# WIRELESS NETWORKING SECURITY CONSIDERATIONS

## The Pitfalls of Wireless Networks

For road warriors, wireless network technology, often referred to as WiFi, offers a readily accessible and speedy on-ramp to the Internet. WiFi hotspots are becoming increasingly common in the UK and abroad, found everywhere from coffee shops to hotels. Community-based wireless network projects such as The Easton Community Wireless Network Project are building publicly-accessible WiFi networks in their hometowns. For more on community wireless networks in the UK see WLAN.org. and Consume.net.

Gartner market research estimates 30 million people will connect to the Internet via public WiFi hot spots in 2004. However, this proliferation of public wireless networks has evolved with ease of use in mind -- data security has been a secondary concern. Standard WiFi security mechanisms such as Wired Equivalent Privacy (WEP) and the newer WiFi Protected Access (WPA) -- can be cumbersome to configure. As a result (with a few exceptions) Wireless Internet Service Providers (WISPs) such as T-Mobile HotSpot have chosen not to implement the kind of security that protects data transmission on their networks. Simply put, they would rather make their networks easy to use than complicate them with security configurations, which could be a potential turn-off for their customers.

Similarly, in a frenetic rush to lure customers, mobile technology manufacturers have rapidly put products on retail shelves that lack proper safety measures. Laptop computers, personal digital assistants (such as Palm devices), Pocket PCs, and powerful mobile phones with *wireless* networking capabilities usually don't require security to operate and most come with these features turned off by default. Again, securing devices and explaining how to implement security requires an investment in time, and often it's just easier to forget about security -- that is, until something disastrous happens as a result.

## Eight Hotspot Dangers and Ways to Protect Yourself

Because of this emphasis on ease of use, wireless networking has a number of vulnerabilities. People connected to an unsecured WiFi *network* could eavesdrop on your data transmissions (the practice is commonly known as sniffing), and hackers could launch viruses and other attacks. When you connect to a hotspot, you should assume that it is a network environment that you can't trust and that there are pitfalls that could make your wireless experience painful. A good defence involves layers of security, each designed to thwart certain threats. Anticipate the following hazards and apply some safeguards against them.

## Viruses and worms

Keep the nasties out with *Antivirus software*. It's not enough to be cautious just with e-mail anymore, either. Two recently unleashed worms, Sasser and Korgo, infect one computer and then start looking for other networked computers close by to attack. This is especially dangerous when you're connected to a hotspot. If one hotspot user catches this kind of bug, it may try to get you next. So keep your Antivirus software up-to-date with the latest definitions. Better yet, configure your software to check automatically for updates on a regular basis.

## Spyware and malware

Another closely related and increasingly common threat is spyware and malware. The steps outlined in the knowledgebase article Removing Spyware, Malware and Viruses from Windows will protect you from most of this harmful software, but you can also install free utilities like Spybot Search & Destroy andLavasoft's Adaware.

## Flaws in software

Be diligent about updating key pieces of software — particularly Microsoft Windows, Outlook, and Internet Explorer — to close vulnerabilities in them. Take advantage of Microsoft's Windows Update service and Apple's Software Update utility to *patch* newly found security vulnerabilities. Like virus protection, you can set your computer to automatically check for and download updates. You may have to take further action to install them after they have downloaded.

## Intrusions

A personal firewall will help prevent active attacks, such as attempts to search through your computer for interesting information or deliver a damaging piece of software to your system. Windows XP and Macintosh OS X have basic firewall capabilities built-in. Read about other personal firewalls and their more advanced features in the article Firewalls.

Like Antivirus protection, a firewall also needs to stay up-to-date and be configured correctly in order to be effective against the latest attacks. Software publishers
like Symantec and McAfee now bundle their personal firewalls with their Antivirus offering. This is often cheaper than buying the two pieces separately, and there is more integration between them, which offers the ability to update both parts with a single click.

## Snoops

Secure the transmission of your data over the wireless network by encrypting it (for more on encryption see the TechSoup article NetAction's Guide to Encryption, Part 1. In basic terms, encryption makes the data you transmit incomprehensible and therefore useless to snoops. If your organisation has aVirtual Private Network(*VPN*), use it to make it virtually impossible to decipher the data you transmit in case someone is listening in.

