place. You might think you have nothing on your computer worth looking at or stealing and therefore see little or no reason to concern yourself with a personal firewall. There are, however, many reasons why hackers may want to break into your computer.

All computers accessing the Internet should use a firewall. This should not be optional or based on your level of Internet activity. The occasional user is just as vulnerable as the full-time user in terms of random scanning by hackers. There are several firewalls available at no cost from major vendors. Refer to their websites for more information and download the one that will best meet your requirements. You can be held liable for unauthorized users attacking others through your insecure computer. Due-care must be shown.

WARNING: From time to time popup windows from your firewall will appear with warnings and you might need to respond to a question. Be sure to take the time to understand the nature of the question so you can respond appropriately.

Install anti-virus software

It is imperative that you install anti-virus software on your computer. Make sure it is the latest version and take advantage of the "automatic update" option offered by most software programs to maintain up-to-date virus definitions. Never open unanticipated files from anyone unless you can positively verify what it is, who sent it, and why it was sent to you. Use anti-virus software to check any suspicious e-mail file attachment.

Anti-virus software stops unwanted and dangerous viruses from entering your computer and other devices such as a PDAs and mobile phones. Viruses are software programs, and the actual effect of any particular virus depends on how it was programmed and for what purpose. Some viruses are deliberately designed to damage files on your system or in some way interfere with your computer's operation. All viruses can potentially damage or destroy files stored on your computer's hard disk.

Be sure to perform regular full virus scans of your system. These scans can be automated to occur at convenient times.

WARNING: Most users understand the need for anti-virus software and have installed it on their computer. However, many forget to keep the virus definitions up to date and this can actually render the software useless. Your best defence is to select the "automatic update" option - this facility automatically checks for new virus definitions each time you log onto the Internet.

Install an anti-spyware program on your computer

Spyware is a software program used for advertising, collecting personal information

for marketing purposes or changing your computer's configuration, all without your consent. You might have spyware installed on your computer if you observe any of the following:

- Pop-up advertisements even when you are not connected to the Internet.
- The page your browser first opens to has changed without your knowledge.
- Your web browser has a new toolbar or other component that you don't remember installing.
- Your computer seems generally sluggish or takes longer than usual to complete certain tasks.
 - Some settings have changed and you can't change them back to what they were.
 - For no apparent reason you are experiencing a rise in computer crashes.

Be sure to perform regular spyware checks on your system to guard against malicious applications. This should be done every two weeks, if not weekly.

WARNING: Each anti-spyware program is designed to look for different types of problems and therefore you should install more than one anti-spyware program. Check with different manufacturers and decide which combination will best meet your needs..

Backup your data

Develop and adhere to a backup strategy for protecting your data. There are many reasons why data is lost and they are not all related to security issues. Power blackouts, hardware failures and human errors can all cause data to be lost. The best protection is to regularly backup your files. You will need to decide on a backup schedule, the type of storage device, and whether you will take advantage of a remote backup service.



Whether you do it yourself or hire a service to do it for you, you will need to determine a backup schedule, with the following in mind:



- **Full backups:** complete set of all data and system files. You generally don't need to do this daily, as most of your files don't change every day.
- **Differential backups:** set of files that have changed since the last full backup.
- **Incremental backups:** set of files that have changed since the previous backup (whether it is a differential, incremental, or full backup). This takes the least time and space, but in the event of data loss you'll need to restore data from several backups and restore them in precisely the correct order.

You can backup to tape, CD, DVD or auxiliary hard disk. There are services available today that allow you to backup with an online service, providing off-site storage that further protects your data from physical disaster (e.g. fires, floods, theft, accidental erasure)

WARNING: It is important to perform periodic tests of your backups. What good is a backup if you can't use it to restore your system? Current best practice is to store backups with a secure, on-line storage facility. This protects your data from physical damage (e.g. fire, flood) as well as unauthorized access.

Update your software regularly

Better yet, take advantage of the "automatic update" option whenever available. The software running on your computer could be a source of security problems if you don't keep it up to date. After a program has been in use for a while, small problems are discovered and

the manufacturer will need to create "updates" or "patches" to fix them. Additionally, with each new version of a software program you can count on new security measures being introduced, as reputable software manufacturers are working hard to make the online environment safer for users. This is especially true for operating system software, be it Windows, Mac or Linux. It is in your best interest to run the most up to date version of your operating system and all application programs all well.

WARNING: The "automatic update" option is the best way to keep your software up to date. However, if you are on a volume-based Internet access plan, you may have to monitor program updates to avoid exceeding imposed download limits. Some updates involve relatively large files.

Don't open e-mail attachments

You should NEVER open an e-mail attachment unless you are certain of the source. For example, e-mail addresses can be forged to look like the sender is a person you know and trust. Since most viruses, worms and Trojans are disseminated by e-mail attachments, your best defense is to check with the sender before opening the file. You can also use your anti-virus software to perform a manual scan of the attachment to determine if it is safe to open.



