የሥራና ክህሎት ሚኒስቴር
Ministry of Labor and Skills

HARDWARE AND NETWORKING SERVICE LEVEL – I

Based on March 2022, Curriculum Version 1

Module Title: Protection Application or System Software

Module code: EIS HNS1 M06 0322

Nominal duration: 50 Hour

August, 2022

Prepared by: Ministry of Labor and Skill **Addis Ababa, Ethiopia**

Table of Content

Contents

Acknowledgment

Ministry of Labor and Skills wish to extend thanks and appreciation to the many representatives of TVET instructors and respective industry experts who donated their time and expertise to the development of this Teaching, Training and Learning Materials (TTLM).

Acronym

Pc - Personal Computer
GPO – Group policy Organization
E-Mai l- Electronic Mail
EOP - Exchange online protection
MSA - Managed service account

Introduction to the Module

This module defines the competence required to keep application or system software working effectively. It covers user accounts controlling, controlling spam and detecting and removing destructive software.

It also designed to meet the industry requirement under the hard ware and Network Servicing occupational standard, particularly for the unit of competency: **Protect Application or System Software**

This module covers the units:

- user accounts are controlled
- destructive software is detected and removed
- spam

Learning Objective of the Module

- Ensuring controlled user accounts
- Detecting and removing destructive software
- Identifying and taking action to stop spam

Module Instruction

For effective use this modules trainees are expected to follow the following module instruction:

1. Read the information written in each unit
2. Accomplish the Self-checks at the end of each unit
3. Perform Operation Sheets which were provided at the end of units
4. Do the “LAP test” giver at the end of each unit and
5. Read the identified reference book for Examples and exercise

Unit one: user accounts are controlled

This unit is developed to provide you the necessary information regarding the following content coverage and topics:

- User account type/privileges
- Managing user accounts
- Modifying default security policy
- displaying appropriate logon legal notices
- Monitoring emails
- Accessing information service
    - Identifying security gaps
    - Taking appropriate actions

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Identify User account type/privileges
- Manage user accounts
- Modify default security policy
- display appropriate logon legal notices
- Monitor emails
- Access information service
    - Identify security gaps
    - Take appropriate actions

1.1. User Account Type/Privileges

What is user Account

A user account allows you to sign in to your computer. By default, your computer already has one user account, which you were required to create when you set up your computer. If you plan to share your computer with others, you can create a **separate user account** for each person.

Using separate user accounts

At this point, you may be wondering why you would even need to use separate user accounts. But if you're sharing a computer with multiple people for example, with your family or at the office user accounts allow everyone to save their own files, preferences, and settings without affecting other computer users. When you start your computer, you'll be able to choose which account you want to use.

☞ *Following are different Types of user accounts with their privileges*

➢ **Administrator, Standard, and Managed accounts**

Before you create new user accounts, it's important to understand the different types.

- **Administrator**:
  - Administrator accounts are special accounts that are used for making changes to system settings or managing other people's accounts.
  - They have full Control and access to every setting on the computer. Every computer will have at least one Administrator account, and if you're the owner you should already have a password to this account.

👍 If you have administrator credentials,
  - You can change the properties of any user account.
  - You can also change the account type from Administrator to Standard User (provided that at least one Administrator account remains on the computer) or vice versa.
  - You create computer accounts and designate permission levels from the Family & Other Users pane of the Accounts category page of the Settings window.

- **Standard**:
  - It have limited or restricted access privilege
  - Standard accounts are the basic accounts you use for normal everyday tasks. As a Standard user, you can do just about anything you would need to do, such as running software or personalizing your desktop.

- **Standard with Family Safety**:
  - These are the only accounts that can have **parental controls**. You can create a Standard account for each child, and then go to the **Family Safety** settings in your **Control Panel** to set website restrictions, time limits, and more.

- **Guest Account:**
  - Windows' guest account lets other people use your computer without being able to change PC settings, install apps or access your private files. That comes in handy when you have to share your computer temporarily.

☞ Generally, it's safer to be signed in to a Standard account than an Administrator account. If you're logged in as an Administrator, it may actually make it easier for an **unauthorized user to make changes** to your computer. Therefore, you may want to create a Standard account for yourself, even if you're not sharing the computer with anyone. You'll still be able to make **Administrator-level changes**; you'll just need to provide your **Administrator password** when making these changes.

