



OFFICE OF THE DISTRICT ATTORNEY  
County of Lackawanna  
SCRANTON, PENNSYLVANIA

ANDREW J. JARBOLA, III  
DISTRICT ATTORNEY  
(570) 963-6717  
FAX (570) 941-8948

September 4, 2009

**As Students Head Back to School,  
District Attorney And Comcast Remind Them To  
Protect Home Wireless Networks**

**September 3, 2009 – (Scranton, PA)** – As college students arrive for the start of the new school year and secure the essentials for their living spaces, many will install wireless hardware to enjoy the convenience of in-home, any room wireless mobility. Unfortunately, many students are unaware their wireless networks extend beyond the walls of their dorm room or apartment and either forget or ignore some simple steps to deter unauthorized Internet access.

The practice of “piggybacking,” or using a wireless connection without permission, may seem harmless or even charitable, particularly on a college campus. However, open wireless networks can invite those looking to tap into sensitive personal information or engage in other illegal activity, leaving the unwitting subscriber potentially vulnerable and accountable. Illegal use of wireless Internet networks include the interception of private usernames, passwords and files, the spread of harmful malware, illicit materials and the distribution of threatening/abusive e-mails.

“College students, and quite frankly any person with a wireless network, should pay close attention to the simple tips recommended by the experts to make their networks safer and more secure,” said Lackawanna County District Attorney Andy Jarbola. “Expertise and sophistication are not limited to technicians and computer experts. ‘Piggybackers’ and ‘hackers’ are self-taught, savvy people that take advantage of the unsuspecting student or average person that does not use precautions to prevent access to their personal information. Play it safe and take advantage of these tips to reduce the odds of becoming a victim.”

“We want our customers to have the best and safest online experience,” said Jim Samaha, senior vice president for Comcast Cable’s Central PA Region. “The reality is ‘piggybackers’ are looking for unsecure wireless networks and are less likely to hack a network that is password protected and encrypted when unprotected ones are available.”

To help protect its customers, Comcast offers the McAfee® Security Suite for no additional charge to Comcast High-Speed Internet subscribers to help keep their computers safe, protected and virus-free.

**The United States Computer Emergency Readiness Team recommends the following tips to minimize the risks to your wireless network:**

**Change default passwords** - Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup. These default passwords are easily found online, so they don't provide any protection. Changing default passwords makes it harder for attackers to take control of the device. Consider using a password that combines both letters and symbols and is no less than eight characters long.

**Restrict access** - Only allow authorized users to access your network. Each piece of hardware connected to a network has a MAC (media access control) address. You can restrict or allow access to your network by filtering MAC addresses. Consult your user documentation to get specific information about enabling these features. There are also several technologies available that require wireless users to authenticate before accessing the network.

**Encrypt the data on your network** - WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) both encrypt information on wireless devices. However, WEP has a number of security issues that make it less effective than WPA, so you should specifically look for gear that supports encryption via WPA. Encrypting the data will help prevent anyone who might be able to access your network from viewing your data.

**Protect your SSID** - To avoid outsiders easily accessing your network, avoid publicizing your SSID. Consult your user documentation to see if you can change the default SSID to make it more difficult to guess.

**Install a firewall** - While it is a good security practice to install a firewall on your network, you should also install a firewall directly on your wireless devices (a host-based firewall). Attackers who can directly tap into your wireless network may be able to circumvent your network firewall—a host-based firewall will add a layer of protection to the data on your computer.

**Always install active and up-to-date anti-virus software** - You can reduce the damage attackers may be able to inflict on your network and wireless computer by installing anti-virus software and keeping your virus definitions up-to-date. Many of these programs also have additional features that may protect against or detect spyware and Trojan horses.

Comcast also offers a comprehensive Security Channel on its consumer portal, Comcast.net, available at [www.comcast.net/security](http://www.comcast.net/security). The Comcast Security Channel serves as an online resource to help customers protect themselves from spam, viruses and other online threats. In addition to the Security Channel, the Comcast toolbar is another resource that can be downloaded from [www.comcast.net](http://www.comcast.net) free of charge, which includes spyware detection and removal, pop-up blocker and anti-phishing software.

## **About Comcast**

Comcast Corporation (Nasdaq: CMCSA, CMCSK) ([www.comcast.com](http://www.comcast.com)) is one of the nation's leading providers of entertainment, information and communication products and services. With 23.9 million cable customers, 15.3 million high-speed Internet customers, and 7.0 million Comcast Digital Voice customers, Comcast is principally involved in the development, management and operation of cable systems and in the delivery of programming content.

Comcast's Eastern Division serves approximately 5.7 million residential and business customers across Delaware, Maryland, New Jersey, North Carolina, Ohio, Pennsylvania, Virginia, West Virginia and Washington, DC. The Eastern Division is based in Oaks, Pennsylvania and employs more than 20,000 people.

##

**Contact:** *Fred DeAndrea*, 609.217.7921; [fred\\_deandrea@cable.comcast.com](mailto:fred_deandrea@cable.comcast.com)