 [Click to Print](#)

[EMAIL THIS](#) | [Close](#)

[ajc.com](#) > [Opinion](#)

GUEST COLUMN

As wireless grows, so do security risks

By RICHARD A. DeMILLO

Published on: 11/03/05

It's a wild, wireless world out there. Credit cards on cellphones, citywide hot spots and wi-fi phone calls are all technologies on the horizon, guaranteed to make our lives better and keep us constantly connected to the things and ones we love. It's our culture's "anything, anytime, anywhere" mantra — but are there new risks associated with this constant connectivity?

As we gear up for the holiday season, consumers are going to be bombarded with ads and commercials for the newest wireless devices. However, while marketers trumpet the amazing benefits of these products, very little is being said about the very real security risks associated with wireless technology.

Take identity theft, for example. This problem has skyrocketed over the past decade as more personal information is stored on devices such as phones and transmitted across the Internet. Now, add wireless to that mix, and the risks can grow significantly.

On Oct. 26, Atlanta's Hartsfield-Jackson International Airport launched its wi-fi (or wireless fidelity) service, making it the country's largest indoor hot spot where anyone with a wi-fi connection on their laptop can access the Internet. However, in Kirsten Tagami's AJC article on Hartsfield's wi-fi ("Now you can wi-fi, then fly," News, Oct. 27), the only recommendation for keeping users safe was to rely on their own firewalls and security patches — precautions of which most casual and business users know very little.

Wireless users in any hot spot need to pay close attention to security risks. Local security company AirDefense demonstrated these risks this year by testing security vulnerabilities of "hot spots."

From a public park using just a laptop, AirDefense employees could effortlessly log on to an unsecured wireless network owned by a nearby hotel and were able to demonstrate how guest e-mails could have been accessed. Makes you think twice about sending that confidential e-mail while on the road, doesn't it?

And who doesn't know about Paris Hilton and her T-Mobile Sidekick? Hackers broke into her wireless device and lifted the contact information of all her celebrity friends. Imagine if she had her credit card and other personal information on that device.

What can be done to keep our wireless world safe? Three words: design, regulate and educate.

Security solutions that consumers can easily work with should be integral and available in any new wireless devices. It is important that carriers design network architectures with security in mind.

For example, BellSouth recently launched its BellSouth Wireless Broadband Service in select markets in Georgia. This same technology is providing wireless high-speed Internet access for New Orleans residents in the wake of Hurricane Katrina. BellSouth specifically addressed security in several ways: implementing advanced technology that transmits directly from the customer's computer to BellSouth's wireless base station; using coding and the unique ID number of the subscriber unit in transmissions; and manufacturing equipment designed to work only within BellSouth.


From a regulatory perspective, wireless and cellular carriers must work with the Federal Communications Commission and other government bodies to propose strong legislation to deter the proponents of these threats.

Finally, education of both the wireless provider and consumer is the key — and Atlanta is the perfect place to start. The area is home to telecom giants as well as leading security technology companies.

On Nov. 15, a group of top executives from companies in the wireless and security industries will converge at the Wireless Security Summit, hosted by the Georgia Tech Information Security Center. Here, in our own backyard, industry and academic leaders will propose a plan of action for reining in the security risks of the wild, wireless world.

Find this article at:

<http://www.ajc.com/opinion/content/opinion/1105/03edwireless.html>

 [Click to Print](#)

[EMAIL THIS](#) | [Close](#)

Check the box to include the list of links referenced in the article.