1.2. User accounts Management

An administrator can give other people access to the computer in one of three ways:

- Create a user account that is linked to an existing Microsoft account.
- Create a user account that is linked to an email address, and register that account as a Microsoft account.
- Create a local account that isn't linked to a Microsoft account.

☞ Every user account has an associated user account name and can have a user account picture and a password. Any user can change the following details for his or her account:

- **Account name** You can change the display name that appears on the Welcome screen and Start menu.
- **Account picture** You can change the picture that identifies you on the Welcome screen and Start menu.
- **Password** You can create or change the password.

☞All types of user accounts are visible in the Family & Other Users pane. However, the processes for managing family accounts and non-family accounts differ, so we cover them separately in the following sections to avoid confusion.

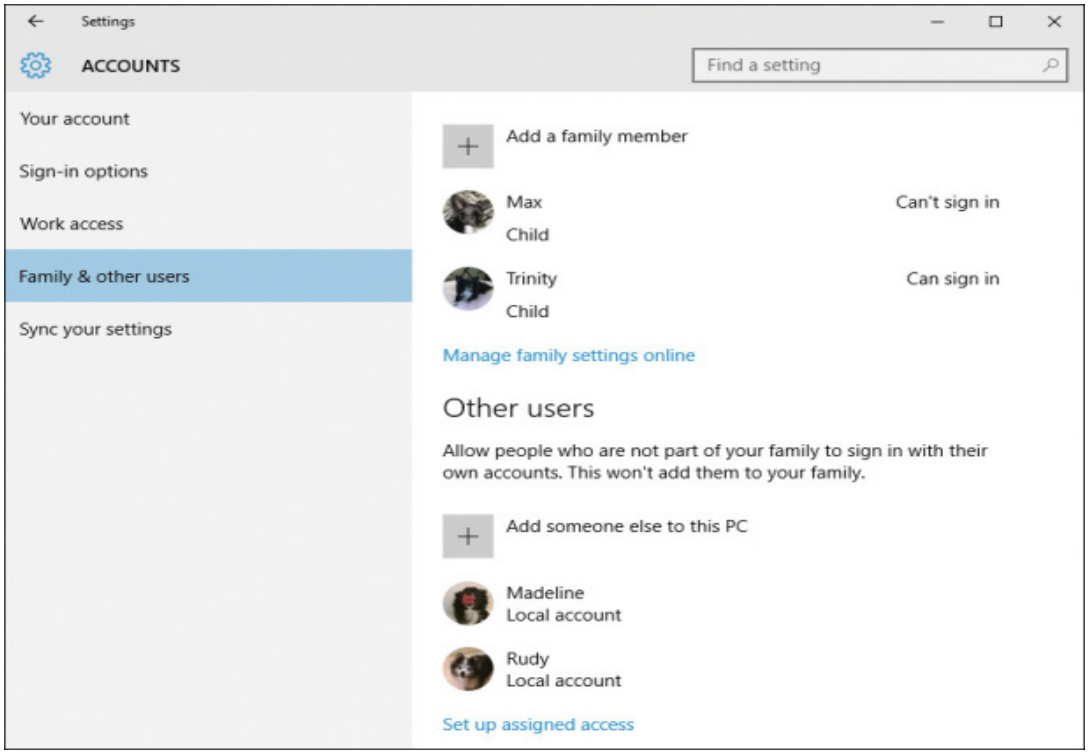


Fig. 1.2.1. User account management

You manage other user accounts from this pane, so the lists don't include your account

- Only administrators can create user accounts if you're signed in with a standard user account, you don't have the option to do so. When you create a user account, you must designate whether the user is part of your family group.
- When you first add a user account, it is identified in lists by its email address or by the name you give it. You can change the user account name (and delete user accounts) from the Users node of the Computer Management console.
- If a person is not going to sign in to a specific computer again, it's a good idea to delete his or her user account. This will clean up the user account lists and recover the hard-drive space that is used by that user's data.
- If you don't want to delete the user account data, you can disable the account instead of deleting it.

Manage user accounts in the Computer Management console

Some user account management tasks can be completed from the Family & Other Users settings pane, but others must be performed in the Users node of the Computer Management console.

