**Name:** Coral S. Schmidt Montilla **ID:** 148830

**Objective:**

Upon completion of this activity, you will be able to identify and discuss the fundamental difference in wired vs wireless network security and identify and discuss the differences between WEP and WPA.

**Student Instructions:**

Please complete the assignment. This activity is worth 10 points. You will have 1 opportunity to complete the activity. Upload a document that includes your comparison between wired and wireless network security and identifies and discusses the differences between WEP and WPA standards.

When setting up or managing a network, understanding how it’s protected is just as important as how it's connected. Security risks exist in both wired and wireless setups, but how those risks show up, and how they’re handled, can look very different. Wireless networks especially require stronger encryption and more attention to authentication protocols because they operate in the open air, making them more exposed than wired networks. That’s where encryption standards like WEP and WPA come in, especially for home and business Wi-Fi networks.

Wired networks are generally considered more secure simply because someone needs physical access to plug them into. That limits a lot of outside threats by default. Wireless networks, however, broadcast signals over the air, which makes it easier to intercept if the proper security isn’t in place. This makes wireless networks more convenient but also more vulnerable without strong encryption, good password policies, and up-to-date configurations. In short, wired networks rely on physical security, while wireless ones rely more on software-based protection.

When it comes to securing wireless networks, encryption protocols matter. WEP (Wired Equivalent Privacy) was the original standard, but it had serious flaws—like using static keys that were easy to crack. WPA (Wi-Fi Protected Access) came next and improved security by rotating keys and using better encryption methods. WPA2 and WPA3 are now the current go-to options, offering much stronger protection through AES encryption and other upgrades. Today, WEP is considered outdated and should be avoided, while WPA2 or WPA3 should be the default for any wireless network.

In conclusion, both wired and wireless networks have their own security concerns, but wireless networks need more attention due to their open nature. Protocols like WPA were developed specifically to make wireless connections more secure, replacing weak standards like WEP. Choosing the right configuration and encryption standard can make a big difference in protecting data, no matter how the network is set up.

References: