



# **INFORMATION TECHNOLOGY SUPPORT SERVICE**

**Level - I**

## **LEARNING GUIDE 33**

<b>Unit of Competence:</b>	<b>Protect Application or System Software</b>
<b>Module Title:</b>	<b>Protecting Application or System Software</b>
<b>LG Code:</b>	<b>ICT ITS1 M09 LO1 – LG33</b>
<b>TTLM Code:</b>	<b>ICT ITS1 TTLM 1019v1</b>

### **LO 1: Ensure User Accounts are Controlled**

**Instruction Sheet****Learning Guide 33**

This learning guide is developed to provide you the necessary information regarding the following content coverage and topics –

- User Account Control
- User Account Configuration
- Notifications Displayed at Logon
- Utilities Used to Check Strength of Passwords
- Accessing Information Services

This guide will also assist you to attain the learning outcome stated in the cover page. Specifically, upon completion of this Learning Guide, you will be able to –

- Modify default user settings to ensure that they conform to security policy
- Previously created user settings are modified to ensure they conform to updated security policy
- Ensure legal notices displayed at logon are appropriate
- Appropriate utilities are used to check strength of passwords and consider tightening rules for password complexity
- Emails are monitored to uncover breaches in compliance with legislation
- information services are accessed to identify security gaps and take appropriate action using hardware and software or patches

**Learning Instructions:**

1. Read the specific objectives of this Learning Guide.
2. Follow the instructions described below 3 to 6.
3. Read the information written in the information “Sheet 1, Sheet 2, Sheet 3 and Sheet 4” in page 3, 14, 20, 25 and 33 respectively.
4. Accomplish the “Self-Check 1, Self-Check 2, Self-Check 3, Self-Check 4 and Self-Check 5” in page 12, 18, 23, 30 and 37 respectively.
5. If you earned a satisfactory evaluation from the “Self-Check” proceed to “Operation Sheet 1, Operation Sheet 2 and Operation Sheet 3 ” in page 39
6. Do the “LAP test” in page 45



## 1.1. User Access

We do want our users to access the system; it's just that we want them to have the appropriate access. The control of user access can take many forms and apply at several levels. Once a computer is physically accessed, the user usually logs on to gain access to applications. These applications will access data in files and folders.

We can simplify the process down to 3 things.

- Physical access
- Authentication
- Authorisation

### 1.1.1. Physical Access

The first layer of management and security is the physical access to the computer. To prevent unauthorised access, a company may make use of:

- locks on the front doors
- locks on each floor
- locks on offices, etc
- security guards
- cameras
- keys on computer systems.

Only those who have permission and keys will be able to access a computer in the company's premises. The Internet, however, presents issues concerning access to corporate information or systems because physical restrictions cannot be imposed.

### 1.1.2. Authentication

Authentication is the process of verifying the identity of people who are attempting to access the network or system. Typically, a user identifies himself to the system, then is required to provide a second piece of information to prove their identity. This information is only known by the user or can only be produced by the user.

The most common method used to authenticate users is the ***Username and Password*** method. Using this method a user identifies itself with a username. They are then prompted for a password. The combination of name and password are then compared by the system to its data on configured users and if the combination matches the system's data the user is granted access.

Other authentication methods include:

- ***Username with static passwords*** - the password stays the same until changed by the user at some time



- **Username with dynamic passwords** - the password is constantly changed by a password generator synchronized with the user and system.
- **Other challenge response systems** - this may involve PINs, questions to the user requiring various answers or actions
- **Certificate Based** - this requires the user to have an electronic certificate or token. This may also need to be digitally signed by a trusted authority.
- **Physical devices** - these include the use of smartcards and biometrics. Generally the entire authentication process occurs on the local workstation, thus eliminating the need for a special server.

Whatever method is used is determined by the organisational policy and security requirements.

### 1.1.3. Authorisation

Once a user has been authenticated (that is their identity validated) they are granted access to the network or system. For the user to then access data or an application or execute some task or command they need be authorised to do so. The authorisation process determines what the user can do on the network. In other words it enforces the organisation policy as applicable to the user.

The Network and System administrators are responsible for the technical configuration of network operating systems, directory services and applications. Part of the configuration includes security settings that authorise user access. The administrators use an organisational policy to determine these settings.

## 1.2. User Account

A user account is a collection of information that tells Windows which *files and folders you can access, what changes you can make to the computer, and your personal preferences*, such as your desktop background or screen saver. User accounts let you share a computer with several people, while having your own files and settings. Each person accesses his or her user account with a username and password.

There are three types of accounts. Each type gives users a different level of control over the computer:

- **Standard Accounts** are for everyday computing.
- **Administrator Accounts** provide the most control over a computer, and should only be used when necessary.
- **Guest Accounts** are intended primarily for people who need temporary use of a computer.



### 1.2.1. Standard User Account

A standard user account lets you use most of the capabilities of the computer. You can use most programs that are installed on the computer and change settings that affect your user account. However, you can't install or uninstall some software and hardware, you can't delete files that are required for the computer to work, and you can't change settings that affect other users or the security of the computer. If you're using a standard account, you might be prompted for an administrator password before you can perform certain tasks.

Why use a Standard User Account instead of an Administrator Account?

The **standard account** can help protect your computer by preventing users from making changes that affect everyone who uses the computer, such as deleting files that are required for the computer to work. We recommend creating a standard account for each user.

When you are logged on to Windows with a standard account, you can do almost anything that you can do with an **administrator account**, but if you want to do something that affects other users of the computer, such as installing software or changing security settings, Windows might ask you to provide a password for an administrator account.

### 1.2.2. Administrator Account

An administrator account is a **user account** that lets you make changes that will affect other users. Administrators can change security settings, install software and hardware, and access all files on the computer. Administrators can also make changes to other user accounts.

When you set up Windows, you'll be required to create a user account. This account is an administrator account that allows you to set up your computer and install any programs that you would like to use. Once you have finished setting up your computer, we recommend that you use a **standard user account** for your day-to-day computing. It's more secure to use a standard user account instead of an administrator account because it can prevent a person from making changes that affect everyone who uses the computer.

### 1.2.3. Guest Account

A guest account allows people to have temporary access to your computer. People using the guest account can't install software or hardware, change settings, or create a password. You have to turn on the guest account before it can be used.



### 1.3. User Profiles

User profile is a collection of settings that make the computer look and work the way you want it to. It contains your settings for desktop backgrounds, screen savers, pointer preferences, sound settings, and other features. Your user profile ensures that your personal preferences are used whenever you log on to Windows.

A user profile is different from a user account, which you use to log on to Windows. Each user account has at least one user profile associated with it.



### 1.4. User Account Control

User Account Control (UAC) is a feature in Windows that can help you stay in control of your computer by informing you when a program makes a change that requires administrator-level permission. UAC works by adjusting the permission level of your user account. If you're doing tasks that can be done as a **standard user**, such as reading e-mail, listening to music, or creating documents, you have the permissions of a standard user—even if you're logged on as an administrator.



When changes are going to be made to your computer that requires administrator-level permission, UAC notifies you. If you are an administrator, you can click Yes to continue. If you are not an administrator, someone with an administrator account on the computer will have to enter their password for you to continue. If you give permission, you are temporarily given the rights of an administrator to complete the task and then your permissions are returned back to that of a standard user. This makes it so that even if you're using an administrator account, changes cannot be made to your computer without you knowing about it, which can help prevent **malicious software (malware)** and **spyware** from being installed on or making changes to your computer.

When your permission or password is needed to complete a task, UAC will notify you with one of four different types of dialog boxes.

**Table 1-1:** The different types of dialog boxes used to notify you and guidance on how to respond to them.

Icon	Type	Description
	A setting or feature that is part of Windows needs your permission to start.	This item has a <b>valid digital signature</b> that verifies that Microsoft is the publisher of this item. If you get this type of dialog box, it's usually safe to continue. If you are unsure, check the name of the program or function to decide if it's something you want to run.
	A program that is not part of Windows needs your permission to start.	This program has a valid digital signature, which helps to ensure that the program is what it claims to be and verifies the identity of the publisher of the program. If you get this type of dialog box, make sure the program is the one that you want to run and that you trust the publisher.



	A program with an unknown publisher needs your permission to start.	This program <b>doesn't have a valid digital signature</b> from its publisher. This doesn't necessarily indicate danger, as many older, legitimate programs lack signatures. However, you should use extra caution and only allow a program to run if you obtained it from a trusted source, such as the original CD or a publisher's website. If you are unsure, look up the name of the program on the Internet to determine if it is a known program or malicious software.
	You have been blocked by your <b>system administrator</b> from running this program.	This program has been <b>blocked</b> because it is known to be <b>untrusted</b> . To run this program, you need to contact your system administrator.

We recommend that you log on to your computer with a standard user account most of the time. You can browse the Internet, send e-mail, and use a word processor, all without an administrator account. When you want to perform an administrative task, such as installing a new program or changing a setting that will affect other users, you don't have to switch to an administrator account; Windows will prompt you for permission or an administrator password before performing the task. We also recommend that you create standard user accounts for all the people who use your computer.

In this version of Windows, you can adjust how often UAC notifies you when changes are made to your computer. If you want to be informed when any change is made to your computer, choose to always be notified.

#### 1.4.1. User Account Control settings

User Account Control (UAC) notifies you before changes are made to your computer that requires administrator-level permission. The default UAC setting notifies you when programs try to make changes to your computer, but you can control how often you are notified by UAC by adjusting the settings.





**Table 1-2:** The description of the UAC settings and the potential impact of each setting to the security of your computer.

Setting	Description	Security Impact
<b>Always Notify</b>	<ul style="list-style-type: none"> <li>You will be notified before programs make changes to your computer or to Windows settings that require the permissions of an administrator.</li> <li>When you're notified, your desktop will be dimmed, and you must either approve or deny the request in the UAC dialog box before you can do anything else on your computer. The dimming of your desktop is referred to as the secure desktop because other programs can't run while it's dimmed.</li> </ul>	<ul style="list-style-type: none"> <li>This is the most secure setting.</li> <li>When you are notified, you should carefully read the contents of each dialog box before allowing changes to be made to your computer.</li> </ul>
<b>Notify me only when programs try to make changes to my computer</b>	<ul style="list-style-type: none"> <li>You will be notified before programs make changes to your computer that requires the permissions of an administrator.</li> <li>You will not be notified if you try to make changes to Windows settings that require the permissions of an administrator.</li> <li>You will be notified if a program outside of Windows tries to make changes to a Windows setting.</li> </ul>	<ul style="list-style-type: none"> <li>It's usually safe to allow changes to be made to Windows settings without you being notified. However, certain programs that come with Windows can have commands or data passed to them, and malicious software can take advantage of this by using these programs to install files or change settings on your computer. You should always be careful about which programs you allow to run on your computer.</li> </ul>
<b>Notify me only when programs try to make changes to my computer (do not dim my desktop)</b>	<ul style="list-style-type: none"> <li>You will be notified before programs make changes to your computer that requires the permissions of an administrator.</li> <li>You will not be notified if you try to make changes to Windows settings that require the permissions of an administrator.</li> <li>You will be notified if a program outside of Windows tries to make changes to a Windows setting.</li> </ul>	<ul style="list-style-type: none"> <li>This setting is the same as "Notify only when programs try to make changes to my computer," but you are not notified on the secure desktop.</li> <li>Because the UAC dialog box isn't on the secure desktop with this setting, other programs might be able to interfere with the dialog's visual appearance. This is a small security risk if you already have a malicious program running on your computer.</li> </ul>





<p style="text-align: center;"><b>Never Notify</b></p>	<ul style="list-style-type: none"> <li>• You will not be notified before any changes are made to your computer. If you are logged on as an administrator, programs can make changes to your computer without you knowing about it.</li> <li>• If you are logged on as a standard user, any changes that require the permissions of an administrator will automatically be denied.</li> <li>• If you select this setting, you will need to restart the computer to complete the process of turning off UAC. Once UAC is off, people that log on as administrator will always have the permissions of an administrator.</li> </ul>	<ul style="list-style-type: none"> <li>• This is the least secure setting. When you set UAC to never notify, you open up your computer to potential security risks.</li> <li>• If you set UAC to never notify, you should be careful about which programs you run, because they will have the same access to the computer as you do. This includes reading and making changes to protected system areas, your personal data, saved files, and anything else stored on the computer. Programs will also be able to communicate and transfer information to and from anything your computer connects with, including the Internet.</li> </ul>
--	--	---

#### 1.4.2. Why is User Account Control necessary?

The most important rule for controlling access to resources is to provide the least amount of access privileges required for users to perform their daily tasks. Many tasks do not require administrator privileges. However, because previous versions of Windows created all user accounts as administrators by default, users logged on to their computers with an administrator account. Without User Account Control (UAC), when a user is logged on as an administrator, that user is automatically granted full access to all system resources.

However, most users do not require such a high level of access to the computer. Often users are unaware that they are logged on as an administrator when they browse the Web, check e-mail, and run software. While logging on with an administrator account enables a user to install legitimate software, the user can also unintentionally or intentionally install a malicious program. A malicious program installed by an administrator can fully compromise the computer and affect all users.

With the introduction of UAC, the access control model changed to help mitigate the impact of a malicious program. When a user attempts to start an administrator application, the User Account Control dialog box asks the user to click Yes or No before the user's full administrator access token can be used. If the user is not an administrator, the user must provide an administrator's credentials to run the program.

Because UAC requires an administrator to approve application installations, unauthorized applications cannot be installed automatically or without the explicit consent of an administrator.



### 1.4.3. How UAC Work

There are two levels of users: standard users and administrators. Standard users are members of the Users group and administrators are members of the Administrators group on the computer.

Both standard users and administrators access resources and run applications in the security context of standard users by default. When a user logs on to a computer, the system creates an access token for the user. This access token contains information about the level of access that the user is granted, including specific **Security Identifiers** (SIDs) and **Windows privileges**. When an administrator logs on, two separate access tokens are created for the user: a standard user access token and an administrator access token. The standard user access token contains the same user-specific information as the administrator access token, but the administrative Windows privileges and SIDs are removed. The standard user access token can start standard user applications but cannot start applications that perform administrative tasks.

When the user needs to run applications that perform administrative tasks (administrator applications), the user is prompted to change or elevate the security context from a standard user to an administrator. This default user experience is called **Admin Approval Mode**. In this mode, applications require specific permission to run as an administrator application.



Self-Check – 1	Written Test
----------------	--------------

**Directions:** Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. \_\_\_\_\_ is a collection of information that tells Windows which files and folders you can access, what changes you can make to the computer, and your personal preferences, such as desktop background or screen saver. **(1 pts)**
2. \_\_\_\_\_ lets you use most of the capabilities of the computer. You can use most programs that are installed on the computer and change settings that affect your user account. **(1 pts)**
3. \_\_\_\_\_ is a user account that lets you make changes that will affect other users change security settings, install software and hardware, and access all files on the computer. **(1 pts)**
4. \_\_\_\_\_ allows people to have temporary access to your computer. **(1 pts)**
5. \_\_\_\_\_ is a collection of settings that make the computer look and work the way you want it to. **(1 pts)**
6. \_\_\_\_\_ is the process of verifying the identity of people who are attempting to access the network or system. **(1 pts)**
7. \_\_\_\_\_ determines what the user can do on the network. In other words it enforces the organization policy as applicable to the user. **(1 pts)**
8. The most common method used to authenticate users is \_\_\_\_\_
9. Why use a Standard User Account instead of an Administrator Account? **(2 pts)**

---

---

---

---

10. List and describe authentication methods used to authenticate users. **(4 pts)**

---

---

---

---

---



11. \_\_\_\_\_ is a feature in Windows that can help you stay in control of your computer by informing you when a program makes a change that requires administrator-level permission. **(1 pts)**
12. List the four different types of dialog boxes that UAC will notify you when your permission or password is needed to complete a task. **(4 pts)**
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
13. List the UAC settings and the potential impact of each setting to the security of your computer. **(4 pts)**
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
14. When a user logs on to a computer, the system creates an access token for the user. This access token contains information about the level of access that the user is granted, including specific \_\_\_\_\_ and \_\_\_\_\_. **(2 pts)**
15. When the user needs to run applications that perform administrative tasks (administrator applications), the user is prompted to change or elevate the security context from a standard user to an administrator. This default user experience is called \_\_\_\_\_. **(1 pts)**

**Note: Satisfactory rating - 13 points**

**Unsatisfactory - below 13 points**

You can ask your teacher for the copy of the correct answers.



## Answer Sheet

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

Name: \_\_\_\_\_

Date: \_\_\_\_\_

### Short Answer Questions

1. \_\_\_\_\_

2. \_\_\_\_\_

3. \_\_\_\_\_

4. \_\_\_\_\_

5. \_\_\_\_\_

6. \_\_\_\_\_

7. \_\_\_\_\_

8. \_\_\_\_\_

9. \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

10. \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

11. \_\_\_\_\_

12. \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

13. \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

14. \_\_\_\_\_ and \_\_\_\_\_

15. \_\_\_\_\_



## 2.1. User Account Configuration

Network and System Administrators are responsible for configuring user accounts. Network operating systems and applications have many security options and setting relating to user access. How does an administrator determine the configuration and setting for user accounts?

Organisation policies and procedures provide the guidelines for administrators.

### 2.1.1. User Account Settings

The organisation's policies should make statements as to the degree of user control that is required. Network procedures should contain details as to how these policies may be implemented. For example, the policy may state that user passwords should not be less than six characters. The procedures will then describe how the administrator should configure the operating system to ensure that all passwords are at least six characters.

The administrator should review the policies to ensure that the procedures produce the desired outcomes. The procedures should describe in detail how to make use of the operating system facilities to configure user accounts in accordance with the security requirements.

The actual way you set these parameters will vary with each operating environment, however, here are some basic parameters covered by most operating systems to consider when setting up user account options:

- **Password requirements** - whether a password is required, minimum length, complexity, needs to be changed at intervals, etc
- **Account lock out settings** - disabling accounts that have made a number of bad logon attempts
- **Access hours** - the standard days and time that users will be permitted to access the network
- **Account expiry dates** - date when account will be disabled
- **Logon restrictions** - accounts can only be used at specified locations or workstations.
- **Home directory information** - a home directory is a folder that usually has the name of the user and the user has full permissions over.
- **Logon scripts** - these perform specific tasks or run specific programs when the user logs on

### 2.1.2. Configuring User Access

Once user account settings have been determined how do we know who should have accounts and what access should be set?



### 2.1.2.1. User Authorisations

Once again, organisational policy and procedures provide the necessary information for the administrators. There should be procedures in place that inform the appropriate people that a person requires a new user account or changes to an existing account or a deletion of accounts. The notification procedure should cover circumstances such as new employees joining the organisation, employees changing positions in the organisation and employees leaving the organisation. These notifications must come from authorised people in the organisation (managers, etc) as stated in the policy and procedures.

Notifications also need to specify what information, data, resources etc the account is permitted to access. The request for access must be authorised by an appropriate person in the organisation (usually department managers). The access permissions for users should be carefully planned and determined in writing by appropriate people who have the authority to allocate the access. Procedures should address:

- Which managers can authorise a new user
- Standards for user id and passwords
- Groups that users can belong to and authority required for each group
- Basic accesses that all users are allowed
- Authorisation requirements to access sensitive data
- Application accesses
- Ability to install additional software
- Email and internet accesses
- Special accesses that may be required.

