**USA TODAY** **Travel** Smarter trips start here

Home
News
Money
Sports
Life
Tech
Weather

**Search Travel:** Enter a keyword **and/or** DESTINATION

SMARTER TRIPS START HERE | TRAVEL HOME | DESTINATIONS | HOTELS | FLIGHTS | DEALS

**Travel ▼**

News
Columnists
Special reports
Site Index
**Destinations**
City Guides
10 Great
Special features
Photo galleries
**Hotels**
Find a hotel
Hotel reviews
Hotel deals
Hotel Hotsheet
**Flights**
Today in the Sky
Flight Tracker
Flight schedules
Managing Miles
**Specials & Deals**
Fare Compare
The Real Deal
Hotel
Air
Car
Vacations
Cruise
Marketplace

Cars ▸

Jobs ▸

- E-MAIL THIS   - PRINT THIS   - SAVE THIS   - MOST POPULAR   - SUBSCRIBE

Posted 11/7/2003 10:29 AM    Updated 11/7/2003 10:40 AM

**REUTERS**

# Is wireless world a secure one?

By Michael Conlon, Reuters

CHICAGO — The wireless world is spreading rapidly, offering business travelers equipped with laptops or other devices the chance to connect everywhere from coffee shops to hotel lobbies.

Headed for Boise? Wayport, a leader in wireless Internet access, recently announced that several McDonald's restaurants in that area were now equipped with "Wi-Fi" environments — local networks where a radio signal allows high-speed access.

McDonald's previously announced plans to provide wireless environments in several hundred of its restaurants by the end of 2003. Wayport (www.wayport.com) says it now provides high-speed Internet access in parts of 12 airports and 675 hotels.

Bangalore, India, recently became that country's first Wi-Fi enabled city with 120 wireless spots, according to "m-Travel.com" (www.m-travel.com), which traces developments in that and related fields. It also reports that while Wi-Fi is growing most Internet access is still done by standard dial-up.

But for those who are entering the wireless world, is there a security or theft concern with all that data and information out there zipping through the air?

Richard Isaacs, senior vice president of the LUBRINCO Group, an international vulnerability management firm that specializes in protecting intellectual assets, says: "The real issue is do you have anything important (worth stealing) and do you have a firewall?"

"If the second is all right you don't have to worry about the first," he said."

He rates the risk of data theft in wireless environments as "very low" for properly protected devices. The bigger problem, he says, is theft of the devices themselves.

"We recommend that everyone use a virtual private network," Dan Lowden, vice president for marketing at Wayport, says. "A VPN will give you a much more secure connection and putting that extra level of security at the device level is what we feel is critical today."

Virtual Private Networks such as the one operated by iPass Inc., (www.ipass.com) automatically add new wireless and other access points each time the user connects.

Lowden says Wi-Fi connections handled by his company have increased 30% each quarter during the past year, and more than 600,000 people made connections through Wayport in the last quarter.

Brian Grimm, spokesman for the WI-FI Alliance, an industry group that developed the broadcast standard, says that since many individual users may not have access to company-provided VPNs, they may want to acquire "VPN-like services."

The alliance carries detailed information on that at its Web site —www.weca.net. He also recommends checking out their site, which lists Wi-Fi locations in more than 50 countries — www.wifizone.org.

The hardware theft issue mentioned earlier has been covered in a recent report from Brigadoon Software, whose products include a program called PhoneHome (www.pcphonehome.com). It enables stolen personal computers to send out secret messages showing where they are being used, allowing them to be traced.

The company says its survey of 676 individuals or companies around the globe is the first to provide a definitive look at the scope of the theft problem. Nearly 45% of those polled said they had suffered a computer theft and of those losses the bulk were mobile devices — 48% laptops and 13% personal digital assistants.

Of all computers stolen more than 16% were taken in transit — taken from cars, trade show exhibits, airports and hotel rooms, the survey found.

USATODAY.com partners: USA Weekend • Sports Weekly • Education • Space.com

Home • News • Money • Sports • Life • Tech • Weather • Travel • Job Center

Resources: Mobile News • Site Map • FAQ • Feedback
Email News • Jobs with Us • Terms of service • Privacy Policy • Media Kit • Press Room

Hotel Reservation Services: Terms & conditions • Reservation questions?

Add USATODAY.com headlines to your Web site

© Copyright 2003 USA TODAY, a division of Gannett Co. Inc.