IT Fundamentals

Unit - Networking

Lesson 2.8.2 - Wireless Security

IT Fundamentals Objectives (FC0-U61)

Objective 2.8 - Given a scenario, install, configure and secure a basic wireless network.

- Best practices
  - Change SSID
  - Change default password
  - Encrypted vs. unenctrypted
    - Open
      - Captive portal
    - WEP
    - WPA
    - WPA2

Grade Level(s)

8, 9

Cyber Connections

- Networks & Internet

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

CYBER.ORG

Teacher Notes:

Wireless Security

Safe and Secure

Security is always an important part in any form of computing. This is no different when setting up a wireless network. One of the first things that should be done to improve security is to change the ***service set identifier*** (SSID). The SSID is the name that wireless users see when they browse available wireless networks. Some SSIDs may be a default name set by the manufacturer, but at the same time there is weakness in naming something along the lines of “Chase Bank, First Avenue” because everyone knows what it’s for (assuming the name is honest).

The next thing to change to increase security is the ***default password***. If a user maintains the default username and password, it may be easier for malicious users to configure settings within the network to their advantage. Once within the network, many malicious activities could be occuring.

Assuming the network is not designed to provide free Internet access to the public, encrypting the network will help ensure its safety and security. If the network is meant to be open to the public, it is still a smart idea to use a ***captive portal***. A captive portal is a webpage used to authenticate a user before providing network access, much like we would see at a Starbucks or McDonalds when accessing their free WiFi.

There are three main methods for encrypting a wireless network, ***wired equivalent privacy*** (WEP), ***wireless protected access*** (WPA), and ***wireless protected access 2*** (WPA2). WEP encryption uses 40-bit encryption to scramble data. Unfortunately, shortly after release, major flaws were found, showing WEP wasn’t secure. WPA was quickly released to address the weaknesses of WEP. WPA offers security enhancements such as encryption key integrity-checking and user authentication through ***Extensible Authentication Protocol*** (EAP). WPA2 is an enhanced version of WPA providing additional benefits over WPA such as using an improved encryption standard called ***Advanced Encryption Standard*** (AES).