### 2.1.2.2. Use of Groups

The most common way of administering access permissions is to create **groups** and put user accounts into appropriate groups. The group is then permitted or denied access as required. Using groups is an efficient way of managing authorisation because you only need to set access permission to a group and not individual accounts.

For example, a company may have thousands of users, but analysis of what those users want to do may show that there are twenty or more different combinations of access permissions required. By assigning users to groups and then allocating permissions to the group, the security administration is greatly simplified.

Once we have users allocated to groups we can explore other levels of controlling access. Allocating permissions to folders and files is a major security provision of network operating systems and one that is important





to set up correctly. Can we go lower and look at the content of a specific file and restrict access there?

The restriction of file access is most applicable in controlling access to database files.

For example, imagine a Payroll system using a database in which the data is stored in tables. These tables have columns and rows of data. Let us think about two groups of user, the payroll department staff and the manager of a department. The payroll group are likely to be allowed full access to all the data although in a very large organisation there may be segregation of access.

But what about a department manager? This person may be allowed to see salary details for the staff that work in the department only.

In the table containing salary details there may be a row for every employee in the organisation. This means that we only want to show this manager the rows that relate to the one department. This would be secured with a filter that only displays staff in the department being examined.

Furthermore there may be information about an employee that even their manager may not be able to see, such as medical or financial information. This information may be restricted by controlling the columns returned in a report or query.

This type of security is really part of the application control rather than the network but it is still an important part of the overall security of the system and needs to be addressed by the organisational procedures.

### **2.1.2.3. Permissions and Rights**

Permissions generally refer to file and directory access. The user account or group can be set with the following type of permissions:

- No access at all to files and directories
- Read only.
- Modify where the contents of files and directories may be accessed but changed or added to but not deleted
- Full Control or Supervisory where files and directories can be view modified and deleted.

Rights (or privileges) generally refer to the restriction on user accounts or group in performing some task or activity. For example a user account or group may be assigned administrator or supervisor rights meaning that the user can perform administration tasks like create, modify or delete user accounts. Care must be taken with rights to ensure security is not compromised.



## 2.2. Managing User Accounts

Once user accounts are configured we still need to manage the accounts as required by organisational policy. For example user accounts for contractors are active only for as long as the contractor are physically on site. This means that accounts need to be enabled and disabled. This activity should be addressed by procedures.

Note also that many networks on different OS's allow 'guest' and 'temporary' accounts. These are usually set up for either read-only or short-term access to people who would not normally have access to the system. Great care must be taken in configuring or using these accounts firstly because they can allow anonymous and uncontrolled use of a system and secondly guest passwords can sometimes be guessed easily and provide a doorway for hackers/crackers.

Administrators need to review procedures to ensure that they remain current and address any changes to the organisation and the network.

Administrators need to be aware of user activities and practices when accessing the network. Organisational policy and procedures should address how users should access the network. In time users may develop shortcuts and practices that knowingly or unknowingly are in breach of policy and may compromise network security. For example a user may log on to the network on one workstation. Then to allow access for a colleague who has forgotten their password the users logs in on another workstation for the colleague. The result is two concurrently network connections for one user account but for two different people who have different user access requirements.

To manage user accounts appropriately administrators should

- Regularly review organisational policies and procedures to be aware of requirements and address any organisational or network changes
- Conduct regular checks to ensure the change management procedures are working for new, changed and deleted users
- Review and investigate current work practices regarding user network access
- Conduct information and training sessions for network users to reinforce appropriate practices and organisational policy
- Conduct regular audits of network access—verifying current users and deleting expired accounts

Managing user accounts can be a complex and tedious task but we can make things easier by ensuring appropriate policy and procedures are in place.



Self-Check – 2	Written Test
----------------	--------------

**Directions:** Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. \_\_\_\_\_ should make statements as to the degree of user control that is required. **(1 pts)**
2. \_\_\_\_\_ need to review procedures to ensure that they remain current and address any changes to the organisation and the network. **(1 pts)**
3. List and describe some basic parameters covered by most operating systems to consider when setting up user account options: **(6 pts)**
4. The most common way of administering \_\_\_\_\_ is to create groups and put user accounts into appropriate groups. **(1 pts)**
5. \_\_\_\_\_ generally refer to file and directory access. **(1 pts)**
6. List type of permissions the user account or group can be set with: **(4 pts)**
7. \_\_\_\_\_ generally refer to the restriction on user accounts or group in performing some task or activity. **(1 pts)**
8. List what administrators should do to manage user accounts appropriately. **(4 pts)**
9. Managing user accounts can be a complex and tedious task but we can make things easier by ensuring appropriate \_\_\_\_\_ are in place. **(1 pts)**

**Note: Satisfactory rating - 11 points**

**Unsatisfactory - below 11 points**

You can ask your teacher for the copy of the correct answers.



## Answer Sheet

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

Name: \_\_\_\_\_

Date: \_\_\_\_\_

### Short Answer Questions

1. \_\_\_\_\_

2. \_\_\_\_\_

3. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

4. \_\_\_\_\_

5. \_\_\_\_\_

6. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

7. \_\_\_\_\_

8. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

9. \_\_\_\_\_



### **3.1. Identifying Logon Restrictions**

Often, authentication problems occur because administrators have configured logon restrictions to enforce the organization's security requirements. Logon restrictions include locking accounts after several incorrect attempts at typing a password, allowing users to log on only during specific hours, requiring users to change their passwords regularly, disabling accounts, and accounts that expire on a specific date. The sections that follow describe each of these types of logon restrictions.

#### **3.1.1. Account Lockout**

If a user provides incorrect credentials several times in a row (for example, if an attacker is attempting to guess a user's password, or if a user repeatedly mistypes a password), Windows can block all authentication attempts for a specific amount of time.

Account lockout settings are defined by Group Policy settings in the Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policies\ node as follows:

- The number of incorrect attempts is defined by the Account Lockout Threshold setting.
- The time that the number of attempts must occur within is defined by the Reset Account Lockout Counter After policy.
- The time that the account is locked out is defined by the Account Lockout Duration policy.

If a user receives an error message indicating that her account is locked out or she cannot log in even if she thinks she has typed her password correctly, you should validate the user's identity and then unlock the user's account. To unlock a user's account, view the user's Properties dialog box, and clear the Account Is Locked Out check box (for local Windows 7 user accounts) Then, click Apply.

#### **3.1.2. Logon Hour Restrictions**

Administrators can also use the Account tab of an AD DS user's properties to restrict logon hours. This is useful when administrators do not want a user to log on outside his normal working hours.

If a user attempts to log on outside his allowed hours, Windows 7 displays the error message *"Your account has time restrictions that prevent you from logging on at this time. Please try again later."* The only way to resolve this problem is to adjust the user's logon hours by clicking the Logon Hours button on the Account tab of the user's Properties dialog box.



### 3.1.3. Password Expiration

Most security experts agree that users should be required to change their passwords regularly. Changing user passwords accomplishes two things:

- If attackers are attempting to guess a password, it forces them to restart their efforts. If users never change their passwords, attackers would be able to guess them eventually.
- If an attacker has guessed a user's password, changing the password prevents the attacker from using these credentials in the future.

Password expiration settings are defined by Group Policy settings in the Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy node as follows:

- The time before a password expires is defined by the Maximum Password Age policy.
- The number of different passwords that users must have before they can reuse a password is defined by the Enforce Password History policy.
- The time before users can change their password again is defined by the Minimum Password Age policy. When combined with the Enforce Password History policy, this can prevent users from changing their password back to a previous password.

If users attempt to log on interactively to a computer and their password has expired, Windows prompts them to change their password automatically. If users attempt to access a shared folder, printer, Web site, or other resource using an expired password, they will simply be denied access. Therefore, if a user calls and complains that she cannot connect to a resource, you should verify that the user's password has not expired. You can prevent specific accounts from expiring by selecting the Password Never Expires check box on the Account tab of the user's Properties dialog box.

### 3.1.4. Disabled Account

Administrators can disable user accounts to prevent a user from logging on. This is useful if a user is going on vacation and you know she won't be logging on for a period of time, or if a user's account is compromised and IT needs the user to contact them before logging on.

To enable a user's disabled account, clear the Account Is Disabled check box in the user's Properties dialog box.



### **3.1.5. Account Expiration**

In AD DS domains, accounts can be configured to expire. This is useful for users who will be working with an organization for only a limited amount of time. For example, if a contract employee has a two-week contract, domain administrators might set an account expiration date of two weeks in the future.

To resolve an expired account, edit the account's properties, select the Account tab, and set the Account Expires value to a date in the future. If the account should never expire, you can set the value to Never.

## **3.2. Determining Logon Context**

Users can authenticate to the local user database or an AD DS domain. Logon restrictions defined for the domain only apply to domain accounts, and vice versa. Therefore, when examining logon restrictions for users, you must determine their logon context.

The quickest way to do this is to open a command prompt and run the command set to display all environment variables. Then, look for the USERDOMAIN line. If the user logged on with a local user account, this will be the computer name (shown on the COMPUTERNAME line). If the user logged on with an AD DS user account, this will be the name of the domain. You can also check the LOGONSERVER line to determine whether a domain controller or the local computer authenticated the user.





Self-Check – 3	Written Test
----------------	--------------

**Directions:** Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. Authentication problems occur because administrators have configured logon restrictions to enforce the organization's \_\_\_\_\_. **(1 pts)**
2. If a user provides \_\_\_\_\_ several times in a row (for e.g., if a user repeatedly mistypes a password), Windows can block all authentication attempts for a specific amount of time. **(1 pts)**
3. If a user attempts to log on outside his allowed hours, Windows 7 displays the error message\_\_\_\_\_. **(2 pts)**
4. Write the two things that changing user passwords accomplishes: **(2 pts)**  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
5. If users attempt to log on interactively to a computer and their password has expired Windows prompts them to \_\_\_\_\_. **(1 pts)**
6. Administrators can \_\_\_\_\_ to prevent a user from logging on. **(1 pts)**

**Note: Satisfactory rating - 5 points**

**Unsatisfactory - below 5 points**

You can ask your teacher for the copy of the correct answers.



## Answer Sheet

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

Name: \_\_\_\_\_

Date: \_\_\_\_\_

### Short Answer Questions

1. \_\_\_\_\_

2. \_\_\_\_\_

3. \_\_\_\_\_  
\_\_\_\_\_

4. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

5. \_\_\_\_\_

6. \_\_\_\_\_



## 4.1. Definitions of a Password

A *password* is a string of characters that people can use *to log on to a computer* and access files, programs, and other resources. Passwords help ensure that people *do not access the computer* unless they have been *authorized* to do so. In Windows, a password can include *letters, numbers, symbols, and spaces*. Windows passwords are also *case-sensitive*. To help keep your computer *secure*, you should always create a *strong password*.

To help keep the information on *your computer secure*, you should *not give out your password* or *write it in a place where others can see it*.

### 4.1.1. STRONG PASSWORDS AND PASSPHRASES

A *password* is a string of characters used to access information or a computer. *Passphrases* are typically longer than passwords, for added security, and contain *multiple words* that create a phrase. Passwords and passphrases help prevent unauthorized people from accessing files, programs, and other resources. When you create a password or passphrase, you should make it strong, which means it's difficult to guess or crack. It's a good idea to use strong passwords on all user accounts on your computer. If you're using a workplace network, your network administrator might require you to use a strong password.

#### Tables 4-1 make a password or passphrase strong

A strong password:	A strong passphrase:
<ul style="list-style-type: none"><li>• Is at least eight characters long.</li><li>• Does not contain your user name, real name, or company name.</li><li>• Does not contain a complete word.</li><li>• Is significantly different from previous passwords.</li></ul>	<ul style="list-style-type: none"><li>• Is 20 to 30 characters long.</li><li>• Is a series of words that create a phrase.</li><li>• Does not contain common phrases found in literature or music.</li><li>• Does not contain words found in the dictionary.</li><li>• Does not contain your user name, real name, or company name.</li><li>• Is different from previous passphrases.</li></ul>

#### Tables 4-1 four categories characters Strong passwords and passphrases contain:

Character category	Examples
Uppercase letters	A, B, C
Lowercase letters	a, b, c
Numbers	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symbols found on the keyboard (all keyboard characters not defined as letters or numerals) and spaces	' ~ ! @ # \$ % ^ & * ( ) _ - + = { } [ ] \   : ; " ' < > , . ? /



A password or passphrase might meet all the criteria above and still be weak. For example, Hello2U! meets all the criteria for a strong password listed above, but is still weak because it contains a complete word. H3ll0 2 U! is a stronger alternative because it replaces some of the letters in the complete word with numbers and also includes spaces.

Help yourself remember your strong password or passphrase by following these tips:

- Create an acronym from an easy-to-remember piece of information. For example, pick a phrase that is meaningful to you, such as My son's birthday is 12 December, 2004. Using that phrase as your guide, you might use Msbi12/Dec,4 for your password.
- Substitute numbers, symbols, and misspellings for letters or words in an easy-to-remember phrase. For example, My son's birthday is 12 December, 2004 could become Mi\$un's Brthd8iz 12124, which would make a good passphrase.
- Relate your password or passphrase to a favorite hobby or sport. For example, I love to play badminton could become ILuv2PlayB@dm1nt()n.

If you feel you must write down your password or passphrase to remember it, make sure you don't label it as such, and keep it in a safe place.

Windows passwords can be much longer than the eight characters recommended above. In fact, you can make a password up to 127 characters long. However, if you are on a network that also has computers running Windows 95 or Windows 98, consider using a password that is no longer than 14 characters. If your password is longer than 14 characters, you might not be able to log on to your network from computers running those operating systems.

## 4.2. Modify User Security Policy

### 4.2.1. Password policy

A **password policy** is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. A password policy is often part of an organization's official regulations and may be taught as part of security awareness training. The password policy may either be advisory or mandated by technical means. Some governments have national authentication frameworks that define requirements for user authentication to government services, including requirements for passwords.

Some policies suggest or impose requirements on what type of password a user can choose, such as:

- the use of both upper- and lower-case letters (case sensitivity)
- inclusion of one or more numerical digits
- Inclusion of special characters, e.g. @, #, \$ etc.



- prohibition of words found in a dictionary or the user's personal information
- prohibition of passwords that match the format of calendar dates, license plate numbers, telephone numbers, or other common numbers
- prohibition of use of company name or an abbreviation
- An Environ password, of the following form: consonant, vowel, consonant, consonant, vowel, consonant, number, number (for example *pinray45*). A disadvantage of this 8-character password is known to potential attackers, the number of possibilities that need to be tested is less than a 6-character password of no form (486,202,500 vs 2,176,782,336).

#### 4.2.2. Common Password Practice

Password policies often include advice on proper password management such as:

- never share a computer account
- never use the same password for more than one account
- never tell a password to anyone, including people who claim to be from customer service or security
- never write down a password
- never communicate a password by telephone, e-mail or instant messaging
- being careful to log off before leaving a computer unattended
- changing passwords whenever there is suspicion they may have been compromised
- operating system password and application passwords are different
- password should be alpha-numeric

#### 4.2.3. Types of Password

Before you will be able to change, clear or remove a computer password, you must first determine the password type that is being used.

- **System Password:** - Does the password appear as the computer is booting? If yes, this is a BIOS or CMOS password. BIOS or CMOS passwords will not allow the computer to be boot at all unless the password is known.
- **Operating System /Network/ Third-Party Password:** - Does the password appear after the computer is done booting and before the operating system runs? If yes, this is a network, Operating System, or third-party password.
- **Window Password:** - Windows users, does the password appear in Windows before the desktop? If yes, this is a Windows or Windows network password. If you are able to press the Escape key and get to Windows, you have a standard Windows password; however, if this does not bypass the password prompt, it is likely you have a Windows network password.



#### **4.2.4. Enforce Password History in Group Policy Editor**

Computer administrators can use the Group Policy Editor to deploy all types of general policy settings. When the "Enforce password history" policy setting is enabled, Windows keeps a record of a specified number of prior user account passwords. When users change their account password, they are prohibited from re-using any of the passwords still in the Windows memory. This policy helps to enhance computer security. By default, the "Enforce password history" policy is set to "0," which means no prior passwords are remembered. To enable the "Enforce password history" policy, the setting has to be a value greater than 0.

#### **4.2.5. Assign Minimum and Maximum Password Age**

##### **4.2.5.1. Minimum Password Age**

The minimum password age must be less than the Maximum password age, unless the maximum password age is set to 0, indicating that passwords will never expire. If the maximum password age is set to 0, the minimum password age can be set to any value between 0 and 998.

Configure the minimum password age to be more than 0 if you want Enforce password history to be effective. Without a minimum password age, users can cycle through passwords repeatedly until they get to an old favorite. The default setting does not follow this recommendation, so that an administrator can specify a password for a user and then require the user to change the administrator-defined password when the user logs on. If the password history is set to 0, the user does not have to choose a new password. For this reason, Enforce password history is set to 1 by default.

##### **4.2.5.2. Maximum Password Age**

This security setting determines the period of time (in days) that a password can be used before the system requires the user to change it. You can set passwords to expire after a number of days between 1 and 999, or you can specify that passwords never expire by setting the number of days to 0. If the maximum password age is between 1 and 999 days, the Minimum password age must be less than the maximum password age. If the maximum password age is set to 0, the minimum password age can be any value between 0 and 998 days.

##### **Note**

- It is a security best practice to have passwords expires every 30 to 90 days, depending on your environment. This way, an attacker has a limited amount of time in which to crack a user's password and have access to your network resources



### 4.3. Password Complexity Requirements

This security setting determines whether passwords must meet complexity requirements. Complexity requirements are enforced when passwords are changed or created.

If this policy is enabled, passwords must meet the following minimum requirements when they are changed or created:

- Passwords must not contain the user's entire same account Name (Account Name) value or entire display Name (Full Name) value. Both checks are not case sensitive:
  - ✓ The same account Name is checked in its entirety only to determine whether it is part of the password. If the same account Name is less than three characters long, this check is skipped.
- The display Name is parsed for delimiters: commas, periods, dashes or hyphens, underscores, spaces, pound signs, and tabs. If any of these delimiters are found, the display Name is split and all parsed sections (tokens) are confirmed not to be included in the password.
- Passwords must contain characters from three of the following five categories:
  - ✓ Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
  - ✓ Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
  - ✓ Base 10 digits (0 through 9)
  - ✓ None alphanumeric characters: ~! @#\$%^&\* \_-+= '\(){}[]:;'"<>.,?/
  - ✓ Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.



<b>Self-Check - 4</b>	<b>Written Test</b>
-----------------------	---------------------

**Directions:** Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. \_\_\_\_\_ is a string of characters that people can use *to log on to a computer* and access files, programs, and other resources. **(1 pts)**
2. In Windows, a password can include \_\_\_\_\_, \_\_\_\_\_, \_\_\_\_\_, and \_\_\_\_\_. **(4 pts)**
3. To help keep your computer *secure*, you should always create a \_\_\_\_\_. **(1 pts)**
4. \_\_\_\_\_ are typically longer than passwords, for added security, and contain *multiple words* that create a phrase. **(1 pts)**
5. When you create a password or passphrase, you should make it strong, which means \_\_\_\_\_. **(2 pts)**
6. Compare a strong password and a strong passphrase. **(3 pts)**

A strong password:	A strong passphrase:

7. Write the four categories of characters Strong passwords and passphrases contain: **(4 pts)**

---

---

---

8. \_\_\_\_\_ is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. (1 pts)



9. Write at least five advices on proper password management included in password policies. **(5 pts)**

---

---

---

---

---

10. Configure the \_\_\_\_\_ to be more than 0 if you want Enforce password history to be effective. **(1 pts)**
11. \_\_\_\_\_ security setting determines the period of time (in days) a password can be used before the system requires the user to change it. **(1 pts)**
12. \_\_\_\_\_ security setting determines whether passwords must meet complexity requirements. **(1 pts)**

**Note: Satisfactory rating - 13 points**

**Unsatisfactory - below 13 points**

You can ask your teacher for the copy of the correct answers.