You can also purchase VPN service from a provider. Some WISPs offer VPN to Windows customers (for an additional charge). For a listing of WISPs in the UK see ISP Review.
Some VPN service providers have partnerships with WISPs to provide wireless VPN access. You might also want to check out HotSpotVPN, which offers a low-cost subscription. If VPN is too expensive, at least don't send sensitive information such as passwords, credit card details, or other personal information without securing it first. All widely-used Web browsers support Secure Sockets Layer (SSL) connections, which is the standard way of temporarily establishing a secure connection with online retailers and other Web sites with whom you might exchange sensitive data (see SearchSecurity.com's definition of SSL).
Also, email is particularly vulnerable to snooping if you are not using encryption. In most cases, email is sent "in the clear" — there's nothing to scramble the messages or even your usernames and passwords. When you log on to Yahoo!Mail for example, unless you specify an SSL connection before sending your password, there is no security applied to obscure the emails you send and receive. Popular email applications such as Microsoft Outlook, Outlook Express, and Eudora offer ways to establish a secure communications link with e-mail service providers that support secure connections.

Finally, don't discount the old-fashioned, over-the-shoulder snoop. In a bustling publicly-accessible space, it's not hard for someone to spy on your keystrokes while you enter the username and password to your online banking account, for example. The same precautions apply to kiosk computers, ATMs, and other machines on which you might enter sensitive information.

## Strong passwords

Of course, it makes it much harder to steal passwords if they are complex. A password such as "R#atg09f" is hard to remember and crack because it has all the elements of a good password — a mixture of capital and lowercase letters, numbers, and special characters. But, how do you remember a password that is by design difficult to recall? Check out the TechSoup article An Introduction to Internet Security in the Workplace for a more detailed look at strong passwords.

## Unrestricted wireless networking configurations

The wireless adapter on your laptop or handheld is capable of operating in two modes, infrastructure and ad-hoc. At a hotspot, you should disable the ad-hoc mode, which could allow another user to piggyback onto your connection. In Windows XP, depending on which service packs and updates you've applied, these options reside within the advanced properties of the wireless network connection configuration, If you are using OS X, deselect "Allow this computer to create networks" in your Network System Preferences, or don't choose "Create Network" from your AirPort drop-down menu.

Also, if your device is powered on and you have your networking set to automatically connect to available wireless networks, you could be associating with wireless access points without even knowing it. To prevent this, turn off any features that automatically connect you to available wireless networks.

## Ignorance of risks

Give yourself the advantage by knowing what to watch out for. By reading this article and other information about security, you're already taking an important step towards protecting your computer. Be familiar with the latest news about security threats. If, for example, you hear on the morning news that there is a virus rapidly making the rounds, update your Antivirus program and have a basic understanding of the mechanism the virus uses to propagate (for example, by email attachments, file sharing, etc.). A bit of knowledge about computer security will help you take the appropriate steps to protect yourself.

# Security at Home

Most likely, you'll want to put your mobile technology to work at home too. If you happen to share a wireless connection to the *Internet* with others in your household or apartment building, the security precautions outlined above will go a long way to protect you. As well, if you set up your own wireless network at home, it's a good idea to implement the security features on your wireless access point. Enabling *WEP* or *WPA*, disabling service set identifier (SSID) broadcast and turning on Media Access Control (*MAC*) filtering will make it harder for malicious users to connect. In an organisational setting, the same rules apply, but it may become harder to implement some of these security measures -- the more users you accommodate on a network, the more difficult it is to administer some of these steps. But with more users come more vulnerable entry points for bad things to happen, so it becomes increasingly important to secure the network.

# Loss and Theft

Of course, no *firewall* or software update is going to protect you from the loss or theft of your equipment. Your information is valuable, but so is the *hardware*itself. Use cable locks and other devices to secure your equipment where appropriate. Also, in the event that you do lose your device, password protection will at least slow down a thief or other prying eyes from pilfering information such as credit card numbers and other important data that you may have stored on your machines. It may just buy you the needed time to cancel your accounts or make other arrangements.

# Time to Get to Work

Now it's time to implement these precautions. There are handy guides on the Knowledgebase and TechSoup to help you with the hands-on work, as well as links to other resources below.

Keep in mind that there is an element of co-operative effort when it comes to security. For instance, if more computer users installed Antivirus protection and kept it up-to-date, it would

make it much harder for viruses and worms to propagate. A firewall on every computer would slow the spread of spyware. Increasing security on your mobile technology ultimately helps everyone, especially those who may not know how to apply the same security. At the same time, all this talk about security may seem a bit daunting and cryptic. Implementing good security requires diligence. When you consider the other work you could be doing for your organisation, the benefits of mitigating security risks may seem small. In reality, only a small portion of the population has the ability, the will, and the time to concoct a virulent virus or hack into a laptop you're using in a café. Also, no matter which security measures you incorporate, nothing is perfect, and there is no way to protect against every conceivable threat. But understanding the risks and having an informed sense of which ones may be the most threatening to you will allow you to take the appropriate steps now and in the future as new threats emerge.

Source : http://www.ictknowledgebase.org.uk/wirelesssecurity