

IT Fundamentals Guided Notes (ANSWER KEY)

Lesson 2.8.2 – Wireless Security

1. What is the SSID of a wireless network?

The SSID is the name the users see when attempting to connect to the wireless network

2. Why can it be a security threat to be super descriptive with an SSID?

This can tell malicious actors about the origin of the network and possibly give information about the target

3. Why is it important to change all default passwords for wireless networks?

Default passwords can be found in manuals, online, or just known by malicious actors and these are tried first when trying to break into a network

4. Why is it important to encrypt traffic on a network versus not encrypting the traffic?

Encrypting the traffic protects the users data from being viewed by anyone else on the network or monitoring the network

5. What is a captive portal?

A captive portal is used to authenticate a user on a network before giving them access to the network

6. What is a captive portal?

A captive portal is used to authenticate a user on a network before giving them access to the network

7. What are the three main ways of encrypting a wireless network?

WEP

WPA

WPA2

8. With WEP, WPA, and WPA2, which is the least secure encrypting method, and which is the most secure?

WEP is the least secure

WPA2 is the most secure