## 5.1. Identify Security Gaps

### 5.1.1. Authenticating Users

Before a user can log on to a computer running Windows, connect to a shared folder, or browse a protected Web site, the resource must validate the user's identity using a process known as *authentication*.

Windows supports a variety of authentication techniques, including

- the traditional user name and password,
- smart cards, and
- third-party authentication components.

In addition, Windows can authenticate users with the local user database.

*Authentication* is the process of identifying a user. In home environments, authentication is often as simple as clicking a user name at the Windows 7 logon screen. However, in enterprise environments, almost all authentication requests require users to provide both a user name (to identify themselves) and a password (to prove that they really are the user they claim to be).

#### 5.1.1.1. Smart Card

Windows 7 also supports authentication using a smart card. The smart card, which is about the size of a credit card, contains a chip with a certificate that uniquely identifies the user. So long as a user doesn't give the smart card to someone else, inserting the smart card into a computer sufficiently proves the user's identity. Typically, users also need to type a password or PIN to prove that they aren't using someone else's smart card. When you combine two forms of authentication (such as both typing a password and providing a smart card), it's called ***multifactor authentication***. Multifactor authentication is much more secure than single-factor authentication.

#### 5.1.1.2. Biometrics

Biometrics is another popular form of authentication. Although a password proves your identity by testing "something you know" and a smart card tests "something you have," biometrics test "something you are" by examining a unique feature of your physiology. Today the most common biometric authentication mechanisms are fingerprint readers (now built into many mobile computers) and retinal scanners.

Biometrics is the most secure and reliable authentication method because you cannot lose or forget your authentication. However, it's also the least commonly used. Reliable biometric readers are too expensive for many organizations, and some users dislike biometric readers because they feel the devices violate their privacy.



### 5.1.2. Troubleshoot Authentication Issues

Sometimes, users might experience problems authenticating to resources that have more complex causes than mistyping a password or leaving the Caps Lock key on. The sections that follow describe troubleshooting techniques that can help you better isolate authentication problems.

#### ***UAC Compatibility Problems***

Users often confuse authentication and authorization issues. This isn't a surprise because both types of problems can show the exact same error message: "Access is denied." Because UAC limits the user's privileges and many applications were not designed to work with UAC, security errors are bound to be even more frequent in Windows Vista and Windows 7 than they were in Windows XP.

Most UAC-related problems are authorization-related, not authentication-related. If the user doesn't receive a UAC prompt at all but still receives a security error, it's definitely an authorization problem. If the user receives a UAC prompt and the user's credentials are accepted (or if the user logs on as an administrator and only needs to click Continue), it's definitely an authorization problem. UAC problems are authentication-related only if UAC prompts a user for credentials and rejects the user's password.

### 5.2. Use Auditing to Troubleshoot Authentication Problems

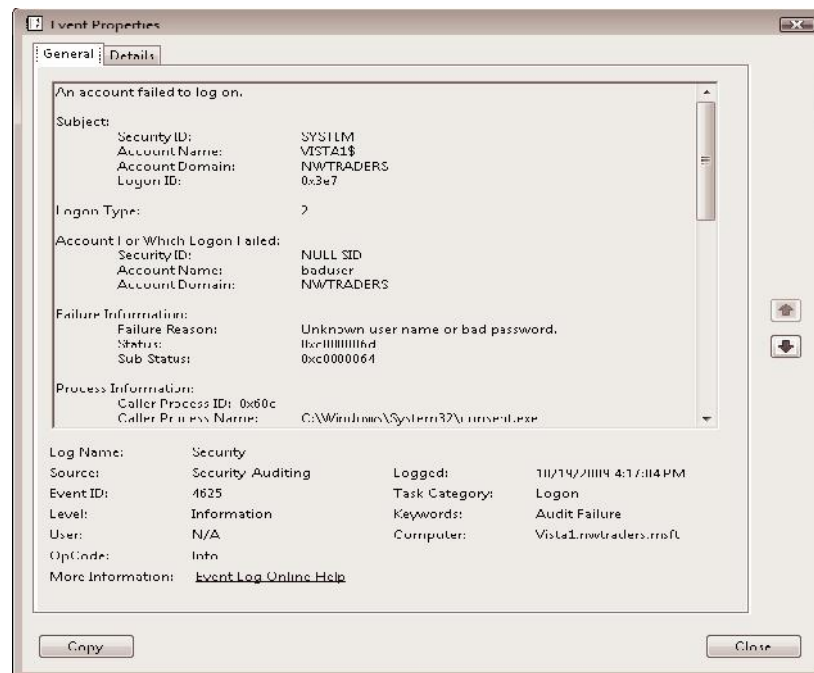
By default, Windows 7 does not add an event to the event log when a user provides incorrect credentials (such as when a user mistypes a password). Therefore, when troubleshooting authentication problems, your first step should be to enable auditing for logon events so that you can gather more information about the credentials the user provided and the resource being accessed.

Windows 7 (and earlier versions of Windows) provides two separate authentication auditing policies:

- **Audit Logon Events** This policy audits authentication attempts for local resources, such as a user logging on locally, elevating privileges using a UAC prompt, or connecting over the network (including connecting using Remote Desktop or connecting to a shared folder). All authentication attempts will be audited, regardless of whether the authentication attempt uses a domain account or a local user account.
- **Audit Account Logon Events** This policy audits domain authentications. No matter which computer the user authenticates to, these events appear only on the domain controller that handled the authentication request. Typically, you do not need to enable auditing of account logon events when troubleshooting authentication issues on computers running Windows 7. However, successful auditing of these events is enabled for domain controllers by default.



Figure 5-1 shows an example of a logon audit failure that occurred when the user provided invalid credentials at a UAC prompt. Notice that the Caller Process Name (listed under Process Information) is Consent.exe, the UAC process.



**FIGURE 5-1** A logon audit failure caused by invalid credentials

Audits from failed authentication attempts from across the network resemble the following code. In particular, the Account Name, Account Domain, Workstation Name, and Source Network Address are useful for identifying the origin computer.

```
An account failed to log on.

Subject:
  Security ID:      NULL SID
  Account Name:     -
  Account Domain:   -
  Logon ID:         0x0

Logon Type:        3

Account For Which Logon Failed:
  Security ID:      NULL SID
  Account Name:     baduser
  Account Domain:   NWTRADERS

Failure Information:
  Failure Reason:   Unknown user name or bad password.
  Status:           0xc000006d
  Sub Status:       0xc0000064

Process Information:
  Caller Process ID: 0x0
  Caller Process Name: -

Network Information:
  Workstation Name:  CONTOSO-DC
  Source Network Address: 192.168.1.212
  Source Port:       4953

Detailed Authentication Information:
  Logon Process:     NtLmSsp
  Authentication Package: NTLM
  Transited Services: -
  Package Name (NTLM only): -
  Key Length:        0
```



When you are authenticating to network resources, authentication failures are always logged on the server, not on the client. For example, if you attempt to connect to a shared folder and you mistype the password, the event won't appear in your local event log—it appears instead in the event log of the computer sharing the folder.





Self-Check - 5	Written Test
----------------	--------------

**Directions:** Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. Before a user can log on to a computer running Windows 7, connect to a shared folder, or browse a protected Web site, the resource must validate the user's identity using a process known as \_\_\_\_\_. **(1 pts)**
2. Windows supports a variety of authentication techniques, including **(3 pts)**

---

---

---

3. \_\_\_\_\_ which is about the size of a credit card, contains a chip with a certificate that uniquely identifies the user. **(1 pts)**
4. When you combine two forms of authentication (such as both typing a password and providing a smart card), it's called \_\_\_\_\_. **(1 pts)**
5. \_\_\_\_\_ is the most secure and reliable authentication method because you cannot lose or forget your authentication. **(1 pts)**
6. When troubleshooting authentication problems, your first step should be to enable \_\_\_\_\_ so that you can gather more information about the credentials the user provided and the resource being accessed. **(1 pts)**
7. list and explain the two separate authentication auditing policies that Windows 7 (and earlier versions of Windows) provides. **(4 pts)**

- ---

---

---

---
- ---

---

---

---

**Note: Satisfactory rating - 7 points**

**Unsatisfactory - below 7 points**

You can ask your teacher for the copy of the correct answers.



## Answer Sheet

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

Name: \_\_\_\_\_

Date: \_\_\_\_\_

### Short Answer Questions

1. \_\_\_\_\_

2. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

3. \_\_\_\_\_

4. \_\_\_\_\_

5. \_\_\_\_\_

6. \_\_\_\_\_

7. \_\_\_\_\_  
Ñ \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Ñ \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_



## Operation Sheet - 1

## Techniques of setting User Account Control

### 1.1. Create a User Account

1. Click on **Start**, and then click on **Control Panel**
2. Click on **User Accounts**.
3. Click **Manage Another Account**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
4. Click on **Create a New Account**.
5. Type the **name you want** to give the user account, Click an **account type**, and then click **Create Account**.

### 1.2. Change Picture for a User Account

1. Click on **Start**, and then Click on **Control Panel**
2. Click on **User Accounts**.
3. Click **Change your picture**.
4. Click the **picture you want to use**, and then Click **Change Picture**.
  - Or If you want to use a picture of your own, Click **Browse** for more pictures, navigate to the picture you want to use, Click **the picture**, and then Click **Open**. You can use a picture of any size, but it must have one of the following file name extensions: **.jpg**, **.png**, **.bmp**, or **.gif**.

### 1.3. Rename a User Account

1. Click on **Start**, and then click on **Control Panel**.
2. Click on **User Accounts**.
3. Click **Change your account name**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
4. Type the **new name**, and then click **Change Name**.

#### Notes

- You **can't** change the name of the **guest account**.
- A username **can't be longer than 20 characters**, consist entirely of periods or spaces, or contain any of these characters: \ / " [ ] : | < > + = ; , ? \* @

### 1.4. Change a User's Account Type

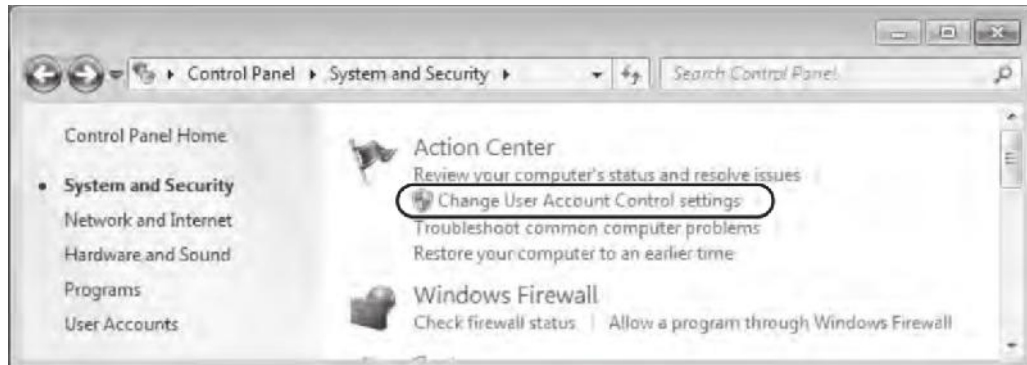
1. Click on **Start**, and then click on **Control Panel**
2. Click on **User Accounts**.
3. Click **Manage another account**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
4. Click the **account you want to change**, and then click **Change the account type**.
5. Select the **account type** you want, and then click **Change Account Type**.

**Note:** Windows requires at least one administrator account on a computer. If you have only one account on your computer, you can't change it to a standard account.

## 1.5. Configuring UAC in Control Panel

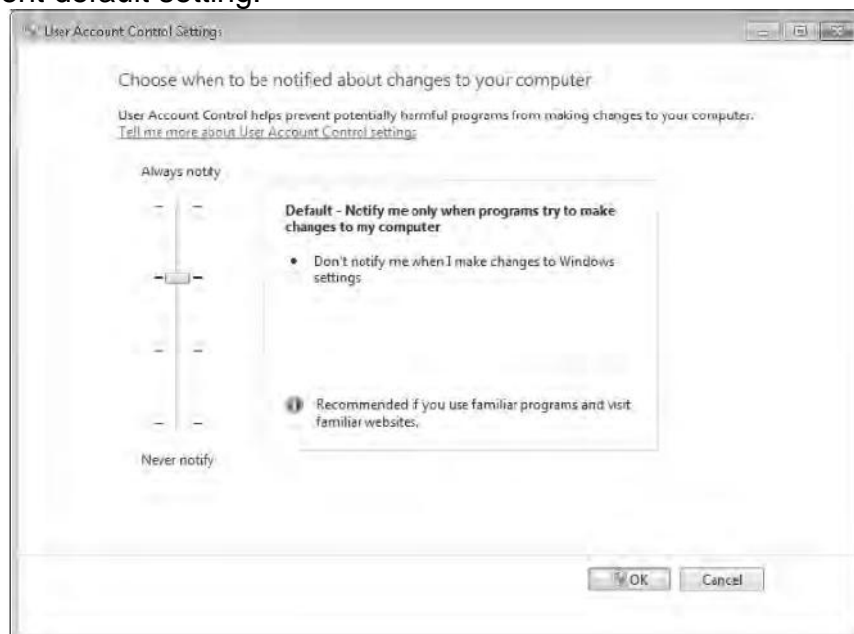
To configure UAC in Control Panel, perform the following steps:

1. In **Control Panel**, click **System and Security**.
2. Under **Action Center**, click **Change User Account Control Settings**, as shown in Figure 1.5-1.



**FIGURE 1.5-1** You can access UAC settings through the Action Center

This step opens the User Account Settings window, one version of which is shown in Figure 5. Note that the set of options that appears is different for administrators and standard users, and that each user type has a different default setting.



**FIGURE 1.5-2** UAC allows you to choose among four notification levels.

3. Choose one of the following notification levels:
  - **Always Notify** This level is the default for standard users, and it configures UAC to act as it does in Windows Vista. At this level, users are notified whenever any changes that require administrator privileges are attempted on the system.
  - **Notify Me Only When Programs Try To Make Changes To My Computer** This level is the default for administrators and is not available for standard users. At this level, administrators are not



notified when they make changes that require administrator privileges. However, users are notified through consent prompt when a program requests elevation.

- **Always Notify Me (And Do Not Dim My Desktop)** This level is not available for administrators. It is similar to the default setting for standard users, except that at this particular level, the Secure Desktop is never displayed. Disabling the Secure Desktop tends to reduce protection against malware, but it improves the user experience. This setting might be suitable for standard users who very frequently need to request elevation.
- **Notify Me Only When Programs Try To Make Changes To My Computer (Do Not Dim The Desktop)** This level is available for both standard users and administrators. At this level, the behavior is the same as with the default administrator level (“Notify me only when programs try to make changes to my computer”), but with this option the Secure Desktop is not displayed.
- **Never Notify** This level disables notifications in UAC. Users are not notified of any changes made to Windows settings or when software is installed. This option is appropriate only when you need to use programs that are incompatible with UAC.

4. Click **OK**.



## Operation Sheet - 2

## Configuring User Account

### 2.1. Add a User Account to a Group

By adding a **user account** to a **group**, you can avoid having to grant the same access and **permission** to many different users one by one. Members of a group can make the same types of changes to settings and have the same access to folders, printers, and other network services.

1. Click on **Start**, and then click on **Control Panel**
2. Click on **Administrative Tools** and then Double-click on **Computer Management**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
3. In the **left pane of Computer Management**, click **Local Users and Groups**.
4. Click on **Groups folder**.
5. Right-click the **group you want to add the user account to**, and then click **Add to Group**.
6. Click **Add**, and then type **the name of the user account**.
7. Click **Check Names**, click **OK**.
8. Click **Apply**, and then click **OK**.

#### Note

- To help make your computer more secure, add a user to the Administrators group only if it is absolutely necessary. Users in the Administrators group have complete control of the computer. They can see everyone's files, change anyone's password, and install any software they want.

### 2.2. Remove a User Account from a Group

1. Click on **Start**, and then click on **Control Panel**
2. Click on **Administrative Tools** and then Double-click on **Computer Management**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
3. In the **left pane of Computer Management**, click **Local Users and Groups**.
4. Click on **Groups folder**.
5. Right-click the **group you want to remove the user account from**, and then click **Properties**.
6. Select **the name of the user account** and then Click **Remove**.
7. Click **Apply**, and then click **OK**.



### 2.3. Disable a User Account

If you have a user account that you want to make unavailable, you can disable it. A disabled account can be enabled again later. Disabling an account is different from deleting an account. If you delete an account, it can't be restored.

1. Click on **Start**, and then click on **Control Panel**
2. Click on **Administrative Tools** and then Double-click on **Computer Management**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
3. In the **left pane of Computer Management**, click **Local Users and Groups**.
5. Click on **Users folder**.
6. Right-click the **user account you want to disable**, and then click **Properties**.
7. On the General tab, **select the Account is disabled check box**, and then Click **OK**.

#### Note

- To enable a disabled account, follow the same steps as you would for disabling an account, but clear the Account is disabled check box.

### 2.4. Delete a User Account

If you have a user account on your computer that is not being used, you can permanently remove it by deleting it. When you delete a user account, you can choose whether you want to keep the files created under that account; however, e-mail messages and computer settings for the account will be deleted.

1. Click on **Start**, and then click on **Control Panel**
2. Click on **User Accounts**.
3. Click **Manage another account**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
4. Click the **account you want to delete**, and then click **Delete the account**.
5. **Decide** if you want to **keep** or **delete the files** created under the account by clicking **Keep Files** or **Delete Files**.
6. Click **Delete Account**.



### **3.1. Enable Audit Logon Events**

To log failed authentication attempts, you must enable auditing by following these steps:

1. Click Start and then click Control Panel. Click System and Security. Click Administrative Tools, and then double-click Local Security Policy.
2. In the Local Security Policy console, expand Local Policies, and then select Audit Policy.
3. In the right pane, double-click Audit Logon Events.
4. In the Audit Logon Events Properties dialog box, select the Failure check box to add an event to the Security event log each time a user provides invalid credentials. If you also want to log successful authentication attempts (which include authentication attempts from services and other nonuser entities), select the Success check box.
5. Click OK.
6. Restart your computer to apply the changes.

### **3.2. View Audit Logon Events**

With auditing enabled, you can view audit events in Event Viewer by following these steps:

1. Click Start, right-click Computer, and then click Manage.
2. Expand System Tools, Event Viewer, Windows Logs, and then select Security.
3. Event Viewer displays all security events. To view only successful logons, click the Filter Current Log link in the Actions pane and show only Event ID 4624. To view only unsuccessful logon attempts, click the Filter Current Log link and show only Event ID 4625.





LAP Test	Practical Demonstration
----------	-------------------------

Name: \_\_\_\_\_ Date: \_\_\_\_\_

Time started: \_\_\_\_\_ Time finished: \_\_\_\_\_

**Instructions:** Given necessary templates, tools and materials you are required to perform the following tasks within 4 hour.