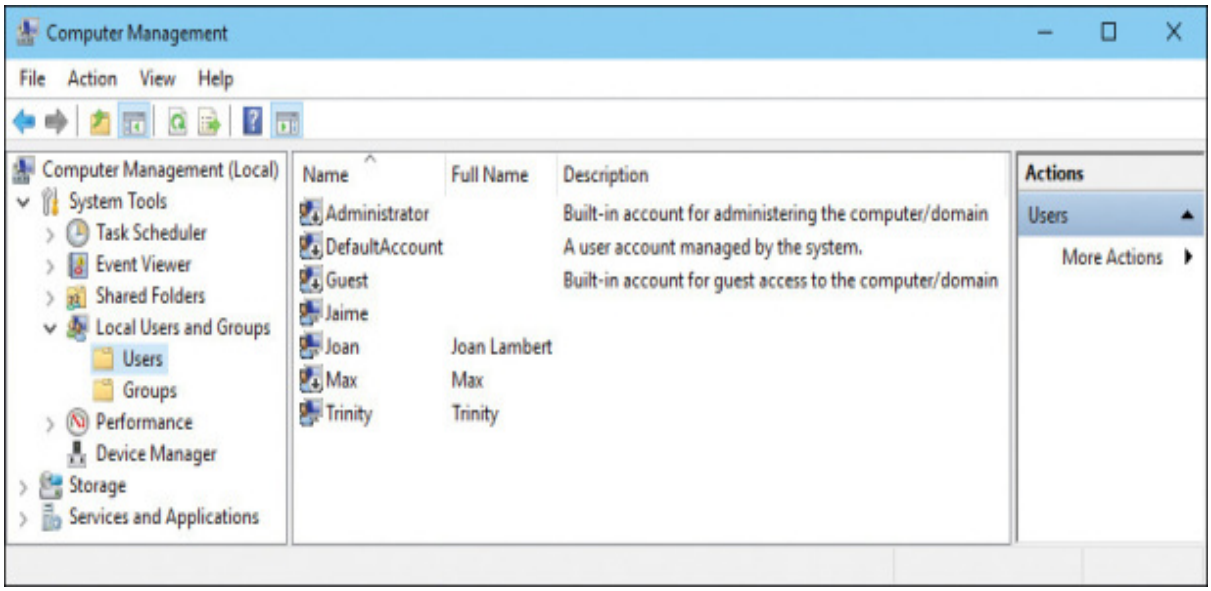


Fig 2.1.2 Managing user account using Computer Management console

1.3. Default security policy Modification

Applying Security policy settings on Windows 10 and Windows 11

Security policy settings are rules that administrators configure on a computer or multiple devices for protecting resources on a device or network. The Security Settings extension of the Local Group Policy Editor snap-in allows you to define security configurations as part of a Group Policy Object (GPO).

The GPOs are linked to Active Directory containers such as sites, domains, or organizational units, and they enable you to manage security settings for multiple devices from any device joined to the domain.

Security settings policies are used as part of your overall security implementation to help secure domain controllers, servers, clients, and other resources in your organization.

Security settings can control:

- User authentication to a network or device.
- The resources that users are permitted to access.
- Whether to record a user's or group's actions in the event log.
- Membership in a group.

To manage security configurations for multiple devices, you can use one of the following options:

- Edit specific security settings in a GPO.
- Use the Security Templates snap-in to create a security template that contains the security policies you want to apply, and then import the security template into a Group Policy Object. A security template is a file that represents a security configuration, and it can be imported to a GPO, applied to a local device, or used to analyze security.

For more info about managing security configurations, see Administer security policy settings.

The Security Settings extension of the Local Group Policy Editor includes the following types of security policies:

- **Account Policies.** These policies are defined on devices; they affect how user accounts can interact with the computer or domain. Account policies include the following types of policies:
  - **Password Policy.** These policies determine settings for passwords, such as enforcement and lifetimes. Password policies are used for domain accounts.
  - **Account Lockout Policy.** These policies determine the conditions and length of time that an account will be locked out of the system. Account lockout policies are used for domain or local user accounts.
  - **Kerberos Policy.** These policies are used for domain user accounts; they determine Kerberos-related settings, such as ticket lifetimes and enforcement.
- **Local Policies.** These policies apply to a computer and include the following types of policy settings:
  - **Audit Policy.** Specify security settings that control the logging of security events into the Security log on the computer, and specifies what types of security events to log (success, failure, or both).

    ☞ For devices running Windows 7 and later, we recommend to use the settings under Advanced Audit Policy Configuration rather than the Audit Policy settings under Local Policies.

