

I am deeply disappointed by Commissioner Abernathy's apparent haste in promoting BPL before all the technical merits (and problems) have been weighed. I have seen the ARRL's evidence and find it compelling. Why then does Riley Hollingsworth ask power companies to curtail their interference to the radio spectrum? Or perhaps interference is no longer a concern of the FCC? I would also like to mention that my employer, one of the nation's largest telecommunications companies, forbids me to use a wireless network because of the risk to proprietary data. Surely, no network administrator would ever allow an unsupervised stranger to plug in a Packet Sniffer into a proprietary corporate network. Given that BPL "signals" will make their way into common HF radios, what assurance is there that the simple combination of a HF receiver and a common network Packet Sniffer won't/can't be used to steal user passwords, credit card numbers, etc? I certainly would not want my private (or corporate) information broadcast, and I think most other internet users would feel the same way. BPL interferes with the existing radio allocations. BPL in turn will certainly suffer interference caused by existing users of the radio spectrum. The power line both sends and receives, as does any other "antenna." Finally, I openly question whether any method of data transmission that functions as an unintended "antenna" can be considered to be Secure. A Packet Sniffer is a device that can listen to a network and pick out the individual packets intended for a specific user. Internet usage and email monitored by a packet sniffer is insecure. Please don't be hasty and suggest to the public that they accept a technology with such a glaring security gap. Here is the text from my corporate security department: To: All Lucent Employees and Contractors

From: Lucent Security

Re: Limiting Wireless Computing in Public Access Areas

If you use wireless computing technology in public access areas such as airports, Internet cafes or wi-fi "hot spots," you need to take precautions.

Software has been developed that captures critical information while you're trying to gain wireless Internet access in public places.

Electronic thieves are using devices with this software to tap the communication path between your wireless device and the valid access point server you're trying to connect with. Their goal is to capture your login/password or credit card information, as well as any information exchanges that may follow. The pirating technology has been designed to generate a strong signal to deceive unsuspecting users into thinking they are connecting to a legitimate server. The interception is virtually transparent to avoid detection, and the thief's host device can be easily concealed, making it easy to carry into and out of public access point areas without detection.

If you use Lucent Remote Access (LRA) VPN, your sessions are not protected until after you authenticate to Lucent's network. That means your access credentials (login/password) for the local access point and credit card information is not protected by the Lucent VPN session.

To help prevent the theft of your access point credentials and credit card information, such as your corporate AMEX, Lucent Security recommends the following:

Restrict use of wireless computing technology to only trusted networking environments, whenever possible. Limit your use of public wireless access points in areas such as airports or Internet cafes to urgent business need ONLY.

If wireless access in a public area is needed, ensure the authenticating server provides a protected (https/SSL) session. If the access point does not provide a protected session, find another access point.

Check the authenticity of the certificate of authority (CA) used by the authenticating server. The name and date of the CA being displayed should agree with the access point you are trying to use. If the CA does not appear authentic, find another access point.

If you have any questions about use of wireless technology with Lucent assets, please contact us at wireless-security@security.lucent.com.

You Keep Lucent Secure.