**Task 1. User Account Control**

1.1. Create the following User Accounts

1.1.1. An Administrator Account

- A. Make the Username “Admin1”
- B. Make the password “Admin@123”
- C. Make the Account picture any picture you want

1.1.2. An Administrator Account

- A. Make the Username “Admin2”
- B. Make the password “Admin@321”
- C. Make the Account picture different picture you want

1.1.3. A Standard Account

- D. Make the Username “Stand1”
- E. Make the password “Stand@123”
- F. Make the Account picture different picture you want

1.1.4. Another Standard Account

- A. Make the Username “Stand2”
- B. Make the password “Stand@210”
- C. Make the Account picture different picture you want

1.1.5. Turn on the Guest Account

1.2. Rename a User Account with

- “Stand2” username to “Stand2Admin”
- “Admin1” username to “Admin2Stand”

1.3. Change a User’s Account Type

- “Stand2Admin” to “Administrator Account”
- “Admin2Stand” to “Standard Account”

1.4. Change User Account Control

- Change Notification Level to “**Always Notify**”



## **Task 2.** Configuring User Account

### 2.1. Disable the User Account with

- “Stand2Admin” username
- “Admin2Stand” username

### 2.2. Delete the User Account with

- “Stand1” username

### 2.3. Enable the User Account with

- “Stand2Admin” username
- “Admin2Stand” username

### 2.4. Add the User Account with

- “Admin2Stand” username to “Administrator” Group
- “Stand2Admin” username to “Users” Group

## **Task 3.** Accessing Information Services

### 3.1. Enable Audit Logon Events

### 3.2. View Audit Logon Events



## List of Reference Materials

MCITP Exam 70-685: Windows 7 Enterprise Desktop Support Technician, Tony Northrup and J.C. Mackin

<https://www.sitepoint.com/5-steps-to-uncovering-your-it-security-gaps/>

[https://en.wikibooks.org/wiki/Fundamentals\\_of\\_Information\\_Systems\\_Security/Access\\_Control\\_Systems#Access\\_Control\\_Assurance](https://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems#Access_Control_Assurance)

[https://en.wikipedia.org/wiki/Computer\\_access\\_control](https://en.wikipedia.org/wiki/Computer_access_control)

[https://en.wikibooks.org/wiki/Category:Book:Fundamentals\\_of\\_Information Systems Security](https://en.wikibooks.org/wiki/Category:Book:Fundamentals_of_Information_Systems_Security)

<https://www.computerweekly.com/opinion/Identify-security-gaps>



# **INFORMATION TECHNOLOGY SUPPORT SERVICE**

**Level - I**

## **LEARNING GUIDE 34**

<b>Unit of Competence:</b>	<b>Protect Application or System Software</b>
<b>Module Title:</b>	<b>Protecting Application or System Software</b>
<b>LG Code:</b>	<b>ICT ITS1 M09 LO2 – LG34</b>
<b>TTLM Code:</b>	<b>ICT ITS1 TTLM 1019v1</b>

### **LO 2: Detect and Remove Destructive Software**



## Instruction Sheet

## Learning Guide 34

This learning guide is developed to provide you the necessary information regarding the following content coverage and topics –

- Common types of destructive software
- Selecting and Installing Virus Protection Software
- Advanced systems of protection
- Installing software updates
- Configuring software security settings

This guide will also assist you to attain the learning outcome stated in the cover page. Specifically, upon completion of this Learning Guide, you will be able to –

- Defining and identifying common types of destructive software
- Selecting and installing virus protection compatible with the operating system
- Describing advanced systems of protection
- Installing software updates on a regular basis
- Configuring software security settings
- Running and/or scheduling virus protection software on a regular basis
- Reporting detected destructive software
- Removing destructive software

### Learning Instructions:

1. Read the specific objectives of this Learning Guide.
2. Follow the instructions described below 3 to 6.
3. Read the information written in the information “Sheet 1, Sheet 2, Sheet 3, Sheet 4 and Sheet 5” in page 3, 14, 26, 30 and 35 respectively.
4. Accomplish the “Self-check 1, Self-check 2 and Self-check 3” in page 12, 24, 28, 33 and 37 respectively
5. If you earned a satisfactory evaluation from the “Self-check” proceed to “Operation Sheet 1, Operation Sheet 2 and Operation Sheet 3” in page 39
6. Do the “LAP test” in page



### 1.1. Destructive Software

Destructive software is referred to as **malware** (malicious software) and the term includes **viruses, worms, logic bombs, rootkits, Trojan horses, adware, keystroke loggers** and **spyware**. **Malware** is software designed to infiltrate a computer system without the owner's informed consent; hostile, intrusive, or annoying software.

**Data-stealing malware** is a threat that divests victims of personal or proprietary information with the intent of monetizing stolen data through direct use or distribution. This type of malware includes **key loggers, screen scrapers, spyware, adware, backdoors** and **bots**. **Malware's** most common pathway from criminals or malicious developers to users is through the Internet: primarily by email and the World Wide Web.

The target of malicious software can be a single computer and its operating system, a network or an application.

### 1.2. The Common Types of Destructive Software

The common types of destructive software are:

- **Virus**

A computer program that can copy itself and infect a computer. The term "virus" is also commonly but erroneously used to refer to other types of malware, adware, and spyware programs that do not have the reproductive ability.

- **Worm**

Write Once, Read Many (Write One, Read Multiple or WORM); a software program capable of reproducing itself that can spread from one computer to the next over a network; WORMs take advantage of automatic file sending and receiving features found on many computers; self-replicating Malware computer program;

- **Logic Bomb**

Set of instructions inserted into a program that are designed to execute (or 'explode') if a particular condition is satisfied; when exploded it may delete or corrupt data, or print a spurious message, or have other harmful effects; it could be triggered by a change in a file, by a particular input sequence to the program, or at a particular time or date.



- **Rootkit**

A type of malware that is designed to gain administrative-level control over a computer system without being detected

- **Trojan Horse**

A Trojan, as the name implies, secretly carries often-damaging software in the guise of an innocuous program, often in an email attachment.

- **Adware**

Adware is software that loads itself onto a computer and tracks the user's browsing habits or pops up advertisements while the computer is in use. Adware and spyware disrupt your privacy and can slow down your computer as well as contaminate your operating system or data files

- **KeyLogger**

The practice of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored

- **Spyware**

Software that obtains information from a user's computer without the user's knowledge or consent

- **Screen Scrapers**

To extract data from (a source such as a webpage) by picking it out from among the human-readable content

- **Backdoor**

An undocumented way to get access to a computer system or the data it contains

- **Bots**

Also known as Crawlers or Spiders, bots are search engine programs that perform automated tasks on the internet – they follow links, and read through the pages in order to index the site in a search engine.

**Greyware (grayware):** a general term sometimes used as a classification for applications that behave in a manner that is annoying or undesirable but less serious or troublesome than malware; greyware encompasses spyware, adware, dialers, joke programs, remote access tools, and any other unwelcome files and programs apart from viruses that are designed to harm the performance of computers on your network.



## 1.3. Virus Origin, History and Evolution

### 1.3.1. Virus Origins

Computer viruses are called viruses because they share some of the traits of biological viruses. A computer virus passes from computer to computer like a biological virus passes from person to person.

Unlike a cell, a virus has no way to reproduce by itself. Instead, a biological virus must inject its DNA into a cell. The viral DNA then uses the cell's existing machinery to reproduce itself. In some cases, the cell fills with new viral particles until it bursts, releasing the virus. In other cases, the new virus particles bud off the cell one at a time, and the cell remains alive.

A computer virus shares some of these traits. A computer virus must **piggyback** on top of some other program or document in order to launch. Once it is running, it can infect other programs or documents. Obviously, the analogy between computer and biological viruses stretches things a bit, but there are enough similarities that the name sticks.

People write computer viruses. A person has to write the code, test it to make sure it spreads properly and then release it. A person also designs the virus's attack phase, whether it's a silly message or the destruction of a hard disk. Why do they do it?

There are at least three reasons. The first is the same psychology that drives vandals and arsonists. Why would someone want to break a window on someone's car, paint signs on buildings or burn down a beautiful forest? For some people, that seems to be a thrill. If that sort of person knows computer programming, then he or she may funnel energy into the creation of destructive viruses.

The second reason has to do with the thrill of watching things blow up. Some people have a fascination with things like explosions and car wrecks. When you were growing up, there might have been a kid in your neighborhood who learned how to make gunpowder. And that kid probably built bigger and bigger bombs until he either got bored or did some serious damage to himself. Creating a virus is a little like that -- it creates a bomb inside a computer, and the more computers that get infected the more "fun" the explosion.

The third reason involves bragging rights, or the thrill of doing it. Sort of like Mount Everest -- the mountain is there, so someone is compelled to climb it. If you are a certain type of programmer who sees a security hole that could be exploited, you might simply be compelled to exploit the hole yourself before someone else beats you to it.

Of course, most virus creators seem to miss the point that they cause real damage to real people with their creations. Destroying everything on a person's hard disk is real damage. Forcing a large company to waste thousands of hours





cleaning up after a virus is real damage. Even a silly message is real damage because someone has to waste time getting rid of it. For this reason, the legal system is getting much harsher in punishing the people who create viruses.

### 1.3.2. Virus History

Traditional computer viruses were first widely seen in the late 1980s, and they came about because of several factors. The first factor was the spread of personal computers (**PCs**). Prior to the 1980s, home computers were nearly non-existent or they were toys. Real computers were rare, and they were locked away for use by "experts." During the 1980s, real computers started to spread to businesses and homes because of the popularity of the IBM PC (released in 1982) and the Apple Macintosh (released in 1984). By the late 1980s, PCs were widespread in businesses, homes and college campuses.

The second factor was the use of computer **bulletin boards**. People could dial up a bulletin board with a modem and download programs of all types. Games were extremely popular, and so were simple word processors, spreadsheets and other productivity software. Bulletin boards led to the precursor of the virus known as the **Trojan horse**. A Trojan horse is a program with a cool-sounding name and description. So you download it. When you run the program, however, it does something uncool like erasing your disk. You think you are getting a neat game, but it wipes out your system. Trojan horses only hit a small number of people because they are quickly discovered, the infected programs are removed and word of the danger spreads among users.



**Figure 1-1 Floppy disks were factors in the spread of computer viruses.**

The third factor that led to the creation of viruses was the **floppy disk**. In the 1980s, programs were small, and you could fit the entire operating system, a few programs and some documents onto a floppy disk or two. Many computers did not have hard disks, so when you turned on your machine it would load the operating system and everything else from the floppy disk. Virus authors took advantage of this to create the first self-replicating programs.

Early viruses were pieces of code attached to a common program like a popular game or a popular word processor. A person might download an infected game from a bulletin board and run it. A virus like this is a small piece of code embedded in a larger, legitimate program. When the user runs the legitimate program, the virus loads itself into memory and looks around to see if it can find any other programs on the disk. If it can find one, it modifies the program to add



the virus's code into the program. Then the virus launches the "real program." The user really has no way to know that the virus ever ran. Unfortunately, the virus has now reproduced itself, so two programs are infected. The next time the user launches either of those programs, they infect other programs, and the cycle continues.

If one of the infected programs is given to another person on a floppy disk, or if it is uploaded to a bulletin board, then other programs get infected. This is how the virus spreads.

The spreading part is the **infection** phase of the virus. Viruses wouldn't be so violently despised if all they did was replicate themselves. Most viruses also have a destructive **attack** phase where they do damage. Some sort of trigger will activate the attack phase, and the virus will then do something -- anything from printing a silly message on the screen to erasing all of your data. The trigger might be a specific date, the number of times the virus has been replicated or something similar.

### 1.3.3. Virus Evolution

As virus creators became more sophisticated, they learned new tricks. One important trick was the ability to load viruses into memory so they could keep running in the background as long as the computer remained on. This gave viruses a much more effective way to replicate themselves. Another trick was the ability to infect the **boot sector** on floppy disks and hard disks. The boot sector is a small program that is the first part of the operating system that the computer loads. It contains a tiny program that tells the computer how to load the rest of the operating system. By putting its code in the boot sector, a virus can **guarantee it is executed**. It can load itself into memory immediately and run whenever the computer is on. Boot sector viruses can infect the boot sector of any floppy disk inserted in the machine, and on college campuses, where lots of people share machines, they could spread like wildfire.

In general, neither executable nor boot sector viruses are very threatening any longer. The first reason for the decline has been the huge size of today's programs. Nearly every program you buy today comes on a compact disc. Compact discs (CDs) cannot be modified, and that makes viral infection of a CD unlikely, unless the manufacturer permits a virus to be burned onto the CD during production. The programs are so big that the only easy way to move them around is to buy the CD. People certainly can't carry applications around on floppy disks like they did in the 1980s, when floppies full of programs were traded like baseball cards. Boot sector viruses have also declined because operating systems now protect the boot sector.

Infection from boot sector viruses and executable viruses is still possible. Even so, it is a lot harder, and these viruses don't spread nearly as quickly as they once did. Call it "shrinking habitat," if you want to use a biological analogy. The



environment of floppy disks, small programs and weak operating systems made these viruses possible in the 1980s, but that environmental niche has been largely eliminated by huge executables, unchangeable CDs and better operating system safeguards. E-mail viruses are probably the most familiar to you. We'll look at some in the next section.

- **E-mail Viruses**

Virus authors adapted to the changing computing environment by creating the **e-mail virus**. For example, the **Melissa virus** in March 1999 was spectacular. Melissa spread in Microsoft Word documents sent via e-mail, and it worked like this:

Someone created the virus as a Word document and uploaded it to an Internet newsgroup. Anyone who downloaded the document and opened it would trigger the virus. The virus would then send the document (and therefore itself) in an e-mail message to the first 50 people in the person's address book. The e-mail message contained a friendly note that included the person's name, so the recipient would open the document, thinking it was harmless. The virus would then create 50 new messages from the recipient's machine. At that rate, the Melissa virus quickly became the fastest-spreading virus anyone had seen at the time. As mentioned earlier, it forced a number of large companies to shut down their e-mail systems.

- **Worms**

A **worm** is a computer program that has the ability to copy itself from machine to machine. Worms use up computer time and network bandwidth when they replicate, and often carry payloads that do considerable damage. A worm called **Code Red** made huge headlines in 2001. Experts predicted that this worm could clog the Internet so effectively that things would completely grind to a halt.

A worm usually exploits some sort of **security hole** in a piece of software or the operating system. For example, the Slammer worm (which caused mayhem in January 2003) exploited a hole in Microsoft's SQL server. "Wired" magazine took a fascinating look inside Slammer's tiny (376 byte) program.

Worms normally move around and infect other machines through computer networks. Using a network, a worm can expand from a single copy incredibly quickly. The Code Red worm replicated itself more than 250,000 times in approximately nine hours on July 19, 2001 [Source: Rhodes].

The Code Red worm slowed down Internet traffic when it began to replicate itself, but not nearly as badly as predicted. Each copy of the worm scanned the Internet for Windows NT or Windows 2000 servers that did not have the Microsoft security patch installed. Each time it found an unsecured server, the worm copied itself to that server. The new copy then scanned for other



servers to infect. Depending on the number of unsecured servers, a worm could conceivably create hundreds of thousands of copies.

The Code Red worm had instructions to do three things:

- ✓ Replicate itself for the first 20 days of each month
- ✓ Replace Webpages on infected servers with a page featuring the message "Hacked by Chinese"
- ✓ Launch a concerted attack on the White House Web site in an attempt to overwhelm it

Upon successful infection, Code Red would wait for the appointed hour and connect to the [www.whitehouse.gov](http://www.whitehouse.gov) domain. This attack would consist of the infected systems simultaneously sending 100 connections to port 80 of [www.whitehouse.gov](http://www.whitehouse.gov) (198.137.240.91).

The U.S. government changed the IP address of [www.whitehouse.gov](http://www.whitehouse.gov) to circumvent that particular threat from the worm and issued a general warning about the worm, advising users of Windows NT or Windows 2000 Web servers to make sure they installed the security patch. .

A worm called Storm, which showed up in 2007, immediately started making a name for itself. Storm uses social engineering techniques to trick users into loading the worm on their computers. So far, it's working -- experts believe between one million and 50 million computers have been infected [source: Schneier].

When the worm is launched, it opens a back door into the computer, adds the infected machine to a botnet and installs code that hides itself. The botnets are small peer-to-peer groups rather than a larger, more easily identified network. Experts think the people controlling Storm rent out their micro-botnets to deliver spam or adware, or for denial-of-service attacks on Web sites.

#### 1.4. Types of Viruses

Viruses are split into different categories, depending on what they do. Here are a few categories of viruses:

- **Boot Sector Virus**

The Boot Sector of a PC is a part of your computer that gets accessed first when you turn it on. It tells Windows what to do and what to load. It's like a "Things To Do" list. The Boot Sector is also known as the Master Boot Record. A boot sector virus is designed to attack this, causing your PC to refuse to start at all!

- **File Virus**

A file virus, as its name suggests, attacks files on your computer. Also attacks entire programs, though.



- **Macro Virus**

These types of virus are written specifically to infect Microsoft Office documents (Word, Excel PowerPoint, etc.) A Word document can contain a Macro Virus. You usually need to open a document in a Microsoft Office application before the virus can do any harm.

- **Multipartite Virus**

A multipartite virus is designed to infect both the boot sector and files on your computer

- **Polymorphic Virus**

This type of virus alters their own code when they infect another computer. They do this to try and avoid detection by anti-virus programs.

- **Electronic Mail (Email) Virus**

Refers to the delivery mechanism rather than the infection target or behavior. Email can be used to transmit any of the above types of virus by copying and emailing itself to every address in the victim's email address book, usually within an email attachment. Each time a recipient opens the infected attachment, the virus harvests that victim's email address book and repeats its propagation process.

## 1.5. Virus Infection, Removal and Prevention

### 1.5.1. Virus Infection

The most common way that a virus gets on your computer is by an **email attachment**. If you open the attachment, and your anti-virus program doesn't detect it, then that is enough to infect your computer. Some people go so far as NOT opening attachments at all, but simply deleting the entire message as soon as it comes in. While this approach will greatly reduce your chances of becoming infected, it may offend those relatives of yours who have just sent you the latest pictures of little Johnny!

You can also get viruses by **downloading programs from the internet**. That great piece of freeware you spotted from an obscure site may not be so great after all. It could well be infecting your PC as the main program is installing.

If your PC is running any version of Windows, and it **hasn't got all the latest patches and updates**, then your computer will be attacked a few minutes after going on the internet! (Non Windows users can go into smug mode!)

Nowadays, they utilized the use of **removable storage devices** to spread viruses. The most common is the use of flash drive. Since removable drives like flash drive, CD/DVDs have the **autorun functionality**, *a simple command that enables the executable file to run automatically*, they exploited and altered it so it will automatically run the virus (normally with .exe, .bat, .vbs format) when you insert your flash drive or CD/DVDs.



## Virus Infection Symptoms

Common symptoms of a virus-infected computer include

- Unusually slow running speeds
- Failure to respond to user input
- System crashes and constant system restarts that are triggered automatically.
- Individual applications also might stop working correctly,
- Disk drives might become inaccessible,
- Unusual error messages may pop up on the screen,
- Menus and dialog boxes can become distorted and peripherals like printers might stop responding.
- You can't access your disk drives
- Other symptoms to look out for are strange error messages, documents not printing correctly, and distorted menus and dialogue boxes.

Try not to panic if your computer is exhibiting one or two items on the list. Keep in mind that these types of hardware and software problems are not always caused by viruses, but infection is certainly a strong possibility that is worth investigating.