  - **User Rights Assignment.** Specify the users or groups that have sign-in rights or privileges on a device
  - **Security Options.** Specify security settings for the computer, such as Administrator and Guest Account names; access to floppy disk drives and CD-ROM drives;
- **Software Restriction Policies.** Specify settings to identify software and to control its ability to run on your local device, organizational unit, domain, or site.
- **Application Control Policies.** Specify settings to control which users or groups can run particular applications in your organization based on unique identities of files.
- **Advanced Audit Policy Configuration.** Specify settings that control the logging of security events into the security log on the device. The settings under Advanced Audit Policy Configuration provide finer control over which activities to monitor as opposed to the Audit Policy settings under Local Policies.

1.4. Displaying logon legal notices

Logon or Startup messages let you display a reminder or any important message, every time users log into a Windows computer. As a company, some may even choose to display legal notices on every start-up. The process of displaying a startup Message Box in Windows 8 is basically similar to what it was in Windows 10/8/7. You can do so via the Group Policy Editor or the Registry Editor. Let us see how to do it!

1.5. Manage email and account settings on Windows 10

E- Mail

- E- Mail (electronic mail) is the exchange of computer-stored messages by tele communication.

Email messages are usually encoded in American Standard Code for Information Interchange (ASCII) text. However, you can also send non text files, such as graphic images and sound files as attachments sent in binary streams.

- If you use more than one account to access your emails and apps, use this guide to add them to your Windows 10 primary account to allow apps easier and faster access.

1.6. Accessing information service

Managing and Secure Service Accounts

Microsoft service accounts are a critical part of any Windows ecosystem because they are used to run essential services and applications, from web servers to mail transport agents to databases. But all too often, they are not used and managed properly which leaves the organization at unnecessary risk of business disruptions, security breaches and compliance failures.

Indeed, problems with service accounts are one of the top four issues that we at Quest uncover during security assessments.

About Microsoft service accounts

- A Microsoft service account is an account used to run one or more services or applications in a Windows environment. For example, Exchange, SharePoint, SQL Server and Internet Information Services (IIS) all run under service accounts.
- The service account provides the security context for the service, in other words, it determines which local and network resources the service can access and what it can do with those resources.
- Service accounts can exist on workstations, member servers and domain controllers (DCs).

There are several types of Microsoft service accounts, each with its own advantages and disadvantages:

- **Built-in service account**: On a local computer, you can configure an application to run under one of the three built-in service accounts: LocalService, NetworkService or LocalSystem. These accounts do not have passwords.

- **Traditional service account** :

  - A traditional Microsoft service account is just a standard user account. Ideally, it should be an account created and used exclusively to run a particular service, but all too often, business users and admins use their regular user accounts as service accounts in the name of expediency. Unlike the built-in service accounts, these accounts do have passwords. However, managing the passwords of hundreds or thousands of service accounts can get complicated very quickly, and changing a service account's password introduces the risk of breaking the applications or services it is used to run. Therefore, many organizations set their service account passwords to never expire and never update them, which is not much better than having no password at all.
  - Traditional service accounts can be created like any other user account, such as with Active Directory Users and Computers (ADUC) or your identity management solution.

- **Managed service account (MSA) or, more precisely, standalone managed service account (sMSA)** :
  - In Windows Server 2008 R2, Microsoft introduced the managed service account, which improves security by eliminating the need for an administrator to manually manage the credentials for each service account. Instead, an sMSA establishes a complex password and changes that password on a regular basis (by default, every 30 days).
  - An sMSA cannot be shared between multiple computers (hence the modifier "standalone").

- **Group managed service account (gMSA) :**
  - The sMSA has been superseded by the group managed service account.
  - A gMSA provides the same functionality as an sMSA but can be used across multiple servers and can be used to run scheduled tasks. GMSAs can be configured and administered only on computers running Windows Server 2012 or later, but they can be deployed in domains that still have DCs running earlier operating systems. There are no domain or forest functional level requirements.To create a gMSA, use the PowerShell cmdlet New-ADServiceAccount. (Be sure to set the desired password change interval because you cannot change it later!) The new gMSA will be located in the Managed Service Accounts container. Then install the gMSA on the host using the **Install-ADServiceAccount** for more details, see Microsoft's step-by-step guide.

- **Virtual service account :**
  - Like sMSAs, virtual accounts were introduced in Windows Server 2008 R2. You cannot manually create or delete a virtual account; it is created automatically when a service is installed, with a name in the format *NT SERVICE\<SERVICENAME>*. A service that runs as a virtual account will access network resources using the credentials of the computer account, in the format <*domain_name*>\<*computer_name*>$.

