LO2 - ANSWER KEYS:

SELF CHECK 1:

Part I: Say True or False

1. _____
2. _____
3. _____
4. _____
5. _____

Part II: Matching Column A with the Column B

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

LO2 - ANSWER KEYS:

SELF CHECK 2:

1. Write at least five kinds of protection software available for a single use device
    - Avast
    - AVG
    - Avira
    - Bitdefender
    - BullGuard
2. **Antivirus software**
3. **False positives**
4. **False negatives**
5. **Anti-Virus**, **Anti-spyware**, and **Anti-spam** Applications.
6. The methods antivirus software can use to identify malware.
    - **Signature based detection** is the most common method. To identify viruses and other malware, antivirus software **compares the contents of a file to a dictionary of virus signatures**. Because viruses can embed themselves in existing files, the entire file is searched, not just as a whole, but also in pieces.
    - **Heuristic-based detection**, like malicious activity detection, can be used to identify unknown viruses.
    - **File emulation** is another heuristic approach. File emulation involves executing a program in a ***virtual environment*** and logging what actions the program performs. Depending on the actions logged, the antivirus software can determine if the program is malicious or not and then carry out the appropriate disinfection actions.
7. When selecting anti-virus software, there are other aspects to take into consideration such as:
    - The types of virus protected against
    - Yearly subscription fees
    - Other services available such as firewalls, SPAM management and system diagnostic software

LO2 - ANSWER KEYS:

SELF CHECK 3:

1. **A Firewall**
2. There are two ways to allow an application through a firewall. Both of them are risky:
    - Add an application to the list of allowed applications (less risky).
    - Open a port (more risky).
3. To help decrease your security risk:
    - Only allow an application or open a port when you really need to,
    - Never allow an application that you don't recognise to communicate through the firewall.
4. **The Windows Firewall page in Control Panel.**
5. **The Windows Firewall with Advanced Security (WFAS) console**

LO2 - ANSWER KEYS:

SELF CHECK 4:

1. **New security vulnerabilities**.
2. **Changing security risks**, **improve the reliability of Windows**, and **add support for new hardware**,
3. **Security threats**
4. Microsoft provides several techniques for applying updates:

    - **Directly from Microsoft**

      For home users and small businesses, Windows 7 is configured to retrieve updates directly from Microsoft automatically. This method is suitable only for smaller networks with fewer than 50 computers.

    - **Windows Server Update Services (WSUS)**

      WSUS enables administrators to approve updates before distributing them to computers on an intranet. If you want, updates can be stored and retrieved from a central location on the local network, reducing Internet usage when downloading updates. This approach requires at least one infrastructure server.

    - **Configuration Manager 2007**

      The preferred method for distributing software and updates in large, enterprise networks, Configuration Manager 2007 provides highly customizable, centralized control over update deployment, with the ability to audit and inventory client systems. Configuration Manager 2007 typically requires several infrastructure servers.

5. **Critical updates**
6. **Service packs**

LO2 - ANSWER KEYS:

SELF CHECK 5:

1. **Microsoft Internet Explorer**,
2. List and describe the four Internet Security Zones
    - **Internet zone**: By default, this zone contains anything that is not on your computer or an intranet, or assigned to any other zone. The default security level for the Internet zone is Medium.
    - **Local intranet zone**: This zone typically contains addresses that you have access to such as shared network drives, and local intranet sites.
    - **Trusted sites zone**: This zone contains sites that are considered trustworthy - sites where you can usually download or run files from without worrying about damage to your computer.
    - **Restricted sites zone**: This zone contains sites that are not trusted - that is, sites that you're not sure whether you can download or run files from without damage to your computer or data.
3. **Low**, **Medium Low**, **Medium**, and **High**