### 1.5.2. Removal of Viruses

The first step in removing computer is **installing any updates** that are available for your operating system; modern operating systems will automatically look for updates if they are connected to the Internet. If you do not already **have anti-virus software** on your computer, install and use the **anti-virus software** to do a complete scan of your computer. Since new computer viruses are constantly being created, set your anti-virus program to automatically check for updates regularly.

### 1.5.3. Prevention from Virus Infections

In order to prevent future computer infections:

- use an **Internet firewall**,
- check for operating system and anti-virus program updates,
- scan your computer regularly and exercise caution when handling email and Internet files.

A **firewall** is a program or piece of hardware that helps screen out viruses, worms and hackers which are attempting to interact with your computer via the Internet. On modern computers, firewalls come pre-installed and are turned on by default, so you probably already have one running in the background. When opening email attachments, don't assume they are safe just because they come from a friend or reliable source; the sender may have unknowingly forwarded an attachment that contains a virus.





Self-Check - 1	Written Test
----------------	--------------

**Directions:** Answer all the questions listed below. Use the Answer sheet provided in the next page:

**Part I: Say True or False**

- \_\_\_\_\_ 1. Once the infected program has been run or installed the virus is activated and begins to spread itself to other programs on the current system.
- \_\_\_\_\_ 2. Adware and spyware not disrupt your privacy and can slow down your computer as well as contaminate your operating system or data files
- \_\_\_\_\_ 3. Virus authors are continually releasing new and updated viruses, so it is important that you have the latest definitions installed on your computer.
- \_\_\_\_\_ 4. Anti-virus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software.
- \_\_\_\_\_ 5. Email Virus refers to the delivery mechanism rather than the infection target or behaviour.

**Part II: Matching Column A with the Column B**

**Column A**

- \_\_\_\_\_ 1. Logic Bomb
- \_\_\_\_\_ 2. Rootkit
- \_\_\_\_\_ 3. Adware
- \_\_\_\_\_ 4. KeyLogger
- \_\_\_\_\_ 5. Spyware
- \_\_\_\_\_ 6. Boot Sector Virus
- \_\_\_\_\_ 7. File Virus
- \_\_\_\_\_ 8. Macro Virus
- \_\_\_\_\_ 9. Multipartite Virus
- \_\_\_\_\_ 10. Polymorphic Virus

**Column B**

- A.** A type of virus alters their own code when they infect another computer.
- B.** A virus that is designed to infect both the boot sector and files on your computer
- C.** Types of virus that are written specifically to infect Microsoft Office documents (Word, Excel PowerPoint, etc.)
- D.** A virus that attacks files on your computer and also attacks entire programs.
- E.** A virus that is designed to attack a boot sector, causing your PC to refuse to start at all!
- F.** Software that obtains information from a user's computer without the user's knowledge or consent
- G.** The practice of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored
- H.** Software that loads itself onto a computer and tracks the user's browsing habits or pops up



## Answer Sheet

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

Name: \_\_\_\_\_

Date: \_\_\_\_\_

### 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. \_\_\_\_\_

**Note: Satisfactory rating - 8 points**

**Unsatisfactory - below 8 points**

You can ask your teacher for the copy of the correct answers.





## **2.1. Protection Software**

We used to call everything a virus, however there are more precise names to further categorize **malware** – among them **virus**, **worm**, **Trojan**, **spyware**, **malware** and **adware**, to name a few.

Infection can have a devastating effect on the functioning of stand-alone machines and networks and can cause irretrievable damage to data and other resources. It is imperative to develop mechanisms to avoid infection. Detecting **malware** is a very sophisticated and well-defined process. Consequently, network administrators rely often rely on third party products to manage this process.

There is a variety of software packages available for both Single Device and Enterprise/Networked devices.

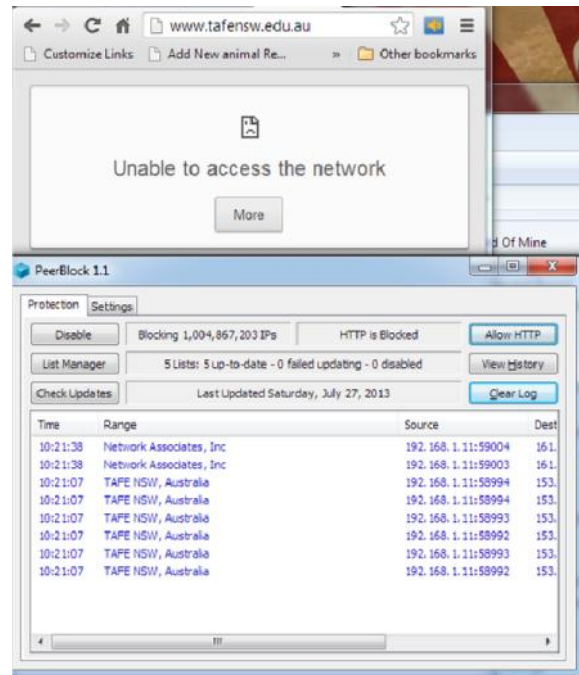
### **2.1.1. Single User**

There are many kinds of protection software available for a single use device. Among them are

- Avast
- AVG
- Avira
- Bitdefender
- BullGuard
- Emsisoft
- ESET NOD32
- Fortinet
- F-Secure
- GData
- Kaspersky
- Kingsoft
- McAfee
- Microsoft Security Essentials
- Panda Cloud
- Qihoo 360
- Sophos
- ThreatTrack Vipre
- Trend Micro Titanium

Specialised software for removal such as Spybot Search & Destroy, Malwarebytes anti-malware and WinZip Malware Protector.

Other specialised programs that can block certain known IP addresses of hackers, unwanted advertising companies. One program that does this is PeerBlock. PeerBlock blocks "known bad" computers from accessing yours, and vice versa. Depending on the lists you have it set up to use, you can block governments, corporations, machines flagged for anti-peer-to-peer activities, even entire countries. The down side of this is that you will have to keep an eye on the program as it can block legitimate sites just because they have possibly been used for hacking attempts.



**Figure 3-1: PeerBlock – What happens when blocking TAFE website**

With Peerblock you can edit your lists and add or remove addresses from the lists so that you can still control which computers you can or cannot access.

### 2.1.2. Multi User/Enterprise

Even though small business antivirus software is usually priced on a per-user basis with a cost that is on par with individual-user products, it often gives business owners important additional features such as the ability to install and manage all installations from a central location. Some of the available products are:

- Bitdefender Small Business Pack
- Kaspersky Endpoint Security for Business
- F-Secure Small Business Suite
- Symantec Endpoint Protection
- G Data AntiVirus Business
- Webroot Secure Anywhere Business
- Vipre Business Premium
- avast! Endpoint Protection Suite
- Panda Security for Business
- Total Defense Threat Manage



## 2.2. Anti-Virus Software

**Antivirus** or **anti-virus software** is used to prevent, detect, and remove malware, including but not limited to computer viruses, computer worm, trojan horses, spyware and adware. This page talks about the software used for the prevention and removal of such threats, rather than computer security implemented by software methods.

No matter how useful antivirus software can be, it can sometimes have drawbacks. Antivirus software can **impair** a computer's performance. Inexperienced users may also have trouble understanding the prompts and decisions that antivirus software presents them with. An incorrect decision may lead to a security breach. If the antivirus software employs heuristic detection, success depends on achieving the right balance between false positives and false negatives. **False positives** can be as destructive as **false negatives**.

**False positives** are wrong detection by an anti-virus where legitimate files were mistakenly identified as viruses while **False negatives** are wrong detection by an anti-virus where legitimate viruses were not detected as viruses.

Finally, antivirus software generally runs at the highly trusted kernel level of the operating system, creating a potential avenue of attack.

Over the years it has become necessary for antivirus software to **check** an increasing **variety of files**, rather than just executables, for several **reasons**:

- Powerful macros used in word processor applications, such as Microsoft Word, presented a risk. **Virus writers could use the macros to write viruses embedded within documents.** This meant that computers could now also be at risk from infection by opening documents with hidden attached macros.
- Later **email programs**, in particular Microsoft Outlook Express and Outlook, were vulnerable to viruses embedded in the email body itself. A user's computer could be infected by just opening or previewing a message.

As always-on broadband connections became the norm, and more and more viruses were released, it became essential to update virus checkers more and more frequently. Even then, a new zero-day virus could become widespread before antivirus companies released an update to protect against it.



## 2.3. Types of Protection Software

Depending on ***the way they fix destructive software*** these can be in the following forms: ***Anti-Virus***, ***Anti-spyware***, and ***Anti-spam*** Applications.

### 2.3.1. Anti-Viruses

- Anti-virus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software.
- Anti-virus software typically uses two different techniques to accomplish this:
  - ✓ Examining (scanning) files to look for known viruses matching definitions in a virus dictionary.
  - ✓ Identifying suspicious behavior from any computer program which might indicate infection. Such analysis may include data captures, port monitoring and other methods.
- Most commercial anti-virus software uses both of these approaches, with an emphasis on the virus dictionary approach.

### 2.3.2. Anti-Spyware

- These are software's that are designed to discover, detect and block spyware.
- Anti-spyware programs can combat spyware in two ways:
  - ✓ They can provide real time protection against the installation of spyware software on your computer. This type of spyware protection works the same way as that of anti-virus protection in that the anti-spyware software scans all incoming network data for spyware software and blocks any threats it comes across.
  - ✓ Anti-spyware software programs can be used solely for detection and removal of spyware software that has already been installed onto your computer. This type of spyware protection is normally much easier to use and more popular.

### 2.3.3. Anti-Spam

- To prevent e-mail spam, both end users and administrators of e-mail systems use various anti-spam techniques.
- None of the techniques is a complete solution to the spam problem, and each has trade-offs between incorrectly rejecting legitimate e-mail vs. not rejecting all spam, and associated costs in time and effort.
- Anti-spam techniques can be broken into two broad categories:
  - ✓ those that require actions by individuals, and
  - ✓ those that can be automated.



## 2.4. Methods Anti-virus Use to Identify Malware

There are several methods which 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.

### 2.4.1. Signature-based detection

Traditionally, antivirus software heavily relied upon signatures to identify malware. This can be very effective, but cannot defend against malware unless samples have already been obtained and signatures created. Because of this, signature-based approaches are **not effective against new**, unknown viruses.

As new viruses are being created each day, the signature-based detection approach **requires frequent updates** of the virus signature dictionary. To assist the antivirus software companies, the software may allow the user to upload new viruses or variants to the company, allowing the virus to be analyzed and the **signature added to the dictionary**.

Although the signature-based approach can effectively contain virus outbreaks, virus authors have tried to stay a step ahead of such software by writing "**oligomorphic**", "**polymorphic**" and, more recently, "**metamorphic**" viruses, which **encrypt parts of themselves** or otherwise modify themselves **as a method of disguise, so as to not match virus signatures in the dictionary**.

### 2.4.2. Heuristics

Some more sophisticated antivirus software uses heuristic analysis to identify new malware or variants of known malware.

Many **viruses start** as a **single infection** and through either mutation or refinements by other attackers, can **grow** into dozens of slightly different strains, called **variants**. Generic detection refers to the detection and removal of multiple threats using a single virus definition.

For example, the **Vundo trojan** has several family members, depending on the antivirus vendor's classification. Symantec classifies members of the Vundo family into two distinct categories, *Trojan.Vundo* and *Trojan.Vundo.B*.



While it may be advantageous to identify a specific virus, it can be quicker to detect a virus family through a **generic signature** or through an inexact match to an existing signature. Virus researchers find common areas that all viruses in a family share uniquely and can thus create a single generic signature. These signatures often contain non-contiguous code, using wildcard characters where differences lie. These wildcards allow the scanner to detect viruses even if they are padded with extra, meaningless code. A detection that uses this method is said to be "heuristic detection."

### 2.4.3. Rootkit detection

Anti-virus software can also scan for rootkits; a **rootkit virus** is a type of malware that is designed to gain administrative-level control over a computer system without being detected. Rootkits can change how the operating system functions and in some cases can tamper with the anti-virus program and render it ineffective. Rootkits are also difficult to remove, in some cases requiring a complete re-installation of the operating system.

## 2.5. Selecting Anti-Virus Software

A good security program needs to be integrated & working actively deep in the system in order to protect it from malicious software. This means that it needs to be active from initial boot up to shutdown, scanning each process or program and how it interacts with the system.

It is therefore important when choosing a virus scanner that protects the system from all kinds of malicious software but also that it doesn't degrade the device's ability to function.
























In the previous module, we have already discussed the planning and analysis that should be undertaken before any systems software is installed onto a computer. The installation of anti-virus software is no different. Each analysis step that we have covered must be undertaken to ensure that the software we choose is going to meet our needs as well as maintain compatibility with the operating system, application software and hardware. When it comes to anti-virus software however, 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

In most cases, this information will be covered on the website of the software manufacturer.

## 2.6. Avast Anti-Virus Software

The screenshot below display the three Avast antivirus products with their features, from essential to complete protection

		 Free AntiVirus Essential	 Internet Security Advanced	 Premier Complete
	Anti-Malware	•	•	•
	Anti-Spyware	•	•	•
	Streaming Updates	•	•	•
	Hardened Mode	•	•	•
	CyberCapture	•	•	•
	Game Mode	•	•	•
	Behavior Shield	•	•	•
	Do Not Track, SiteCorrect, Anti-Phishing <b>ENHANCED</b>	•	•	•
	Wi-Fi Inspector	•	•	•
	Web / File / Mail Shield	•	•	•
	Smart Scan	•	•	•
	Passwords	•	•	•
	Software Updater	Manual	Manual	Automatic
	Ransomware Shield <b>NEW</b>		•	•
	Sandbox		•	•
	Real Site		•	•
	Anti-Spam		•	•
	Firewall		•	•
	Data Shredder			•
	Webcam Shield <b>NEW</b>			•





## 2.7. Installing Anti-Virus Software

The Following system requirements are recommended in order to install and run Avast! Free Antivirus on your computer:

- Microsoft Windows XP Service Pack 2 or higher (any Edition, 32-bit or 64-bit), Microsoft Windows Vista (any Edition excl. Starter Edition, 32-bit or 64-bit) or Microsoft Windows 7 (any Edition, 32-bit or 64-bit).
- Windows fully compatible PC with Intel Pentium III processor or above (depends on the requirements of used operating system version and other 3rd party software installed).
- 256 MB RAM or above (depends on the requirements of used operating system version and other 3rd party software installed).
- 210 MB free space on the hard disk, 300MB if also included Google Chrome will be installed (to download and install).
- Internet connection (to download and register the product, for automatic updates of program engine and antivirus database).
- Optimally standard screen resolution not less than 1024 x 768 pixels.

Before you begin the installation of Avast! Free Antivirus please ensures that:

- You are logged in to Windows as Administrator or as a user with administrator permissions
- All other programs in Windows are closed and not running
- Your previous antivirus software is fully uninstalled (for instructions refer to your vendor's documentation),

Once you have installed an anti-virus package, you should scan your entire computer periodically. Always leave your Anti-virus software running so it can provide constant protection.

- **Automatic Scans-** Depending what software you choose, you may be able to configure it to automatically scan specific files or directories and prompt you at set intervals to perform complete scans.
- **Manual Scans-** It is also a good idea to manually scan files you receive from an outside source before opening them. This includes:
  - ✓ Saving and scanning *email attachments* or *web downloads* rather than selecting the option to open them directly from the source
  - ✓ Scanning *flash disks*, *CDs*, or *DVDs* for viruses before opening any of the files





## **TIPS TO BOOST YOUR MALWARE DEFENSE AND PROTECT YOUR PC**

### **1. Install Antivirus and Antispyware Programs from a Trusted Source**

- Never download anything in response to a warning from a program you didn't install or don't recognize that claims to protect your PC or offers to remove viruses. It is highly likely to do the opposite!
- Get reputable anti-malware programs from a vendor you trust. (Microsoft Security Essentials offers free real-time protection against malicious software for your PC. Or, choose from a list of Microsoft partners who provide anti-malware software). Other reputable defenders include Avast!, McAfee, Kaspersky, Norton's, and AVG.

### **2. Update Software Regularly**

Cybercriminals are endlessly inventive in their efforts to exploit vulnerabilities in software, and many software companies work tirelessly to combat these threats. That is why you should:

- Regularly install updates for all your software, namely your antivirus and antispyware programs, browsers (like Windows Internet Explorer), operating systems (like Windows), and word processing and other programs. Software updates repair vulnerabilities as they are discovered.
- Subscribe to automatic software updates whenever they are offered—for example, you can automatically update all Microsoft software.
- Uninstall software that you don't use. You can remove it using Windows Control Panel.

### **3. Use Strong Passwords and Keep Them Safe**

- Strong passwords are at least 14 characters long and include a combination of letters, numbers, and symbols.
- Don't share passwords with anyone.
- Don't use the same password on all sites. If it is stolen, all the information it protects is also at risk.
- Create different strong passwords for the router and the wireless key of your wireless connection at home. Find out how from the company that provides your router.

### **4. Never Turn Off your Firewall**

A firewall protects networked computers from hostile intrusion. It may be a hardware device or a software program. In either case, it has at least 2 network interfaces – one for the network or computer that it is protecting and one for the network that it is exposed to. Often the case is of a private network/computer and the Internet. A firewall prevents computers outside the protected area from gaining access. Windows Vista, Windows 7, Server 2008 and Linux all make use of software firewalls.



A firewall puts a protective barrier between your computer and the Internet. Turning it off for even a minute increases the risk that your PC will be infected with malware.

## **5. Use Flash Drive with Caution**

Minimize the chance that you'll infect your computer with malware:

- Don't put an unknown flash (or thumb) drive into your PC.
- Hold down the SHIFT key when you insert the drive into your computer. Holding down "Shift" will keep the computer from auto-playing the device. If you forget to do this, click in the upper-right corner to close any flash drive-related pop-up windows.
- Don't open any files on your drive that you're not expecting.

## **Don't be tricked into downloading malware**

Follow this advice:

- Be very cautious about opening attachments or clicking links in email or IM (Instant Messaging), or in posts on social networks (like Facebook)—even if you know the sender. Call to ask if a friend sent it; if not, delete it or close the IM window.
- Avoid clicking "Agree", "OK", or "I Accept" in banner ads, in unexpected pop-up windows or warnings, on websites that may not seem legitimate, or in offers to remove spyware or viruses.
- Instead, press CTRL + F4 on your keyboard. (CTRL + F4 closes the Window)
- If that doesn't close the window, press ALT + F4 on your keyboard to close the browser. If asked, close all tabs and don't save any tabs for the next time you start the browser.
- Only download software from websites you trust. Be cautious of "free" offers of music, games, videos, and the like. They are notorious for including malware in the download.



Self-Check - 2	Written Test
----------------	--------------

**Directions:** Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. Write at least five kinds of protection software available for a single use device

---

---

---

---

---

2. \_\_\_\_\_ is used to prevent, detect, and remove malware, including but not limited to computer viruses, computer worm, trojan horses, spyware and adware.

3. \_\_\_\_\_ are wrong detection by an anti-virus where legitimate files were mistakenly identified as viruses.

4. \_\_\_\_\_ are wrong detection by an anti-virus where legitimate viruses were not detected as viruses.

5. Depending on ***the way they fix destructive software*** these can be in the following forms: \_\_\_\_\_, \_\_\_\_\_, and \_\_\_\_\_ Applications.