Top 10 best practices for creating, using and managing Microsoft service accounts
Know what service accounts you have and what they are being used for.

The first step in effectively managing just about anything is to get a complete and accurate inventory of all those things. In our case, it's vital to identify all accounts that are being used as service accounts, understand exactly where and how they are being used, and track key metrics such as when their passwords were last changed.

Unfortunately, that task is far more difficult than it might initially seem. As noted earlier, Microsoft service accounts can exist on workstations, member servers and DCs, and there are many different types of accounts that can be used as service accounts, including regular user accounts. With native tools, you have to go out to each of the different machines and figure out how the applications and services on it have been configured. Doing that manually clearly is not a feasible approach. Therefore, you'll want to automate the scan by writing a script using the Get-ADServiceAccount PowerShell cmdlet or by using a comprehensive enterprise security reporting solution.

Self-check 1

Instruction I: Write True if the statement is correct and False if the statement is incorrect

1. A **user account** allows you to **sign in** to your computer
2. to share your computer with others, you can create a **separate user account** for each person
3. Standard user account can change the properties of any user account
4. It's safer to be signed in to a Standard account than an Administrator account
5. User Rights Assignment, Specify the users or groups that have sign-in rights or privileges on a device
6. Kerberos Policy are used for domain user accounts
7. Password Policy determine settings for passwords

Instruction II. Choosing

1. Any user can his or her account
   A. Password
   B. User Name
   C. Picture
   D. All
   E. None
2. _____ kind of user account have limited or restricted access privilege
   A. Standard
   B. Administrator
   C. Computer
   D. All
   E. None
3. _____ kind of account let's other people use your computer without being able to change PC settings, install apps or access your private files.
   A. Administrator
   B. Guest
   C. User Account
   D. All
   E. None

4. Security settings can control:
   A. User authentication to a network or device.
   B. The resources that users are permitted to access.
   C. Membership in a group.
   D. All
   E. None

5. To manage security configurations for multiple devices, you can use one of the following options:
   A. Edit specific security settings in a GPO
   B. Use the Security Templates snap-in
   C. A and B
   D. None

Operation Sheet 1

Operation Title: Create local User Account

- **Purpose:** To practice and demonstrate the knowledge and skill required in **Creating User account**
- **Instruction:** you have given 20min and demonstrate to your trainer
- **Tools and requirement:**
    1. Personal Computer
    2. Peripheral Devices
- **Precautions:** take under consideration any required Safety measures during work
- **Procedures used to accomplishing the task**

1.Select **Start** > **Settings** > **Accounts** and then select **Family & other users.** (In some versions of Windows you'll see **Other users**.)
2.Next to **Add other user**, select **Add account**.
3.Select **I don't have this person's sign-in information**, and on the next page, select **Add a user without a Microsoft account**.
4.Enter a user name, password, or password hint—or choose security questions—and then select **Next**.

☞ Open Settings and create another account

Change a local user account to an administrator account

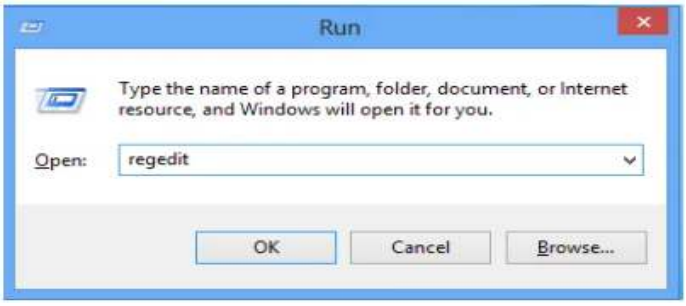
1.Select **Start** > **Settings** > **Accounts** .
2.Under **Family & other users**, select the account owner name (you should see "Local account" below the name), then select **Change account type**.
3.Under **Account type**, select **Administrator**, and then select **OK**.
4.Sign in with the new administrator account

