Cyber Security Issues for Insurance Agents – Securing Your Agency Wireless Router

With the continued usage of wireless technology, most independent agencies have incorporated wireless routers within their agency. Wireless routers allow computers to connect to the agency network to access information on the system and the internet. Potential hackers can have a field day with gaining access to your agency data if the router is not re-configured from the factory settings.

In this agency security briefing, we will focus on what agency owners need to know about their wireless routers and how to resolve potential threats to your network. Below are some suggested ideas for helping to secure your wireless router and your data.

1. First, change the default Service Set Identifier (SSID). Most vendors of wireless routers will have a standard SSID. If left unchanged, a knowledgeable hacker would find it easier to login to your network and gain access to your agency data. If the SSSID has not been changed, then most likely the SSID password has not been changed either.

   You can locate the instructions on how to change the SSID from the manufacture of the wireless router and you could also Google "how to change the SSID for my (insert vendor name)?". When changing the name DO NOT use the name of your agency or anything pertaining to insurance. If you use your agency name, this is like an advertisement to a hacker. Try using something non-descriptive, but something your team will know.

2. Change the admin username and password. Most wireless routers will come with a default username and password. Some of these default username passwords are available online, thus giving hackers easy access. When changing the admin username and password, make sure the password adheres to our previous discussion on passwords. (Make the password at least 8 to 12 characters with uppercase, lowercase, symbols, and numbers.)

3. Change router passwords at least every quarter and each time an employee leaves your agency.

4. Configure the WiFi protected access to WPA2+AES. Each router will have several different protection options. Among those are WPA2+AES and WEP. Using WEP is easier for hackers to gain access so you want to make the WiFi protected access to WPA2.

5. Disable Remote Management – This will prevent potential hackers from gaining access to your router on a wide area network. If you are using an outside IT firm, discuss this with them in case they need access. (Make sure you have a Business Associate Agreement with the Vendor. – Look for a future article on Business Associate Agreements.)

6. Make sure the router is in a secured and locked area to prevent tampering for unauthorized individuals.

These are just a few suggested ways to secure your wireless router and help prevent a potential hacker from gaining access to your valuable data. Let us know of other ideas you might have to secure your router. If you have any additional thoughts, please send your comments to ACT@iiaba.net.