6. List and describe the methods antivirus software can use to identify malware.

---

---

---

7. When selecting anti-virus software, there are other aspects to take into consideration such as:

---

---

---



## Answer Sheet

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

Name: \_\_\_\_\_

Date: \_\_\_\_\_

### Short Answer Questions

1. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_
4. \_\_\_\_\_
5. \_\_\_\_\_, \_\_\_\_\_, and \_\_\_\_\_
6. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
7. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_



### **3.1. Firewalls**

A Firewall is a software program that sits between the internet and a private network and works as a barrier to keep destructive viruses away from a computer. The purpose is to prevent unauthorised access into the company by outsiders. Data can only travel from the Internet to the network through the firewall. The software can be configured to accept links only from trusted sites.

The firewall prevents direct communication between computers outside the network (in other words, out on the Internet) and computers on the private network. It also monitors and logs everything passing between the two so as to prevent a hacker or any other unauthorised person from connecting through to your network.

### **3.2. Risks of Allowing Applications Through a Firewall**

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).

When you add an application to the list of allowed applications in a firewall (sometimes called unblocking) or when you open a firewall port, you allow a specific application to send information to or from your PC through the firewall, as though you've drilled a hole in the firewall. This makes your PC less secure and might create opportunities for hackers or malware to use one of those openings to access your files or use your PC to spread malware to other PCs.

Generally, it's safer to add an application to the list of allowed applications than to open a port. A port stays open until you close it, but an allowed application only opens the "hole" when needed.

To help decrease your security risk:

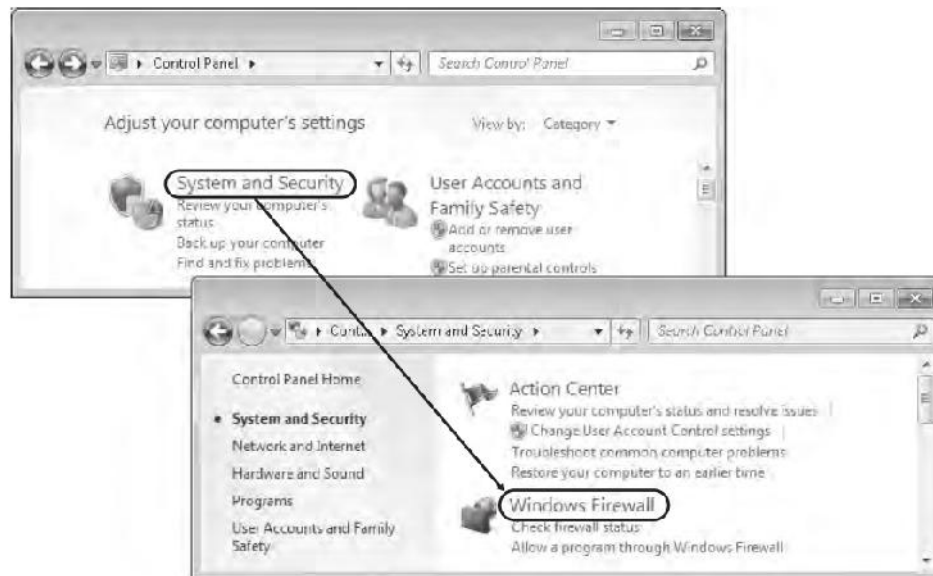
- Only allow an application or open a port when you really need to,
- Never allow an application that you don't recognise to communicate through the firewall.

### **3.3. Configuring Windows Firewall**

Windows Firewall is a host firewall that is built into Windows 7. Unlike firewall devices that control traffic between networks, host firewall define which traffic types are allowed to pass between the local computer and the rest of the network.

You can configure Windows Firewall by using two separate tools.

- If you want to control inbound traffic based on its associated application, use the Windows Firewall page in Control Panel. To open this tool, open Control Panel, click System and Security, and then click Windows Firewall, as shown in Figure 3-1.



**FIGURE 3-1** Accessing Windows Firewall settings in Control Panel



**FIGURE 3-2** Windows Firewall page in Control Panel

- If you want to control outbound traffic, or if you want to control inbound traffic based on additional criteria such as source address or destination port, you need to use the Windows Firewall with Advanced Security (WFAS) console. To open this console, click Advanced Settings on the Windows Firewall page in Control Panel



Self-Check - 3	Written Test
----------------	--------------

**Directions:** Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. \_\_\_\_\_ is a software program that sits between the internet and a private network and works as a barrier to keep destructive viruses away from a computer.

2. There are two ways to allow an application through a firewall. Both of them are risky:

---

---

3. To help decrease your security risk:

---

---

4. If you want to control inbound traffic based on its associated application, use

---

5. If you want to control outbound traffic, or if you want to control inbound traffic based on additional criteria such as source address or destination port, use

---

**Note: Satisfactory rating - 3 points**

**Unsatisfactory - below 3 points**

You can ask your teacher for the copy of the correct answers.



## Answer Sheet

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

Name: \_\_\_\_\_

Date: \_\_\_\_\_

### Short Answer Questions

1. \_\_\_\_\_

2. \_\_\_\_\_  
\_\_\_\_\_

3. \_\_\_\_\_  
\_\_\_\_\_

4. \_\_\_\_\_

5. \_\_\_\_\_





### **4.1. Updating Windows**

Although Windows is designed to minimize security risks out of the box, attackers are constantly developing new security vulnerabilities. To adapt to changing security risks, improve the reliability of Windows, and add support for new hardware, you must deploy updates to your client computers.

In homes and small offices, Windows automatically downloads the newest critical updates from Microsoft, allowing computers to stay up to date without any administrative effort. This approach does not scale to enterprises, which must manage thousands of computers. In enterprises, IT departments need to test updates to ensure that they do not cause widespread compatibility problems. In addition, having each computer download the same update across the Internet would waste your bandwidth, potentially affecting your network performance when Microsoft releases large updates.

Because security threats are evolving constantly, Microsoft must release updates to Windows and other Microsoft software regularly. Deploying and managing these updates are some of the most important security tasks an IT department can perform.

#### **4.1.1. Methods for Deploying Updates**

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.



#### **4.1.2. Windows Update Client**

Whether you download updates from Microsoft or use WSUS, the Windows Update client is responsible for downloading and installing updates on computers running Windows 7 and Windows Vista. The Windows Update client replaces the Automatic Updates client available in earlier versions of Windows. Both Windows Update in Windows 7 and Automatic Updates in earlier versions of Windows operate the same way: they download and install updates from Microsoft or an internal WSUS server. Both clients install updates at a scheduled time and automatically restart the computer if necessary. If the computer is turned off at that time, the updates can be installed as soon as the computer is turned on. Alternatively, Windows Update can wake a computer from sleep and install the updates at the specified time if the computer hardware supports it.

The Windows Update client provides for a great deal of control over its behavior. You can configure individual computers by using the Control Panel\System and Security\Windows Update\Change Settings page.

After the Windows Update client downloads updates, the client checks the digital signature and the Secure Hash Algorithm (SHA1) hash on the updates to verify that they have not been modified after they were signed by Microsoft. This helps mitigate the risk of an attacker either creating malware that impersonates an update or modifying an update to add malicious code.

#### **4.1.3. How to Check Update Compatibility**

Microsoft performs some level of compatibility testing for all updates. *Critical updates* (small updates that fix a single problem) receive the least amount of testing because they occur in large numbers and they must be deployed quickly. Service packs (large updates that fix many problems previously fixed by different critical updates) receive much more testing because they are released infrequently.

Whether you are planning to deploy critical updates or a service pack, you can reduce the chance of application incompatibility by testing the updates in a lab environment. Most enterprises have a Quality Assurance (QA) department that maintains test computers in a lab environment with standard configurations and applications. Before approving an update for deployment in the organization, QA installs the update on the test computers and verifies that critical applications function with the update installed.

Whether you have the resources to test updates before deploying them, you should install updates on pilot groups of computers before installing the updates throughout your organization. A pilot group is a small subset of the computers in your organization that receive an update before wider deployment. Ideally, pilot groups are located in an office with strong IT support and have technology-savvy users. If an update causes an application



compatibility problem, the pilot group is likely to discover the incompatibility before it affects more users.

#### **4.1.4. How to Install Updates**

Ideally, you would deploy new computers with all current updates already installed. After deployment, you can install updates manually, but you'll be much more efficient if you choose an automatic deployment technique. For situations that require complete control over update installation but still must be automated, you can script update installations.

#### **4.1.5. How to Verify Updates**

Microsoft typically releases updates once per month. If a computer does not receive updates, or the updates fail to install correctly, the computer might be vulnerable to security exploits that it would be protected from if the updates were installed. Therefore, it's critical to the security of your client computers that you verify updates are regularly installed.

#### **4.1.6. How to Remove Updates**

Occasionally, an update might cause compatibility problems. If you experience problems with an application or Windows feature after installing updates and one of the updates was directly related to the problem you are experiencing, you can uninstall the update manually to determine whether it is related to the problem.

If removing the update does not resolve the problem, you should reapply the update. If removing the update does solve the problem, inform the application developer (in the case of a program incompatibility) or your Microsoft support representative of the incompatibility. The update probably fixes a different problem, so you should make every effort to fix the compatibility problem and install the update.

### **4.2. Updating Anti-Virus Software**



Self-Check - 4	Written Test
----------------	--------------

**Directions:** Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. Although Windows is designed to minimize security risks out of the box, attackers are constantly developing \_\_\_\_\_.
2. To adapt to \_\_\_\_\_, \_\_\_\_\_, and \_\_\_\_\_, you must deploy updates to your client computers.
3. Because \_\_\_\_\_ are evolving constantly, Microsoft must release updates to Windows and other Microsoft software regularly.
4. list and explain techniques for applying updates provided by Microsoft:
  - \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
  - \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
  - \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
5. \_\_\_\_\_ (small updates that fix a single problem) receive the least amount of testing because they occur in large numbers and they must be deployed quickly.
6. \_\_\_\_\_ (large updates that fix many problems previously fixed by different critical updates) receive much more testing because they are released infrequently.

**Note: Satisfactory rating - 3 points**

**Unsatisfactory - below 3 points**

You can ask your teacher for the copy of the correct answers.



## Answer Sheet

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

Name: \_\_\_\_\_

Date: \_\_\_\_\_

### Short Answer Questions

1. \_\_\_\_\_

2. \_\_\_\_\_, \_\_\_\_\_, and \_\_\_\_\_,

3. \_\_\_\_\_

4.

- \_\_\_\_\_

---

---

---

---

- \_\_\_\_\_

---

---

---

---

- \_\_\_\_\_

---

---

---

---

5. \_\_\_\_\_

6. \_\_\_\_\_

## 5.1. Internet Security

We have already discussed some of the functionality of anti-virus and firewall software when it comes to protecting your computer network. Since many of these threats come from the Internet, many web browsing software programs contain inbuilt security settings which allow you to restrict or block access to sites before they can become a problem.

In Microsoft Internet Explorer, security is handled by division of sites into restricted zones. This means that different web sites can have different security levels.

There are four Internet Security Zones, and within each zone a different security level can be set.

### 5.1.1. Security Zones

You can tell which zone the current Web page is in by looking at the right side of the Internet Explorer status bar. Whenever you open or download content from the Web, Internet Explorer checks the security settings for that Web site's zone.

- Search for and view any website.
- Look at the bottom right of the screen:

We will access a screen in Internet Explorer which explains these zones, and where you can make changes to the zone settings.

### 5.1.2. Viewing Security Zones

If you are on a PC where changes can be made, you change the Internet Zones through **Tools, Internet Options, Security**

- Choose Tools, Internet Options.
- Click on the Security tab.

The top of the dialog box displays the four available security zones. The remainder of the dialog box allows you to choose a security level for that zone.



**Figure 5-1** The Internet zone with medium security level



## 5.2. Different Security Zones

There are four different 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.

Settings can be customized within a zone from Low, Medium Low, Medium, and High. If you are in a workplace or college, these security decisions have probably been made for you and it is unlikely that you can change these. However for the purposes of this exercise, we will view the different zones and their security settings.



Self-Check - 5	Written Test
----------------	--------------

**Directions:** Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. In \_\_\_\_\_, security is handled by division of sites into restricted zones. This means that different web sites can have different security levels.
2. List and describe the four Internet Security Zones

- \_\_\_\_\_:  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
- \_\_\_\_\_:  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
- \_\_\_\_\_:  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
- \_\_\_\_\_:  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

3. Internet Security Zones Settings can be customized within a zone from \_\_\_\_\_, \_\_\_\_\_, \_\_\_\_\_, and \_\_\_\_\_.





## Answer Sheet

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

Name: \_\_\_\_\_

Date: \_\_\_\_\_

### Short Answer Questions

1. \_\_\_\_\_,

2.

- \_\_\_\_\_:

---

---

---

- \_\_\_\_\_:

---

---

---

- \_\_\_\_\_:

---

---

---

- \_\_\_\_\_:

---

---

---

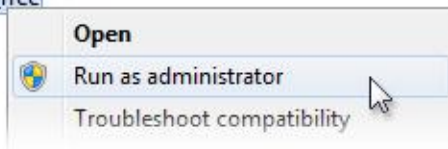
3. \_\_\_\_\_, \_\_\_\_\_, \_\_\_\_\_, and \_\_\_\_\_.

## Operation Sheet - 1

## Installing Avast! Free Antivirus

To prevent Avast! Free Antivirus from being incorrectly installed or aborted unexpectedly. When you are ready, proceed as follows:

1. Firstly download the Avast! Free Antivirus from the Avast! Website and save it to your computer, in a location where you will easily be able to locate it. For example save the downloaded setup file `avast_free_antivirus_setup.exe` on your Windows Desktop.
2. Locate the downloaded setup file `avast_free_antivirus_setup.exe` (depending on your system preferences, the file extension may be hidden), on your Windows Desktop for example. Now, in case you are logged in to:



- Windows 7 or Windows Vista as a user with administrator permissions, right-click on the setup file and choose 'Run as administrator' from the context menu,
- Windows XP as Administrator or as a user with administrator

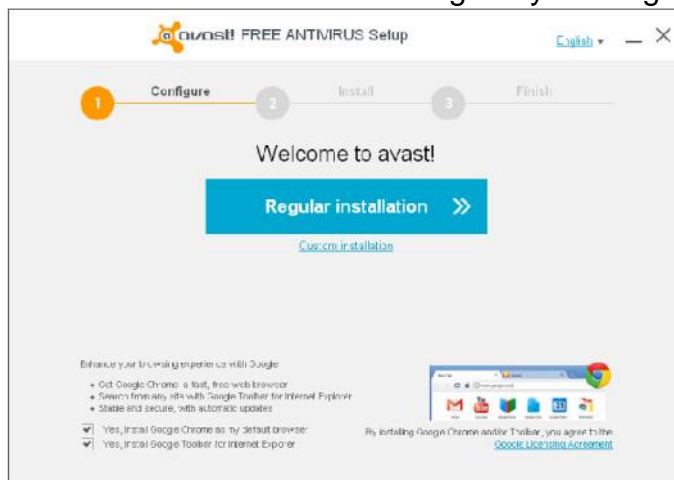
permissions, or you are logged in to Windows 7 or Windows Vista as Administrator (i.e. not a user with administrator permissions), double-click the setup file to begin the installation process,

If prompted by User Account Control dialog for permissions, click 'Yes' (or 'Continue' in Windows Vista) to begin the installation process.

For a few seconds you will briefly see the setup process copy the installation files to your computer.



When Avast! Setup Wizard starts you will see a welcome screen. Preferred language for the installation can be changed by clicking on the current language shown on the top right corner. Before continuing with the installation of Avast! Free Antivirus please read the User License Agreement.



At the bottom of the welcome screen you can choose whether you wish to install Google Chrome. By ticking the checkbox 'Make Google Chrome my default browser', you can also select, if it should be opened as your default



web browser when accessing the Internet. For details, please read enclosed Terms of Use and Privacy Policy.

Then choose what type of installation you prefer:

➤ **Regular Install or Custom Install**

***Regular Installation of Avast! Free Antivirus***

1. Click the 'Regular Installation' button in the middle of the welcome screen to proceed with default installation of Avast! Free Antivirus in preferred language and with minimal user interaction during the setup process.
2. You will now be prompted to Accept the End User License Agreement by Clicking on the 'Continue' button.
3. The Avast! Setup Wizard will create a system restore point, then will display an installation progress bar,




4. When

installation has successfully completed click 'Done'. Now Avast Free Antivirus will perform a quick scan of your system. Depending upon the speed of your machine, it may take a few minutes to complete.

Avast! Free Antivirus is now installed on your computer and ready to use. But it works for 30 days in trial mode after installation. During this period you need to register to get your free license key to continue to use it and stay protected.



Avast! User interface is accessible via orange ball icon  in your system tray or orange shortcut icon on your Windows Desktop.



## Operation Sheet - 2

## Running and Scheduling Avast! Free Antivirus





LAP Test	Practical Demonstration
----------	-------------------------

Name: \_\_\_\_\_ Date: \_\_\_\_\_

Time started: \_\_\_\_\_ Time finished: \_\_\_\_\_

**Instructions:** Given necessary templates, tools and materials you are required to perform the following tasks within --- hour.



## List of Reference Materials



# **INFORMATION TECHNOLOGY SUPPORT SERVICE**

**Level - I**

## **LEARNING GUIDE 35**

<b>Unit of Competence:</b>	<b>Protect Application or System Software</b>
<b>Module Title:</b>	<b>Protecting Application or System Software</b>
<b>LG Code:</b>	<b>ICT ITS1 M09 LO3 – LG35</b>
<b>TTLM Code:</b>	<b>ICT ITS1 TTLM 1019v1</b>

**LO 3: Identify and Take Action to  
Stop Spam**





## Instruction Sheet

## Learning Guide 35

This learning guide is developed to provide you the necessary information regarding the following content coverage and topics –

- Define and Identify common types of spam
- Spam Control and combat
- Configure and use spam filters
- Report spam

This guide will also assist you to attain the learning outcome stated in the cover page. Specifically, upon completion of this Learning Guide, you will be able to –

- Define and Identify common types of **spam**
- Take **appropriate action** in order to protect unauthorized access of spammers
- Configure and use spam filters
- Report and document spam to identify the security threats and be able to perform recommended action

Learning Instructions:

1. Read the specific objectives of this Learning Guide.
2. Follow the instructions described below 3 to 6.
3. Read the information written in the information “Sheet 1 and Sheet 2” in page 3 and 9 respectively.
4. Accomplish the “Self-check 1 and Self-check 2” in page 7 and 12 respectively
5. If you earned a satisfactory evaluation from the “Self-check” proceed to “Operation Sheet 1, Operation Sheet 2 and Operation Sheet 3” in page 23
6. Do the “LAP test” in page



### 1.1. Definition of Spam

Spam is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately. It is the electronic equivalent of receiving “junk” mail in your letter box. While the most widely recognized form of spam is **e-mail spam**, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam and file sharing network spam.

Spamming is economically viable to advertisers because their operating costs are so low, and it is difficult to hold senders accountable for their mass mailings. Spam can be used to spread computer viruses, Trojan horses or other malicious software. The objective may be identity theft, or worse. Some spam attempts to capitalize on human greed whilst other attempts to use the victims' inexperience with computer technology to trick them (phishing).

Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it.

Most spam is **commercial advertising**, often for dubious products, get-rich-quick schemes, or quasi-legal services. Spam costs the sender very little to send -- most of the costs are paid for by the recipient or the carriers rather than by the sender.

### 1.2. Types of Spam

There are **four common types of spam**, and they have different effects on users.

