

Data Security

Chapter 3 Network Security

LEARNING OBJECTIVES

1. Understand the term Network, and recognize the common network types.
 2. Understand the role of the network administrator, and the function of a firewall.
 3. Recognize different types of wireless security.
 4. Recognize good password policies, and identify common biometric security techniques.
-

WHAT IS A NETWORK?

A Network is formed where two or more computers are connected, so that they can share resources.

- Such as, printers, scanners, exchange files, or allow secure electronic communication.

PURPOSE OF A NETWORK?

- To **share** a single Internet connection.
 - To **access** the same hardware and software.
 - To **share** centralized backup devices.
-

NETWORK TYPES

Computer networks can be categorized by their size, and are mainly four types:

- LAN (Local Area Network)
 - PAN (Personal Area Network)
 - MAN (Metropolitan Area Network)
 - WAN (Wide Area Network)
-

NETWORKS

NETWORK ADMINISTRATOR

Is responsible for keeping an organization's computer network up-to-date and operating as intended.

OPTIONS FOR CONNETING TO A NETWORK

Computers in a network connect to each other either wirelessly or with cables.

FIREWALL

Is a device, hardware or software that guards “the gateway” access to a private network or computer, keeping unauthorized or unwanted network traffic out.

PROTECT ACCESS TO WIRELESS NETWORK

- ❑ If the network is not secure/ protected, i.e. it is an **open connection**, and people with computers and devices might be able to access.
 - ❑ When connecting to an unsecure network, be aware that **wireless eavesdroppers** (someone with the right tools) can see everything you do.
-

TYPES OF WIRELESS SECURITY/ WIRELESS PROTOCOLS

- ❑ Wired Equivalent Privacy (**WEP**)
 - ❑ Wi-Fi Protected Access (**WPA**) and Wi-Fi Protected Access II (**WPA2**)
 - ❑ Media Access Control (**MAC**)
-

ACCESS CONTROL

☐ **USERNAME AND PASSWORD**

Many computer systems or networks will require a user to **sign on** before using a system or network.

☐ **GOOD PASSWORD POLICIES**

- Create a password with adequate length.
 - Create a password with adequate character mix.
 - Do not share passwords.
 - Change password regularly.
 - Do not pick a password that is easy to guess.
 - Do not pick a password that can be found in a dictionary.
-

ACCESS CONTROL (Cont'd)

- Biometrics refers to the identification of humans by their characteristics or traits, such as:
 - **Fingerprint Scan.**
 - **Hand Geometry.**
 - **Retina Scan (Eye Scan).**
 - **Face Recognition.**
-