When setting up your wireless network, did you:

- Control your broadcast area? [Page 9](#)
- Change default passwords and user names? [Page 10](#)
- Turn on encryption? [Page 10](#)
- Use network names (SSIDs) carefully and wisely? [Page 10](#)

For advanced users

- Limit access rights? [Page 12](#)
- Authenticate all users? [Page 13](#)
- Limit the number of user addresses? [Page 12](#)

To secure your computer and personal data, make sure you:

- Upgrade to latest version of your operating system. [Page 22](#)
- Create “strong” passwords. [Page 22](#)
- Install a personal firewall. [Page 23](#)
- Install anti-virus software. [Page 24](#)
- Install anti-spyware programs. [Page 24](#)
- Backup regularly. [Page 24](#)
- Upgrade all application programs to the latest version. [Page 25](#)
- Don’t open e-mail attachments. [Page 25](#)

26

Wireless Security Checklist



Before accessing the Internet from a public wireless hotspot, did you:

- Turn off “file and printer sharing”? [Page 14](#)
- Disable “computer-to-computer (ad-hoc) networking”? [Page 14](#)
- Clear list of “preferred networks”? [Page 14](#)
- Check to make sure you aren’t transmitting sensitive information? [Page 15](#)
- Encrypt all files? [Page 15](#)

Before using your mobile phone or PDA to access the Internet, did you:

- Install a firewall? [Page 17](#)
- Install anti-virus software? [Page 17](#)
- Create a “strong” password? [Page 17](#)
- Enable encryption? [Page 17](#)
- Turn off Bluetooth when not in use? [Page 18](#)
- Back up your data? [Page 16](#)

To be certain you are not in violation of the law, make sure you:

- Don’t access private wireless networks without explicit permission. [Page 20](#)
- Don’t try to covertly access the data of other users of private wireless networks. [Page 20](#)
- Don’t make any unauthorized changes to data or settings on any components of private networks. [Page 21](#)
- Don’t eavesdrop on private wireless networks without permission. [Page 20](#)
- Ensure that any wireless network within your responsibility is secure against unauthorized use. [Page 21](#)



LINKS

www.ieee.org	The IEEE (Eye-triple-E) is a non-profit, technical professional association of more than 360,000 individual members in approximately 175 countries.
standards.ieee.org/wireless/	The IEEE Wireless Standards Zone
www.wi-fi.org	The WiFi Alliance is a non-profit, international association formed in 1999 to certify interoperability of wireless Local Area Network (LAN) products based on IEEE 802.11 specifications
www.apple.com/support/security/	Apple computer's security page
www.microsoft.com/security	Microsoft's security home page

ACKNOWLEDGEMENTS

While this booklet was written by Michael Baker and Jan Gessin of AOEMA, many people participated in its development by giving freely of their time and advice. In particular, employees of the following governments played a vital role in ensuring the accuracy of this document:

- Australian Government
- Office of the Government Chief Information Officer, Government of the Hong Kong Special Administrative Region
- The Royal Thai Government
- United States Government

Additionally, individuals from the private sector and academia took the time to review this booklet and we would like to acknowledge their contribution:

- Nick Ellsmore – SIFT Pty Ltd (Australia)
- Cynthia Kuo - Carnegie Mellon University
- Adrian Perrig - Carnegie Mellon University
- Craig Searle - SIFT Pty Ltd (Australia)
- Dr Corey Schou – NIATEC, Idaho State University
- Rosemary Sinclair – International Telecommunications Users Group (INTUG)
- Richard Thwaites – Rich Communications
- Dr. Jesse Walker - INTEL



Asia-Pacific
Economic Cooperation

APEC Publication #205-TC-01.1

www.apec.org



Asia Oceania Electronic
Marketplace Association

www.aoema.org



Foundation for
Multimedia Communications

FMCC (Japan)
www.fmcc.or.jp

Disclaimer and Copyright

The information and URLs contained in this guide book are accurate at the time of printing.

© Copyright is jointly held by APEC, AOEMA and FMCC, with AOEMA managing all rights and permissions. This guide book may not be reproduced, translated, or published in any electronic or machine readable form in whole or in part and is prohibited from commercial use such as sales and publication without prior written approval of the APEC Secretariat, Asia Oceania Electronic Marketplace Association. APEC,

AOEMA and FMCC and members who are involved in the development of the guide book accept no liabilities for any losses and damages caused directly and indirectly through the use of this guide book. When using this guide book for any purposes, you should explicitly stipulate the source of quotation or reference from "Safety Wireless" by APEC, AOEMA and FMCC.

Please email us at info@aoema.org for feedback, comments or more information.

March, 2005.



Safety Wireless

What you need to know

Answers to your questions

Configuring your Access Point

Using Public Hot Spots

Using Mobile Phones and PDAs

Wireless Security Checklist

Other Publications in this series



Use this guide to create
your own "Safety Net".



Use this guide to communicate
safely on the Internet.