#### 1.2.1. Cancellable Usenet spam

Cancellable Usenet spam is a single message sent to 20 or more Usenet newsgroups. (Through long experience, Usenet users have found that any message posted to so many newsgroups is often not relevant to most or all of them.) Usenet spam is aimed at “**lurkers**”, people who read newsgroups but rarely or never post and give their address away. Usenet spam robs users of the utility of the newsgroups by overwhelming them with a barrage of advertising or other irrelevant posts. Furthermore, Usenet spam subverts the ability of system administrators and owners to manage the topics they accept on their systems.

#### 1.2.2. Email Spam

Email spam targets individual users with direct mail messages. Email spam lists are often created by scanning Usenet postings, stealing Internet mailing lists, or searching the Web for addresses. Email spams typically cost users money out-of-pocket to receive. Many people - anyone with measured phone service - read or receive their mail while the meter is running, so to speak. Spam costs them



additional money. On top of that, it costs money for ISPs and online services to transmit spam, and these costs are transmitted directly to subscribers.

One particularly **nasty variant of email spam is sending spam to mailing lists (public or private email discussion forums.)** Because many mailing lists limit activity to their subscribers, spammers will use automated tools to subscribe to as many mailing lists as possible, so that they can grab the lists of addresses, or use the mailing list as a direct target for their attacks.

### 1.2.3. Instant Messaging Spam

Some examples of instant messengers are Yahoo! Messenger, AIM, Windows Live Messenger, Tencent QQ, ICQ, XMPP and Myspace chat rooms. All are targets for spammers. Many IM systems offer a directory of users, including demographic information such as age and sex. Advertisers can gather this information, sign on to the system, and send unsolicited messages, which could include commercial scam-ware, viruses, and links to paid links for the purpose of **click fraud**. Microsoft announced that the Windows Live Messenger version 9.0 would support specialized features to combat messaging spam. In most systems users can already block the vast majority of spam through the use of a **whitelist**. Whitelisting is the act of authorising contact.

### 1.2.4. SMS & MMS Spam

SMS (Short Messaging Service) is a mechanism which allows brief text messages to be sent to a mobile phone. MMS (Multimedia Messaging Service) can include including videos, pictures, text pages and sound.

Mobile phone spam is a form of spamming directed at these messaging services of mobile telephony. It is described as mobile spamming, SMS spam, text spam, or SpaSMS but is most frequently referred to as m-spam. These types of spam can be particularly annoying for the recipient because, unlike email, some recipients may be charged a fee for every message received, including spam!

## 1.3. Reasons Make Spam Bad

Why do we get so upset when we receive E-mail which was not requested?

There are several reasons:

- **The Free Ride.** E-mail spam is unique in that the [receiver pays](#) so much more for it than the sender does. For example, AOL has said that they were receiving 1.8 million spams from Cyber Promotions per day until they got a court injunction to stop it. Assuming that it takes the typical AOL user only 10 seconds to identify and discard a message, that's still 5,000 hours per day of connect time per day spent discarding their spam, just on AOL. By contrast, the spammer probably has a T1 line that costs him about \$100/day. No other kind of advertising costs the advertiser so little and the recipient so much. The



closest analogy I can think of would be auto-dialing junk phone calls to cellular users (in the US, cell phone users pay to receive as well as originate calls); you can imagine how favorably that might be received.

- **The “Oceans of Spam” Problem.** Many spam messages say “please send a REMOVE message to get off our list.” Even disregarding the question of why you should have to do anything to get off a list you never asked to join, this becomes completely impossible if the volume grows. At the moment, most of us only get a few spams per day. But imagine if only 1/10 of 1 % of the users on the Internet decided to send out spam at a moderate rate of 100,000 per day, a rate easily achievable with a dial-up account and a PC. Then everyone would be receiving 100 spams every day. If 1% of users were spamming at that rate, we’d all be getting 1,000 spams per day. Is it reasonable to ask people to send out 100 “remove” messages per day? Hardly. **If spam grows, it will crowd our mailboxes to the point that they’re not useful for real mail.** Users on AOL, which has a lot of trouble with internal spammers, report that they’re already nearing this point.
- **The Theft of Resources.** An increasing number of spammers, such as **Quantum Communications**, send most or all of their mail via innocent intermediate systems, to avoid blocks that many systems have placed against mail coming directly from the spammers’ systems. (Due to a historical quirk, most mail systems on the Internet will deliver mail to anyone, not just their own users.) This fills the intermediate systems’ networks and disks with unwanted spam messages, takes up their managers’ time dealing with all the undeliverable spam messages, and subjects them to complaints from recipients who conclude that since the intermediate system delivered the mail, they must be in league with the spammers.

Many other spammers use “**hit and run**” spamming in which they **get a trial dial-up account at an Internet provider for a few days, send tens of thousands of messages, then abandon the account** (unless the provider notices what they’re doing and cancels it first), leaving the unsuspecting provider to clean up the mess. Many spammers have done these tens or dozens of times, forcing the providers to waste staff time both on the cleanup and on monitoring their trial accounts for abuse.

- **It’s All Garbage.** The spam messages I’ve seen have almost without exception advertised stuff that’s **worthless**, deceptive, and partly or entirely fraudulent. (I include the many MLMs in here, even though the MLM-ers rarely understand why there’s no such thing as a good MLM). It is spam software, funky miracle cures, off-brand computer parts, vaguely described get rich quick schemes, dial-a-porn, and so on downhill from there. It’s all stuff that’s too cruddy to be worth advertising in any medium where they’d actually have to pay the cost of the ads. Also, since the cost of spamming is so low, there’s no point in targeting



your ads, when for the same low price you can send the ads to everyone, increasing the noise level the rest of us have to deal with.

- **They're Crooks.** Spam software invariably comes with a list of names falsely claimed to be of people who've said they want to receive ads, but actually consisting of **unwilling victims culled at random from usenet or mailing lists**. Spam software often promises to run on a provider's system in a way designed to be hard for the provider to detect so they can't tell what the spammer is doing. Spams invariably say they'll remove names on request, but they almost never do. Indeed, people report that when they send a test "remove" request from a newly created account, they usually start to receive spam at that address.

Spammers know that **people don't want to hear from them**, and generally **put fake return addresses** on their messages so that they don't have to bear the cost of receiving responses from people to whom they've send messages. Whenever possible, they use the "**disposable**" **trial ISP accounts** mentioned above so the ISP bears the cost of cleaning up after them. It's hard to think of **another line** of business where the **general ethical level is so low**.

- **It Might Be Illegal.** Some kinds of spam are illegal in some countries on the Internet. Especially with **pornography**, mere possession of such material can be enough to put the recipient in jail. In the United States, child pornography is highly illegal and we've already seen spammed child porn offers.



Self-Check - 1	Written Test
----------------	--------------

**Directions:** Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. \_\_\_\_\_ is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately.

2. List and explain the four common types of spam

1. \_\_\_\_\_

---

---

---

2. \_\_\_\_\_

---

---

---

3. \_\_\_\_\_

---

---

---

4. \_\_\_\_\_

---

---

---

3. Why do we get so upset when we receive E-mail which was not requested?

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_



## Answer Sheet

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

Name: \_\_\_\_\_

Date: \_\_\_\_\_

### Short Answer Questions



## 2.1. Spam Control

**Spam** is flooding the Internet with many copies of the same message, in a Spam now constitutes an overwhelming majority of **email traffic**.

### 2.1.1. The Effects of Spam

The never-ending onslaught of junk messages:

- Strains networks
- Erodes user productivity
- Propagates dangerous malware and costs business millions of dollars.

### 2.1.2. Types of Spam

Though all junk email might look the same, spam continues to arrive in a seemingly endless number of configurations, ranging from the innocuous to the lethal. The major spam types include:

- **Advertising Spam:** is used to promote an entire spectrum of products and services, from software to real estate to questionable medical and nutritional offerings.
- **Malware Delivery:** Spam is one of the main distribution channels for delivering viruses and other types of malware. Targeted individuals, believing they have received an important document or media file, are often tricked into opening a malware attachment.
- **Scams:** Posing as Nigerian princes, Swiss bankers, tragically ill children and other stock types, scammers prey on recipients' sympathy and greed.
- **Phishing:** Hiding behind the names of respected retailers, financial institutions, businesses, charities and government bodies. **Phishers** attempt to lure unsuspecting recipients to bogus Web sites where they steal personal financial or identity information.
- **Nonsense:** A significant chunk of junk-mail text is pure gibberish. Some of this material is generated in an effort to trick **spam-filtering technologies** into passing an attached message onto recipients. Many nonsensical messages seem to exist for no purpose at all.

### 2.1.3. Spam Media

Spam is overwhelmingly an [email](#) problem. Yet as Internet technology advances, junk content is rapidly spilling over to many other types of IP media, including:

- **IM (instant messaging)** : Spam is a growing problem on [IM](#) networks, where the threats closely parallel those of email spam.





- **VoIP** Voice over IP: SPIT (Spam over Internet Telephony) is a rare but potentially dangerous form of spam that threatens to annoy users and jam voice-mail inboxes.
- **Search Engines:** Using techniques such as hidden text, doorway pages and mirror sites, a search-engine spammer attempts to boost a Web site's ranking by redirecting traffic to the site. This practice is also known as "spamdexing."
- **Web Message Boards:** Spammers like to use Web message boards and Usenet.com groups to promote products and services that are usually unrelated to the site's content focus.
- **Blogs:** Junk advertising is inserted into a blog's reader-comment area.
- **Online Video:** YouTube LLC and other video-sharing sites are plagued by video spam, which consists of thinly disguised commercials for products and services of dubious value.

## 2.2. Combating Spam

It sometimes seems as if **anti-spam technologies** and methodologies are proliferating as rapidly as spam itself. These are the main tools that can keep spam under control:

- **Spam Filters:** A growing number of technology vendors are targeting spam with products that are designed to block and quarantine suspected spam. These offerings use sophisticated algorithms to scan each incoming message for signs that it may contain spam.
- **Firewalls:** **Spam firewalls** offload message filtering from the email server, freeing up network resources and bandwidth. Spam-firewall appliances usually come preconfigured and can be set up in minutes. Maintenance is usually minimal.
- **Anti-Malware Technologies:** Hardware- and software-based anti-malware products can block dangerous attachments from reaching employees' inboxes.
- **Client Control:** Leading email clients, such as Microsoft Outlook and Outlook Express, as well as Mozilla Foundation's Thunderbird, offer built-in controls that are designed to minimize inbox spam.
- **White Lists/Black Lists:** This feature is found in many spam filters and client controls. White lists of trusted email addresses allow messages to proceed to the user's inbox unimpeded by any filter or client settings. Black lists work in the opposite way, routinely blocking incoming email from known offenders.
- **Disposable Email Addresses:** Many businesses and individuals routinely distribute different email addresses to every external contact, then funnel all incoming messages into a single account. This way, if one address begins spamming, it can be safely eradicated without affecting the flow of messages originating from other contacts.



- **Legal Action** : While it's rare for an individual business to sue a junk-mail sender, a growing number of law-enforcement bodies are targeting spammers, particularly organized crime rings that use the technology for financial and identity theft.
- **Policies**: All businesses need a comprehensive anti-spam policy. Besides mandating the use of filtering and other good spam-fighting technologies, the policy should cover routine workplace practices. **Business Web sites, for example, should never publish visible email addresses that can be "harvested" by spammer software.** Employees should also be encouraged not to post business email addresses on message boards, social-network sites and personal Web pages.
- **Education**: The simple task of teaching employees to be wary of phishing messages, and not to open unknown attachments, can help any business minimize spam's impact.

### 2.3. 12 Tips for Fighting Spam

Fighting spam involves diligence in using anti-malware applications and keeping them, your operating system and applications updated, as you will see:-

- Use filtering software - Most e-mail programs have an automatic spam filtering function. Internet service providers can also install mail filters in their mail transfer agents as a service to all of their customers. Due to the growing threat of fraudulent websites, Internet service providers filter URLs in email messages to remove the threat before users click. Corporations often use filters to protect their employees and their information technology assets. There are 3rd party spam filters available as well – among them SpamAssassin and Norton Internet Security.
- Install anti-virus software and keep it updated
- Use a personal firewall – available in Windows and Mac Operating Systems
- Download security patches – these address known issues as they come to hand
- Choose long and random passwords that involve letters, numbers and symbols
- Protect your email address
  - ✓ Be careful about to whom you give your email address.
  - ✓ When it is necessary to forward messages to bulk recipients who don't know one another, it is good practice to list the recipient names in the "BCC:" field instead of after "TO:". Unscrupulous recipients will not be able to see or copy that list of email addresses.
  - ✓ Avoid responding to spam; even be careful about “unsubscribe” in a suspect email.
  - ✓ Beware of contact forms on websites, they may be harvesting your details, nor can you see the address you are sending to in some cases.



- ✓ Using HTML in email allows web browser functionality such as the display of html, URLs and images. Mail clients which do not automatically download and display HTML, images or attachments, have fewer risks, as do clients who have been configured to not display these by default.
- Protect your mobile phone number
  - ✓ A helpful SMS spam-reduction technique is guarding one's mobile phone number. One of the biggest sources of SMS spam is number harvesting carried out by Internet sites offering "free" ring tone downloads. In order to facilitate the download, users must provide their phones' numbers; which in turn are used to send frequent advertising messages to the phone.
  - ✓ Another countermeasure is to use a service that provides a public phone number and publishes the SMS messages received at that number to a publicly accessible website. Google Voice can be used in this way, but with numbers and messages kept private. (At the time of writing Google Voice is not fully operational in Australia.
- Read terms and conditions carefully - Often the terms and conditions will contain a clause that reveals the intent to put a user's contact details into a mailing list.
- Beware of email scams and fraud –
- Don't open suspicious attachments
- Don't "unsubscribe" if the source seems dubious. Just delete it. The unsubscribe link or button may simply confirm the validity of your contact details.
- Report any email, instant messaging, SMS and MMS spam to the concerned body



Self-Check - 2	Written Test
----------------	--------------

**Directions:** Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. List The Effects of Spam

---

---

---

2. List and explain Spam Media

---

---

---

---

---

---

3. list and describe the main tools that can keep spam under control:

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---



## Answer Sheet

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

Name: \_\_\_\_\_

Date: \_\_\_\_\_

### Short Answer Questions



### 3.1. Anti-Spam Techniques

Various anti-spam techniques are used to prevent email spam (unsolicited bulk email).

No technique is a complete solution to the spam problem, and each has trade-offs between incorrectly rejecting legitimate email (false positives) as opposed to not rejecting all spam (false negatives) – and the associated costs in time, effort, and cost of wrongfully obstructing good mail.

Anti-spam techniques can be broken into four broad categories:

- **End-User Techniques:** those that require actions by individuals,
- **Automated techniques for email administrators:** those that can be automated by email administrators,
- **Automated techniques for email senders:** those that can be automated by email senders and
- Those employed by researchers and law enforcement officials.

#### 3.1.1. End-User Techniques

There are a number of techniques that individuals use to restrict the availability of their email addresses, with the goal of reducing their chance of receiving spam.

- Discretion
- Address Munging
- Avoid Responding to Spam
- Contact Forms
- Disable HTML in Email
- Disposable Email Addresses
- Ham Passwords
- Reporting Spam

#### 3.1.2. Automated Techniques for Email Administrators

There are now a large number of applications, appliances, services, and software systems that email administrators can use to reduce the load of spam on their systems and mailboxes. In general these attempt to reject (or "block"), the majority of spam email outright at the SMTP connection stage. If they do accept a message, they will typically then analyze the content further – and may decide to "quarantine" any categorized as spam.

- Authentication
- Challenge/Response Systems
- Checksum-Based Filtering
- Country-Based Filtering
- DNS-Based Blacklists



- URL Filtering
- Strict Enforcement of RFC Standards
  - ✓ *Greeting delay.*
  - ✓ *Temporary rejection*
  - ✓ *HELO/EHLO checking*
  - ✓ *Invalid pipelining*
  - ✓ *Nolisting*
  - ✓ *Quit detection*
- Honeypots
- Hybrid Filtering
- Outbound Spam Protection
- PTR/Reverse DNS Checks
- Rule-Based Filtering
- SMTP Callback Verification
- SMTP Proxy
- Spamtrapping
- Statistical Content Filtering
- Tarpits

### 3.1.3. Automated Techniques for Email Senders

There are a variety of techniques that email senders use to try to make sure that they do not send spam. Failure to control the amount of spam sent, as judged by email receivers, can often cause even legitimate email to be blocked and for the sender to be put on DNSBLs.

- Background Checks on New Users and Customers
- Confirmed Opt-In for Mailing Lists
- Egress Spam Filtering
- Limit Email Backscatter
- Port 25 Blocking
- Port 25 Interception
- Rate Limiting
- Spam Report Feedback Loops
- FROM Field Control
- Strong AUP and TOS Agreements



## **3.2. Managing SPAM**

There are a number of ways that SPAM and other email threats can be managed. Most anti-virus software programs contain some sort of SPAM management functionality as well as most Email programs. In the following pages, we will demonstrate the email management processes of Microsoft Outlook 2010.

### **3.2.1. Managing Junk Email**

As SPAM or other unsolicited Emails are received, Outlook 2010 allows us to block or quarantine the sender so as to remove our exposure to risk or annoyance in future.

### **3.2.2. Automatic blocking**

Unfortunately, the lovely folk who like to send us message after message about cheap pharmaceuticals do not always use the same address. So we block one, another appears in our inbox. To counter this, we can set up some automatic blocking processes to block emails by type rather than sender.





Self-Check - 3	Written Test
----------------	--------------

**Directions:** Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. List the four broad categories anti-spam techniques:

---

---

---

---

2. List the techniques that individuals use to restrict the availability of their email addresses, with the goal of reducing their chance of receiving spam.

---

---

---

---

---

---

---

---

3. List the techniques that email senders use to try to make sure that they do not send spam.

---

---

---

---

---

---

---

---



## Answer Sheet

Score = \_\_\_\_\_

Rating: \_\_\_\_\_

Name: \_\_\_\_\_

Date: \_\_\_\_\_

### Short Answer Questions



#### **4.1. Junk Email**

Like everything, there are a number of risks that go with having your own email address. As you give your email address to others, use it online to purchase items or use it as a contact point for entry into competitions, you open yourself up to a bombardment of "Junk" email.

Junk email can include:

- Subscriptions to company information sites and online brochures (the online version of junk mail).
- Spam - A process for sending unsolicited messages (usually for cheap online pharmaceuticals, scams or x rated sites) to many recipients at once. SPAM covers emails, instant messaging, SMS and other mobile phone messaging.
- Distribution of malicious software such as viruses.
- Hoax emails (such as emails requesting online banking details etc.).

#### **4.2. Legal Countermeasures**

If an individual or organization can identify harm done to them by spam, and identify who sent it; then they may be able to sue for a legal remedy, e.g on the basis of trespass to chattels. A number of large civil settlements have been won in this way, although others have been mostly unsuccessful in collecting damages.

Criminal prosecution of spammers under fraud or computer crime statutes is also common, particularly if they illegally accessed other computers to create botnets, or the emails were phishing or other forms of criminal fraud.

Finally, in most countries specific legislation is in place to make certain forms of spamming a criminal offence, as outlined below:

- **European Union**

Article 13 of the European Union Directive on Privacy and Electronic Communications (2002/58/EC) provides that the EU member states shall take appropriate measures to ensure that unsolicited communications for the purposes of direct marketing are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.

