Securing Your Router

These simple steps will help keep your data safe.

BY MICHAEL L. BRODY, DPM

First: what is a router? A router is the device that accepts a signal from your internet provider and then distributes that signal to the computers in your home or office. There will be one port that your Internet service plugs into and many other ports that your computers and devices plug into. Figure 1 is an example of a wireless router.

Your Internet would plug into the yellow port and your computers would plug into the blue ports. When you unpack the router from the box and plug it in, you can use a web browser to visit the set-up page for the router. Typically, you will put an address such as 192.168.0.1 into a web browser but you should look at the manual for your router to see the setup page.

When you get to the setup page you will first see a login page where you need to enter a username and password. Initially the username and password are the factory defaults and may be Admin/Password. Once again, your manual will tell you what these are.

The first thing you need to do is log onto the router and ***change*** the password. The default usernames for most routers are Admin and the default password for most routers are Admin or Password, or just blank. The initial log-in page will show your router make and model. *Anybody* who can get to the setup page can also visit the instruction page for your router and find out the default username and password. If you do NOT change the default password, then anybody can break into your router and take over your network.

If your router is wireless, the next step is to

Continued on page 54

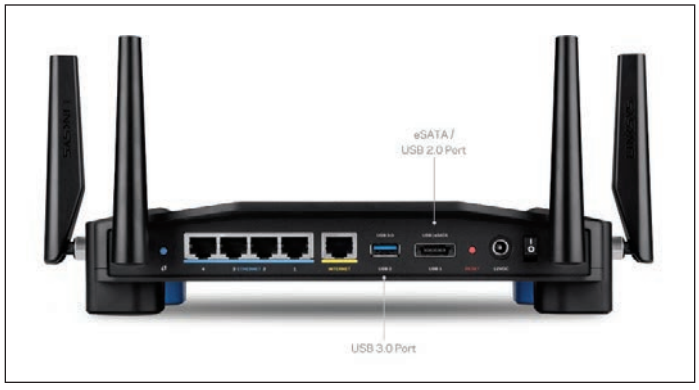

Figure 1: A typical wireless router

Router *(from page 53)*

set up wireless security. All routers sold today support WPA-2. You should select this level of security. When you choose this, you will need to create a "passphrase"--this is the code that any wireless device that wants to connect to your network will have to "know" in order to connect to the network.

The next step is to make sure that the firmware is up-to-date. When you log into the router, you will be able to look at the firmware version. Hopefully, there will be a button that allows you to "update" the firmware to the most recent version. This is vital in protecting the security of your router. If you cannot find this button, please refer to your manual and read the instructions on how to update the router firmware.

These recommendations should be followed for all routers in both your office and in your home to protect your computers from cyber threats.

The last thing to do for basic security set-up is to register your router with the manufacturer. Once you have registered your device, you will receive email updates when there are firmware updates to your device, which will allow you to maintain your router in the most secure manner.

Depending upon the router you purchase and the security features available, there may be more you can do to improve the security of your network. Read the manual and reach out to the manufacturer or your IT professional for recommendations on how to best set up security on your device. These recommendations should be followed for all routers in both your office and in your home to protect your computers from cyber threats. **PM**

Dr. Michael Brody has presented webinars for the e-Health initiative, (www.ehealthinitiative.org/) and is active in the EMR workgroup of the New York E Health Collaborative (www.nyehealth.org/). He has provided consulting services to physicians for the implementation of EHR software and to EHR vendors to assist in making their products more compatible with CCHIT and HIPAA guidelines. Dr. Brody is a member of AAPPM.