BACHILLERATO TÉCNICO
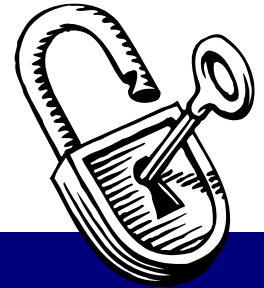Opción: Infraestructura Tecnológica y Servicios Informáticos

READING AND WRITING DOCUMENTS IN ENGLISH ON NETWORK AND COMPUTER SECURITY

SEGUNDO AÑO DE BACHILLERATO	
BTVITSI 2.6	
72 HRS	5 SEM
LECTURA Y ESCRITURA DE DOCUMENTOS EN INGLÉS SOBRE REDES Y SEGURIDAD INFORMÁTICA	

©2015 by Juan Zavaleta
www.teacherzavaleta.jimdo.com

Network Security

Tuesday November 3, 2015

Network Security

STEPS:

1. Copy this article on your notebook.

2. Underline technical vocabulary.

3. Read and analyze the article.

4. In groups of 4 students, prepare an explanation about the article.

5. Share your points of view to the class.

Network security consists of the policies adopted to prevent and monitorauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administratorUsers choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Network security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name —i.e., the password— this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g., a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' also used (e.g., a fingerprint or retinal scan).

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users.[1] Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network like wireshark traffic and may be logged for audit purposes and for later high-level analysis.

Communication between two hosts using a network may be encrypted to maintain privacy.