In the United Kingdom, for example, unsolicited emails cannot be sent to an individual subscriber unless prior permission has been obtained or unless there is a pre-existing commercial relationship between the parties.

- **United States**

In the United States, many states enacted anti-spam laws during the late 1990s and early 2000s. All of these were subsequently superseded by the CAN-SPAM



Act of 2003, which was in many cases less restrictive; and any further potential state laws preempted. However, CAN-SPAM leaves intact laws not specific to e-mail. Courts have ruled that spam is, e.g., Trespass to Chattel.

Bulk commercial email does not violate CAN-SPAM, provided that it meets certain criteria, e.g., a truthful subject line, no forged information in the headers. If it fails to comply with any of these requirements it is illegal. Those opposing spam greeted the new law with dismay and disappointment, almost immediately dubbing it the "You Can Spam" Act.

In practice it had little positive impact. In 2004, less than one percent of spam complied with CAN-SPAM, although a 2005 review by the Federal Trade Commission claimed that the amount of sexually explicit spam had significantly decreased since 2003 and the total volume had begun to level off. Many other observers viewed it as having failed, although there have been several high-profile prosecutions.

- **Australia SPAM Act 2003**

As a result of increasing instances of unsolicited bulk email flooding company and personal networks, the Australian Federal Government introduced the SPAM Act. The Spam Act became law on 12 December 2003 and, after a grace period; all provisions of the Spam Act came into effect from 10 April 2004 and covers the following message types:

- Email
- Short message service (SMS)
- Multimedia message service (MMS)
- Instant messaging (IM)

In simple terms, the SPAM Act covers the following:

1. Unsolicited commercial electronic messages must not be sent. Messages should only be sent to an address when it is known that the person responsible for that address has consented to receive it.
2. Businesses must not use electronic address harvesting software. or lists which have been generated using such software, for the purpose of sending unsolicited commercial electronic messages.
3. Commercial electronic messages must contain
  - Accurate information about the sender of the message;
  - A functional way for the message's recipients to indicate that they do not wish to receive such messages in the future - that they wish to unsubscribe.

The maximum penalties under the Spam Act include a range of warning and breach options up to a Court imposed penalty of up to \$220,000 for a single day's contraventions up to \$1.1 million for a second offence.



### 4.3. Reporting SPAM

Tracking down a spammer's ISP and reporting the offense can lead to the spammer's service being terminated and criminal prosecution. Unfortunately, it can be difficult to track down the spammer, and while there are some online tools such as SpamCop and Network Abuse Clearinghouse to assist, they are not always accurate. Historically, reporting spam in this way has not played a large part in abating spam, since the spammers simply move their operation to another URL, ISP or network of IP addresses.

In many countries consumers may also forward unwanted and deceptive commercial email to the authorities, e.g. in the US to the email address (spam at uce.gov) maintained by the US Federal Trade Commission (FTC), or similar agencies in other countries.

Emails inundated with SPAM or other unsolicited messages such as hoax emails, they can report it to the Australian Communications and Media Authority by undertaking any of the following

Users forward spam to the ACMA's Spam Intelligence Database using report@submit.spam.acma.gov.au email address.

Note: When forwarding an email message, please do not change the subject line of the message or add additional text. The ACMA will only contact you in relation to a report if it requires further information to assist it in its anti-spam activities.

- Organisations, such as Internet Service Providers or universities, which collect large amounts of spam associated with the management of their email systems can be report to the ACMA via command-line or batch reporting.
- Spam SMS messages can be forwarded to a dedicated telephone number 0429 999 888 to report it directly to the ACMA. Your report will be recorded in the ACMA's database and used to monitor SMS spam activity.



## Operation Sheet - 1

## Filter Incoming Messages in Windows Live

To organize your Inbox by creating filters to direct incoming messages to specific folders, follow these steps:

1. Sign in to the **Windows Live Hotmail** website with your **Windows Live Hotmail account**.
2. In the upper-right corner of the page, click **Options**, and then click **More options**.
3. Under Customize your mail, Click **Automatically sort e-mail into folders**.
4. Perform one of the actions as per your requirement:
5. Click **New filter** to Create a new filter
6. Click **Edit** next to the filter that you want to edit.
7. Click **Delete** next to the filter that you want to delete.
8. Follow the **on-screen instructions** to specify which messages you want to filter and where you want to filter them, and then click **Save**.



## List of Reference Materials

[http://www.bukisa.com/articles/345103\\_how-to-configure-spam-filter-in-microsoft-outlook#ixzz1CfEcieYW](http://www.bukisa.com/articles/345103_how-to-configure-spam-filter-in-microsoft-outlook#ixzz1CfEcieYW)

[www.acma.gov.au](http://www.acma.gov.au)

<http://www.google.com/googlevoice/about.html>

[www.scamwatch.gov.au](http://www.scamwatch.gov.au)



## LO1 - ANSWER KEYS:

### SELF CHECK 1:

1. A user account
2. A standard user account
3. An administrator account
4. A guest account
5. User profile
6. Authentication
7. The authorization process
8. Username and Password method.
9. The standard account can help protect your computer by preventing users from making changes that affect everyone who uses the computer, such as deleting files that are required for the computer to work. We recommend creating a standard account for each user.

When you are logged on to Windows with a standard account, you can do almost anything that you can do with an administrator account, but if you want to do something that affects other users of the computer, such as installing software or changing security settings, Windows might ask you to provide a password for an administrator account.

10. Authentication methods used to authenticate users
  - **Username with static passwords** - the password stays the same until changed by the user at some time
  - **Usernames with dynamic passwords** - the password is constantly changed by a password generator synchronized with the user and system.
  - **Other challenge response systems** - this may involve PINs, questions to the user requiring various answers or actions
  - **Certificate Based** - this requires the user to have an electronic certificate or token. This may also need to be digitally signed by a trusted authority.
  - **Physical devices** - these include the use of smartcards and biometrics.

Generally the entire authentication process occurs on
11. User Account Control



## LO1 - ANSWER KEYS:



12. When your permission or password is needed to complete a task, UAC will notify you with one of four different types of dialog boxes.

- A setting or feature that is part of Windows needs your permission to start.
- A program that is not part of Windows needs your permission to start.
- A program with an unknown publisher needs your permission to start.
- You have been blocked by your system administrator from running this program.

13. The UAC settings and the potential impact of each setting to the security of your computer.

Setting	Security Impact
<b>Always Notify</b>	<ul style="list-style-type: none"><li>• This is the most secure setting.</li><li>• When you are notified, you should carefully read the contents of each dialog box before allowing changes to be made to your computer.</li></ul>
<b>Notify me only when programs try to make changes to my computer</b>	<ul style="list-style-type: none"><li>• It's usually safe to allow changes to be made to Windows settings without you being notified. However, certain programs that come with Windows can have commands or data passed to them, and malicious software can take advantage of this by using these programs to install files or change settings on your computer. You should always be careful about which programs you allow to run on your computer.</li></ul>
<b>Notify me only when programs try to make changes to my computer (do not dim my desktop)</b>	<ul style="list-style-type: none"><li>• This setting is the same as "Notify only when programs try to make changes to my computer," but you are not notified on the secure desktop.</li><li>• Because the UAC dialog box isn't on the secure desktop with this setting, other programs might be able to interfere with the dialog's visual appearance. This is a small security risk if you already have a malicious program running on your computer.</li></ul>
<b>Never Notify</b>	<ul style="list-style-type: none"><li>• This is the least secure setting. When you set UAC to never notify, you open up your computer to potential security risks.</li><li>• If you set UAC to never notify, you should be careful about which programs you run, because they will have the same access to the computer as you do. This includes reading and making changes to protected system areas, your personal data, saved files, and anything else stored on the computer. Programs will also be able to communicate and transfer information to and from anything your computer connects with, including the Internet.</li></ul>

14. **Security Identifiers (SIDs) and Windows privileges**

15. **Admin Approval Mode**

# LO1 - ANSWER KEYS:



## SELF CHECK 2:

### 1. The organisation's policies

### 2. Administrators

### 3. Some basic parameters covered by most operating systems to consider when setting up user account options:

- **Password requirements** - whether a password is required, minimum length, complexity, needs to be changed at intervals, etc
- **Account lock out settings** - disabling accounts that have made a number of bad logon attempts
- **Access hours** - the standard days and time that users will be permitted to access the network
- **Account expiry dates** - date when account will be disabled
- **Logon restrictions** - accounts can only be used at specified locations or workstations.
- **Home directory information** - a home directory is a folder that usually has the name of the user and the user has full permissions over.
- **Logon scripts** - these perform specific tasks or run specific programs when the user logs on

### 4. Access permissions

### 5. Permissions

### 6. The user account or group can be set with the following type of permissions

- No access at all to files and directories
- Read only.
- Modify where the contents of files and directories may be accessed but changed or added to but not deleted
- Full Control or Supervisory where files and directories can be view modified and deleted.

### 7. Rights (or privileges)

### 8. To manage user accounts appropriately administrators should

- Regularly review organisational policies and procedures to be aware of requirements and address any organisational or network changes
- Conduct regular checks to ensure the change management procedures are working for new, changed and deleted users
- Review and investigate current work practices regarding user network access
- Conduct information and training sessions for network users to reinforce appropriate practices and organisational policy
- Conduct regular audits of network access—verifying current users and

### 9. Policy and procedures

# LO1 - ANSWER KEYS:



## **SELF CHECK 3:**

- 1. Security requirements.**
- 2. Incorrect credentials**
3. “your account has time restrictions that prevent you from logging on at this time.  
Please try again later.”
4. Changing user passwords accomplishes two things:
  - If attackers are attempting to guess a password, it forces them to restart their efforts. If users never change their passwords, attackers would be able to guess them eventually.
  - If an attacker has guessed a user’s password, changing the password prevents the attacker from using these credentials in the future.
- 5. Change their password automatically.**
- 6. Disable user accounts**

# LO1 - ANSWER KEYS:



## SELF CHECK 4:

1. **A password**
2. **Letters, numbers, symbols, and spaces.**
3. **Strong password.**
4. **Passphrases**
5. **It's difficult to guess or crack.**
6. Compare a strong **password** and a strong **passphrase**

<b>A strong password:</b>	<b>A strong passphrase:</b>
<ul style="list-style-type: none"><li>• Is at least eight characters long.</li><li>• Does not contain your user name, real name, or company name.</li><li>• Does not contain a complete word.</li><li>• Is significantly different from previous passwords.</li></ul>	<ul style="list-style-type: none"><li>• Is 20 to 30 characters long.</li><li>• Is a series of words that create a phrase.</li><li>• Does not contain common phrases found in literature or music.</li><li>• Does not contain words found in the dictionary.</li><li>• Does not contain your user name, real name, or company name.</li><li>• Is different from previous passphrases.</li></ul>

7. The four categories of characters Strong passwords and passphrases contain:
  - Uppercase letters
  - Lowercase letters
  - Numbers
  - Symbols found on the keyboard (all keyboard characters not defined as letters or numerals) and spaces
8. **A password policy**
9. Password policies include advice on proper password management such as:
  - never share a computer account
  - never use the same password for more than one account
  - never tell a password to anyone, including people who claim to be from customer service or security
  - never write down a password
  - never communicate a password by telephone, e-mail or instant messaging
  - being careful to log off before leaving a computer unattended
  - changing passwords whenever there is suspicion they may have been compromised
  - operating system password and application passwords are different
  - password should be alpha-numeric

### **10. Minimum password age**

### **11. Maximum Password Age**

### **12. Password Complexity Requirements**



# LO1 - ANSWER KEYS:

## SELF CHECK 5:

### 1. Authentication

### 2. Windows supports a variety of authentication techniques, including

- The traditional user name and password,
- Smart cards, and
- Third-party authentication components.

### 3. The smart card

### 4. Multifactor authentication.

### 5. Biometrics

### 6. Auditing for logon events

### 7. Windows 7 (and earlier versions of Windows) provides two separate authentication auditing policies:

- **Audit Logon Events** This policy audits authentication attempts for local resources, such as a user logging on locally, elevating privileges using a UAC prompt, or connecting over the network (including connecting using Remote Desktop or connecting to a shared folder). All authentication attempts will be audited, regardless of whether the authentication attempt uses a domain account or a local user account.
- **Audit Account Logon Events** This policy audits domain authentications. No matter which computer the user authenticates to, these events appear only on the domain controller that handled the authentication request. Typically, you do not need to enable auditing of account logon events when troubleshooting authentication issues on computers running Windows 7. However, successful auditing of these events is enabled for domain controllers by default.



## 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

## LO3 - ANSWER KEYS:



### SELF CHECK 1:

1. **Spam** is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately.
2. List and explain the **four common types of spam**

#### **1. Cancellable Usenet spam**

Cancellable Usenet spam is a single message sent to 20 or more Usenet newsgroups. (Through long experience, Usenet users have found that any message posted to so many newsgroups is often not relevant to most or all of them.) Usenet spam is aimed at "**lurkers**", people who read newsgroups but rarely or never post and give their address away. Usenet spam robs users of the utility of the newsgroups by overwhelming them with a barrage of advertising or other irrelevant posts. Furthermore, Usenet spam subverts the ability of system administrators and owners to manage the topics they accept on their systems.

#### **2. Email Spam**

Email spam targets individual users with direct mail messages. Email spam lists are often created by scanning Usenet postings, stealing Internet mailing lists, or searching the Web for addresses. Email spams typically cost users money out-of-pocket to receive. Many people - anyone with measured phone service - read or receive their mail while the meter is running, so to speak. Spam costs them additional money. On top of that, it costs money for ISPs and online services to transmit spam, and these costs are transmitted directly to subscribers.

One particularly **nasty variant of email spam is sending spam to mailing lists (public or private email discussion forums.)** Because many mailing lists limit activity to their subscribers, spammers will use automated tools to subscribe to as many mailing lists as possible, so that they can grab the lists of addresses, or use the mailing list as a direct target for their attacks.

#### **3. Instant Messaging Spam**

Some examples of instant messengers are Yahoo! Messenger, AIM, Windows Live Messenger, Tencent QQ, ICQ, XMPP and Myspace chat rooms. All are targets for spammers. Many IM systems offer a directory of users, including

## LO3 - ANSWER KEYS:



demographic information such as age and sex. Advertisers can gather this information, sign on to the system, and send unsolicited messages, which could include commercial scam-ware, viruses, and links to paid links for the purpose of **click fraud**. Microsoft announced that the Windows Live Messenger version 9.0 would support specialized features to combat messaging spam. In most systems users can already block the vast majority of spam through the use of a **whitelist**. Whitelisting is the act of authorising contact.

### 4. SMS & MMS Spam

SMS (Short Messaging Service) is a mechanism which allows brief text messages to be sent to a mobile phone. MMS (Multimedia Messaging Service) can include including videos, pictures, text pages and sound.

Mobile phone spam is a form of spamming directed at these messaging services of mobile telephony. It is described as mobile spamming, SMS spam, text spam, or SpaSMS but is most frequently referred to as m-spam. These types of spam can be particularly annoying for the recipient because, unlike email, some recipients may be charged a fee for every message received, including spam!

3. Why do we get so upset when we receive E-mail which was not requested?

- **The Free Ride**
- **The “Oceans of Spam” Problem**
- **The Theft of Resources**
- **It’s All Garbage**
- **They’re Crooks**
- **It Might Be Illegal**

## LO3 - ANSWER KEYS:



### SELF CHECK 2:

#### 1. List The Effects of Spam

The never-ending onslaught of junk messages:

- Strains networks
- Erodes user productivity
- Propagates dangerous malware and costs business millions of dollars.

#### 2. List and explain Spam Media

Junk content is rapidly spilling over to many other types of IP media, including:

- **IM (instant messaging)** : Spam is a growing problem on [IM](#) networks, where the threats closely parallel those of email spam.
- **VoIP** Voice over IP: SPIT (Spam over Internet Telephony) is a rare but potentially dangerous form of spam that threatens to annoy users and jam voice-mail inboxes.
- **Search Engines**: Using techniques such as hidden text, doorway pages and mirror sites, a search-engine spammer attempts to boost a Web site's ranking by redirecting traffic to the site. This practice is also known as "spamdexing."
- **Web Message Boards**: Spammers like to use Web message boards and Usenet.com groups to promote products and services that are usually unrelated to the site's content focus.
- **Blogs**: Junk advertising is inserted into a blog's reader-comment area.
- **Online Video**: YouTube LLC and other video-sharing sites are plagued by video spam, which consists of thinly disguised commercials for products and services of dubious value.

#### 3. List and describe the main tools that can keep spam under control:

- **Spam Filters**: A growing number of technology vendors are targeting spam with products that are designed to block and quarantine suspected spam. These offerings use sophisticated algorithms to scan each incoming message for signs that it may contain spam.
- **Firewalls**: **Spam firewalls** offload message filtering from the email server, freeing up network resources and bandwidth. Spam-firewall appliances usually come preconfigured and can be set up in minutes. Maintenance is usually minimal.
- **Anti-Malware Technologies**: Hardware- and software-based anti-malware products can block dangerous attachments from reaching employees' inboxes.
- **Client Control**: Leading email clients, such as Microsoft Outlook and Outlook Express, as well as Mozilla Foundation's Thunderbird, offer built-in controls that are designed to minimize inbox spam.
- **White Lists/Black Lists**: This feature is found in many spam filters and client controls. White lists of trusted email addresses allow messages to proceed to

## LO3 - ANSWER KEYS:



the user's inbox unimpeded by any filter or client settings. Black lists work in the opposite way, routinely blocking incoming email from known offenders.

- **Disposable Email Addresses:** Many businesses and individuals routinely distribute different email addresses to every external contact, then funnel all incoming messages into a single account. This way, if one address begins spamming, it can be safely eradicated without affecting the flow of messages originating from other contacts.
- **Legal Action :** While it's rare for an individual business to sue a junk-mail sender, a growing number of law-enforcement bodies are targeting spammers, particularly organized crime rings that use the technology for financial and identity theft.
- **Policies:** All businesses need a comprehensive anti-spam policy. Besides mandating the use of filtering and other good spam-fighting technologies, the policy should cover routine workplace practices. **Business Web sites, for example, should never publish visible email addresses that can be "harvested" by spammer software.** Employees should also be encouraged not to post business email addresses on message boards, social-network sites and personal Web pages.
- **Education:** The simple task of teaching employees to be wary of phishing messages, and not to open unknown attachments, can help any business minimize spam's impact.

## LO3 - ANSWER KEYS:



### SELF CHECK 3:

1. List the four broad categories anti-spam techniques:
  - **End-User Techniques:** those that require actions by individuals,
  - **Automated techniques for email administrators:** those that can be automated by email administrators,
  - **Automated techniques for email senders:** those that can be automated by email senders and
  - Those employed by researchers and law enforcement officials.
2. List the techniques that individuals use to restrict the availability of their email addresses, with the goal of reducing their chance of receiving spam.
  - Discretion
  - Address Munging
  - Avoid Responding to Spam
  - Contact Forms
  - Disable HTML in Email
  - Disposable Email Addresses
  - Ham Passwords
  - Reporting Spam
3. List the techniques that email senders use to try to make sure that they do not send spam.
  - Background Checks on New Users and Customers
  - Confirmed Opt-In for Mailing Lists
  - Egress Spam Filtering
  - Limit Email Backscatter
  - Port 25 Blocking
  - Port 25 Interception
  - Rate Limiting
  - Spam Report Feedback Loops
  - FROM Field Control
  - Strong AUP and TOS Agreements