

**PROFIT**guide.com

YOUR ONLINE GUIDE TO BUSINESS SUCCESS

SITE SEARCH



Home ownership  
for small business owners  
made easier.



YOUR BUSINESS

## PROFIT Magazine

### Wondering about Wi-Fi

Is the hottest thing in high-tech right for you? Let our Q&A show the way

By Andrew Wahl  
September 2003

SPECIAL FEATURES

What is Wi-Fi?

Short for "wireless fidelity," Wi-Fi is the nickname for the 802.11b wireless networking protocol that enables high-speed wireless local area networks (WLAN). It uses radio signals broadcast at distances of up to 100 metres from access points known as "hotspots," allowing tether-free access to computer networks from any computing device — be it a PDA or a printer — equipped with a Wi-Fi card (\$60 to \$100) or Intel's Centrino chip. So, for instance, Wi-Fi can let you plug into your corporate intranet from anywhere in the office, or plug into the Internet at a growing number of high-traffic public locations that offer Wi-Fi access. Top speed: 11 megabits per second — about 100 times faster than a dial-up 56k modem.

WINNERS

buy this issue



Who can benefit from Wi-Fi?

"It all depends on the mobility of your employees," says Mark Pineau, principal consultant with Fujitsu Consulting in Toronto. "If they are away from their desks more than half the time, then you're going to get a benefit." And, in some situations, implementing Wi-Fi is much cheaper than running new cable throughout an office, particularly in

older buildings. That said, there are limitations, says Scott Murphy, vice-president of Waterloo, Ont.-based Data Perceptions. "For instance, a wireless network can't handle really big files as effectively as a wired connection."

Can't Wi-Fi networks be hacked?

"There is an increased security risk to wireless," says Murphy. "However, if you have the proper security mechanisms and procedures, the reality is you're going to be equally secure as with a wired network. But there are additional processes you have to put in place to deal with it." Doing the basic things is enough to keep almost everyone out of the network. Michael Rozender, an Oakville, Ont.-based IT consultant specializing in broadband wireless, points out that many of the early Wi-Fi security breaches were caused by executives using inexpensive consumer Wi-Fi gear. Pineau stresses that the first step is educating employees: "A lot of time has to be spent up front enforcing policies to make sure people aren't bringing other access points in or doing silly things like turning off security features." Obviously, firewalls are important. And if you want employees to use public Wi-Fi hotspots, you'll need VPN (virtual private network) software with 128-bit encryption, which requires authentication before allowing access to your corporate network. Depending on the sophistication of the software, it can cost less than \$100 per user or upwards of a \$1,000. But Rozender points out that for most work on Web-based intranets and extranets, it's often enough just to turn on your Internet browser's SSL (Secure Socket Layer), which scrambles the pages being viewed. It's easier to use and cheaper for IT staff to administer.

How much does it cost to use public hotspots?

Individual monthly subscriptions to Wi-Fi services cost between \$25 and \$75. Unfortunately, a subscription to Service A won't give you access to a hotspot running on Service B. In the likely event you're stuck without service, you can purchase single-day access for about \$15.

Is Wi-Fi another piece of hype?

No question, there is a lot of overexuberance about public hotspots. While there are currently about 450 in Canada, some industry watchers expect to see as many as 4,200 by 2007. Some business owners have launched free service to their customers, but few insiders think that will last. As for paid-access to public Wi-Fi, the jury is still out on what business models will prove sustainable. "Just about everybody agrees that we haven't figured out how to make money at this thing," says Rozender. But Wi-Fi is a consumer-driven phenomenon that will inevitably infiltrate your corporation. "Every company today should have a wireless strategy," says Rozender, even if that strategy is as simple as banning all Wi-Fi from the workplace. If they don't, he says, it's only a matter of time before early-adopter employees bring in their own off-the-shelf access points and hook into the corporate intranet — and suddenly there'll be a virtual hole in the company wall.

S  
(and unsubscribe)

e

e

e

e

first name:

|

last name:

|

e

|

[TOP](#)

© 2003 Andrew Wahl