

1. Security Tips for Wireless Devices for SMEs

Wireless computing devices that offer technology advances to SMEs are now widely accepted as a cost effective means for the Small Business owner/manager to connect computers and peripherals as the business grows in size.

Wireless computing technology is instant on, now, and it comes straight out of the box, ready to use.

As the owner/manager of an SME, a key consideration is how much you save in time and cost, by being able to "do it yourself" and the device can be ready in minutes.

2. Wireless Technology Issues

There are some key technology issues with wireless computing devices that owner/managers of SMEs need to be aware of that need to be considered to make sure that the SME business and data, is adequately protected against a range of risks.

3. What risks?

Wireless networks (and associated devices) can be attacked through rogue access points e.g., ad hoc or free WiFi networks, or by accidental discovery, or malicious association, through unprotected access points and wireless network monitoring devices, that can be easily installed in public areas and/or are located nearby your office or place of business.

4. Plug and Play/Instant On

All the latest wireless devices come with a "plug and play – instant on" capability inbuilt, so in most cases, hooking wireless systems together is a breeze, when you know how.

With wireless computing devices, the retailer (and the manufacturer) will tell you, that it's just a question of selecting the right device for your needs, opening the box, turning on the power and presto, the device discovers and connects to your existing system such as Microsoft Vista or Windows XP. It's as simple as that, you can have the wireless router, printer, laptop or PDA connected in minutes rather than hours.

Wireless Connectivity, can happen in an instant (almost) and you can surf the internet, send emails, touch base with the office and get in touch with customers and suppliers, instantly, using your new wireless connection.

5. Back to Basics

Wireless devices can transmit over a distance without the use of hardwired data cable. The distances involved for wireless computing devices may be short (a few metres as in wireless mouse and keyboards, & television remote controls), longer for routers and telephones, digital cameras, printers, Blackberries/PDAs etc. In reality, "Wireless" has been around for years in one form or another with some of the earliest "consumer related" examples being garage door openers, along with cordless telephones.

6. Wireless is booming

Retailers will tell you, with a bit of prompting, that sales of wireless computing devices such as GPS, iPods, Bluetooth and 3G telephones, Blackberry and personal digital assistants (PDAs), along with wireless routers, mice, keyboards, digital cameras, wireless printers, etc are at an increased tempo.

Wireless devices for use in the wider consumer market such as; TV remote controls, wireless security alarm systems, stereo headsets, LCD, Plasma and satellite television and state-of-the-art digital cordless telephones were also high on the sales list, but these aren't as big an issue for SMEs in terms of security issues, unless they are embedded within the business as part of the office equipment tools in use to run the business.

7. Out Of The Box Installation

If you are a typical owner/manager of an SME, unless you already know this, most of the devices will be installed using the Out-Of-The-Box settings, known as the "manufacturer default settings".

This is "manufacture by design" to allow and enable the new device to automatically detect the wireless access point closest to the new wireless device, so that the functionality and operation can commence immediately once charged up, if battery driven, or powered on at the mains.

8. Key Areas to be considered

SMEs are typically time poor when it comes to adminstrivia, and may have overlooked or not be aware of the default settings risks in their rush to use the new wireless computing device.

There are 3 key areas containing around 12 different aspects containing default settings that need to be considered; Authentication, Encryption & Access Control.

Within these areas there are some vital keys or settings that can be a single point of risk for an SME/SOHO business, and when more than 2 of these items are left unchanged (or are set inappropriately) then the level of risk increases significantly.

9. Factory default settings apply

In practise, most wireless devices in the SME/SOHO environment are rarely altered from factory settings by SME/SOHO users, hence the risks of loss of data, or malicious use of information can be potentially damaging for the small business owner/manager.

10. Turn It Off (When not needed)

If you don't need access 24 hours a day 7 days a week, switch off the wireless access points across the business (e.g. after hours and on weekends) to minimise potential exposure to malicious activity.

PCProfile is mindful of the fact that for SMEs the business "hours of operation" is a 24 hours a day / 7 days a week affair in most cases!

Can you afford to lose customer database information, credit card data, membership lists, designs, and documentation, and other sensitive financial data etc that is on your systems through lack of knowledge about the issues presented by the use of wireless computing devices?

