

UnderstandIT

From **MAY DAY CONSULTING LIMITED** in association with **FACILITATORS UK**

A publication designed to inform and enable businesses to understand the implications, costs and advantages of using Information and Communications Technology. Distributed through Chambers of Commerce.

COMPUTER SECURITY: OVER-REACTION OR COMMON SENSE?

Glancing back over recent editions of Understand IT, it is somewhat surprising to realise the large amount of coverage that we have given to issues of computer security.

Some might say that the complex issues of computer and network security are a gross over-reaction; that it has proved to be just another opportunity for the development of a new sector in the IT industry. The sceptics among us might even go so far as to suggest that much of the insecurity has come about with the collusion of the industry itself – another conspiracy theory.

What is certainly true is that many of the problems experienced are to some extent self-inflicted – both in the business and the residential sectors.

In reality, it is the very success of the Internet and computer technology in general that has attracted the attention of the fraudsters, the hackers and plain mischievous.

User education is essential to raise the level of awareness of the seriousness of some threats. A recent straw-poll survey in the USA (as reported by the National Cyber Security Alliance), concluded that over 30% of the respondents considered that they would be more likely to be struck by lightning, audited by the IRS or win the lottery before they would be the subject of some computer security threat. In reality, the chances of being hit by some form of cyber threat is 70%, compared with considerably less than 1% in the case of the other events!

The trick is to balance good business practice with a common sense approach to security. There is little point in implementing such stringent security measures that they severely hinder your company carrying out its core business. However, in many sectors, demonstrating the implementation of stringent security is a necessity – in the banking sector for example.

We make no apologies for continually stressing the need for a pragmatic and professional approach to the implementation of security on your computing and networking environments.

If you have any concerns at all about the implementation of any security on your individual computer(s) or your network, don't become a statistic - please call Alan Finch on 01224 657497 as soon as possible.

WIRELESS NETWORK SECURITY

In the June 2004 edition, we briefly discussed the need for improving security on the growing number of wireless networks in use, both in small and large offices, but also in many residential situations.

In this article, we will talk a little about configuring a wireless router/access point to ensure that security features provided with most devices are implemented to provide a basic level of protection. We apologise if this goes into some technical detail, but it is necessary at this level to understand how to configure basic security. We will attempt to explain as many of the technical terms as possible

We were recently called by a client who uses one of these devices to provide a peer-to-peer network in their office. They were complaining that in their view the performance of their Internet link had dropped dramatically in recent days. Even when no one was accessing the Internet, the Internet port was showing considerable activity (indicated on the front panel LED – Light Emitting Diode).

By accessing the device's configuration information we investigated further to reveal that someone in the vicinity was using the wireless router to access the Internet at the expense of our client.

The router had been set up with only the default configuration, with no security implemented at all. Therefore anyone within a 100 metre range of the router, suitably equipped with a wireless access card in their computer was able to access our client's network and "share" their Internet link.

Unfortunately, this is a common problem with users of wireless access points and routers. The following notes demonstrate how this problem can be overcome by implementing the basic security features provided by such devices.

For the purposes of this article, we are using the Linksys Wireless Access Point/Router as an example (Linksys is now owned by Cisco). Other manufacturers' devices will have similar features, and will be implemented in a similar fashion.

The Linksys Model BEFW11S4 is a wireless transceiver conforming to the CCITT radio specification 802.11b.

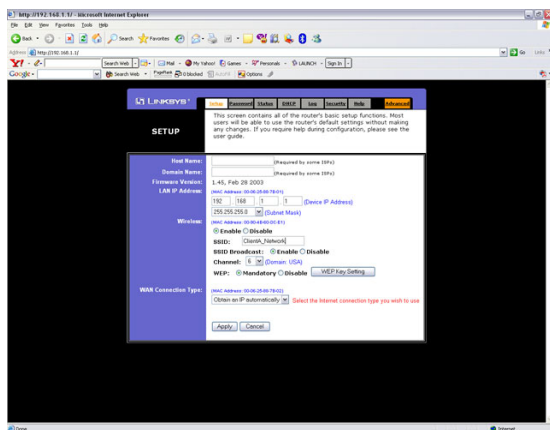


It has 4 physical network ports for connecting conventionally cabled computers and one Wide Area Network (WAN) port for connecting to the Internet. It can support any number of wireless users.

Administration and configuration of the device is carried out via a web interface using Internet Explorer or Netscape Navigator. In the case of the Linksys device, the address is 192.168.1.1. Typing this address in the address bar of IE will produce a Logon panel.



Leave the User ID field blank and type “admin” in the password field. This will produce the “home” page of the internal ‘web site’ within the device. From here you can configure every feature.



The first task was to change the identification name of the client’s office network – the SSID (Service Set Identifier). The device is pre-configured with a default name of “Linksys”. We changed this setting by typing in a name for the network that is not immediately apparent to any passing stranger. It can perhaps be cryptic. Remember this name has to be used to configure each of the client PCs wireless network cards, otherwise they will not be able to connect to the network (and neither will any mischievous passer-by).

The second task was to implement the WEP (Wired Equivalent Privacy algorithm) security feature. This provides encryption of information that is transmitted between the computers on the network and the access point/router. In order to do this, we had to specify a “pass phrase” or password, which is then encrypted into a hexadecimal string of characters.

The process is carried out by hitting the WEP KEY SETTING button on the “home” page of the Linksys configuration screen. You can then decide to use either 64-bit or 128-bit encryption (128 is considerably more secure). Enter the pass phrase into the appropriate box and hit GENERATE button. This will produce the 26-character hexadecimal string. The encrypted string was then placed in the configuration of each wireless card on the client’s network. Having completed these steps, APPLY the settings and logout of the configuration screen.

Following the implementation of these features, our client’s security was enhanced and his network was closed to all but his own authorised users.

If you require assistance with implementing these features on your own wireless network, then please contact Alan Finch as soon as possible on 01224 697457.

LOOKOUT FOR OUTLOOK

We recently discovered a very useful tool that has been developed by two enthusiastic technology entrepreneurs. Whilst we do not often recommend commercial products, we thought many of our readers may be interested in trying this utility out.

The product is called LOOKOUT, and is a lightning-fast search tool for use within Microsoft’s Outlook product. It allows you to carry out complex searches for items within your email, contacts, tasks and other categories of information stored within your Outlook folders.

The product has gained such a good reputation that it has come to the notice of Microsoft, who recently announced that have bought the product and are planning to incorporate its technology into their own strategy for enhancing their method of searching for information.

The product is free, and is still available from download from:

<http://www.lookoutsoft.com/Lookout/download.html>

When the software is installed, it creates an additional toolbar within the Outlook window and hitting the SEARCH button produces a window where you enter the search term, which can be a single word or phrase, and the search results are displayed almost instantaneously.

The software can be configured to include searching of more than one set of Personal Folders, and Webmail folders that you have and the Archive folder(s).

Watch for the technology to be integrated by Microsoft within future versions of the Outlook product

We wish to acknowledge with thanks that some of the material contained within this publication has been sourced from Computer Weekly.

May Day Consulting Limited and your Chamber of Commerce have endeavoured to ensure the accuracy of the information contained in this publication, but do not accept liability for any inaccuracy or omission contained within it.

Information on other Business and IT services can be found on our web site at: <http://www.maydayconsulting.co.uk> or by calling Alan Finch on 07968 262079.

May Day Consulting Ltd

....stress free IT

9 Benbecula Road
ABERDEEN AB16 1FT
Tel: (01224) 697457

E-mail: info@maydayconsulting.co.uk
Internet: <http://www.maydayconsulting.co.uk>