11. Reverting to default settings is a risk too!

Not to be overlooked is the impact of “reverting to the default settings” after a service or support issue, or some major outage, (or advised by the Helpdesk at the ISP – who should know better!) which then returns the settings back to factory defaults. This is often done by inexperienced personnel or through lack of knowledge. Reverting to factory default settings without considering the issues and implications, will overturn any levels of protection previously employed over data and exposes you to risk.

12. Check that Your level of security is right for your business

It’s time to check your systems and make sure that you have security measures in place, appropriate to your level of business risk, as it could be a “Plug and Pray” environment that now exists at some sites!

13. Practical Wireless Security Tips

PCProfile offers the following key tips for SME owner/managers when using Wireless computing devices in their business from a Software Tutorial Package called “Tips and Tricks for Wireless Systems” - It is recommended that multiples of these techniques (not just one only!) be employed at all times for a high level of protection!

- ALL Factory default settings should be changed and unique keys used;
- Default User name and Password must be altered;
- Service Set IDs (SSIDs) must be changed to something that is meaningless to outsiders;
- Beacon intervals need to be set to a reasonably long length to minimise exposure;
- WEP and WPA keys must be altered from factory settings;
- Infrared ports need to be disabled,
- Encryption may need to be enabled;
- File sharing needs to be TURNED OFF!;
- Make sure all wireless access points are securely firewalled and;
- Ensure that recommended manufacturer patches and fixes are promptly applied to wireless devices and PCs.

Learn how to secure your systems!



Tips and Tricks for Wireless Systems

For more information purchase the complete tutorial which shows illustrated examples

Available from www.pcprofile.com





Worldwide Copyright Notice

Copyright © 2007-2008 PCProfile trading as Rob Harmer Consulting Services Pty Ltd ABN 77 035 134
400 All rights reserved worldwide.

Guidance For Publishers

Publishers are encouraged to publish this report as free content resource in accordance with the following guidelines:

- 1) Articles must be published "as is" (unedited);
- 2) Articles must be published with the author's bio paragraph and copyright information included;
- 3) URLs listed should be set as hyperlinks, with no redirection;
- 4) Whenever possible, authors should be notified of intent to publish;
- 5) This Published Article cannot be used in spam communications or sold;
- 6) PCProfile prohibits the use of copyrighted material in a manner that violates the copyright owner's rights;
- 7) Publishers who violate copyright law are legally liable and subject to possible fines under Copyright Laws worldwide.

Disclaimer

The content of this report is provided for informational purposes only as "guidance notes" and for redistribution as outlined in the "Guidance For Publishers" paragraph and Copyright Notice above. PCProfile does not represent that all technology aspects have been outlined as a complete position and does not accept any responsibility or liability for the use or misuse of the content of this report or reliance by any person of the publishers contents.

About the Author

PCProfile is an Adelaide based company with over 30 years practical computing experience in small, medium and large enterprises and offers managers and business owners in SMEs, and SOHO businesses practical tips and advice on how to get the best out of the technology used by your SME/SOHO business.

Other Self Help "Tips and Tricks" Tutorials and feature articles are available on;

- Outlook Express Tips and Tricks,
- email Tips and Tricks,
- email Newsletter Tips and Tricks.

PCProfile also runs seminars on technology topics for SME and SOHO business owners.

www.pcprofile.com email enquiries@pcprofile.com Mobile 0448 650 227

ORDER FORM

ONLY 1 LICENSED set needed per SME/SOHO

ORDER PAYMENT DETAILS
For your security orders are only taken **VIA FAX** using credit card details we offer Visa, Mastercard & Amex facilities

Contact Name:..... Organisation:.....

Postal address for invoice mailing
.....City/Suburb.....Country.....PostCode.....

Phone.....Facsimile..... Order number to be quoted on Invoice _____

Payment - via Credit Card - Please circle one - Visa - Mastercard - American Express

Card Number _____ Expiry Date...../.....

Cardholders name..... Signature.....

WirelessTaT	Wireless Security Tips and Tricks	\$ 50	Price includes 10% GST
		TOTAL this order	\$50

PLEASE INSERT e-mail address for shipment of zipped files

e-mail address _____@_____

Files will be sent via zipped e-mail within 24 hours of credit card authorization.

Australian customers have 10% GST already included in the above prices

Please fax your signed order details to: (08) 82651961

We post our official Tax Invoice with credit card receipt for your security to your business address.

Rob Harmer Consulting Services Pty Ltd ABN 77 053 134 400 <http://www.pcprofile.com>