Operation Sheet 2

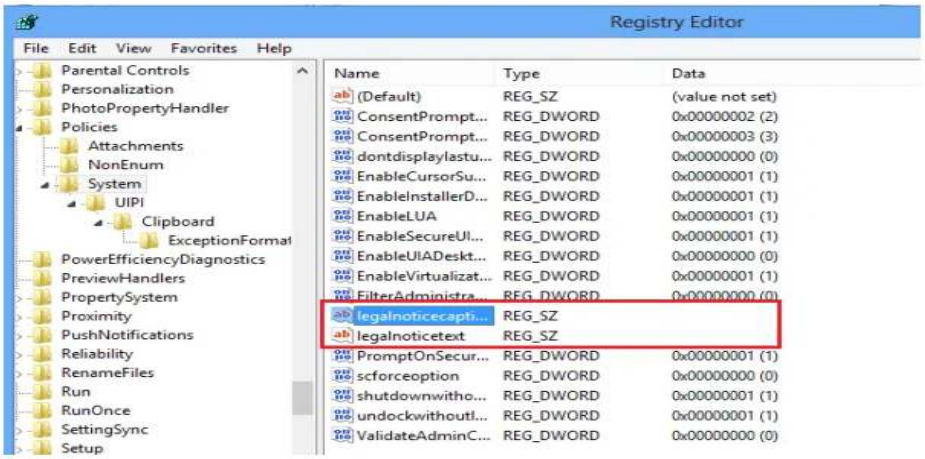
Operation Title : Display legal message on start-up in Windows 10 Using Windows Registry

- **Purpose:** To practice and demonstrate the knowledge and skill required in **Deploy legal message on start-up**
- **Instruction:** For this operation you have given 20min and demonstrate to your trainer
- **Tools and requirement:**
  - Personal Computer
- **Precautions:** take under consideration any required Safety measures during work
- **Procedures used to accomplishing the task**

Step 1. Press Win+R in combination to show up the 'Run' dialog box. In the empty field of run dialog box, type the following keyword – regedit and hit the 'OK' button.



Step 2: Next, when in the 'Registry Editor' window, navigate to the following key:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Policies\System



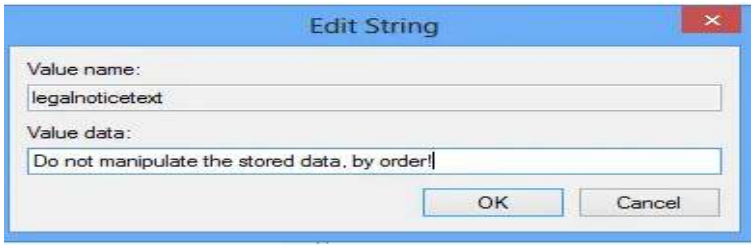
Step 3: Under this key, you will notice two entries. It is these entries that need modification, to activate a start-up message:

- Legalnoticecaption
- Legalnoticetext

Step 4: For doing so, right-click on the each of them, one after the other and choose the '***Modify***' option.

- is first essential to understand the function of these two values. The first one, i.e., the **legalnoticecaption** value controls the **title of the message**. The message appears in a large font on your computer screen.

Step 4: The second one, i.e., the **legalnoticetext** value, controls the **body of the message**. It can be seen below the title. It is this place wherein you can enter any additional information to be displayed in your message.

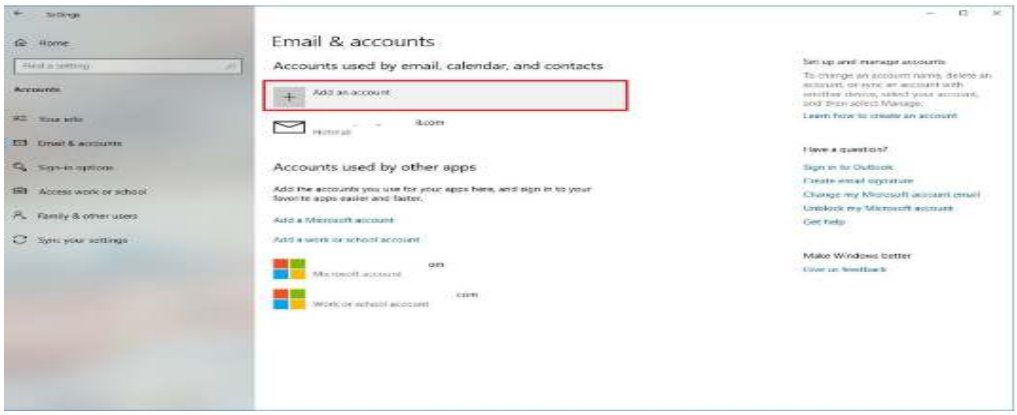


Step 5: Click Ok and Exit

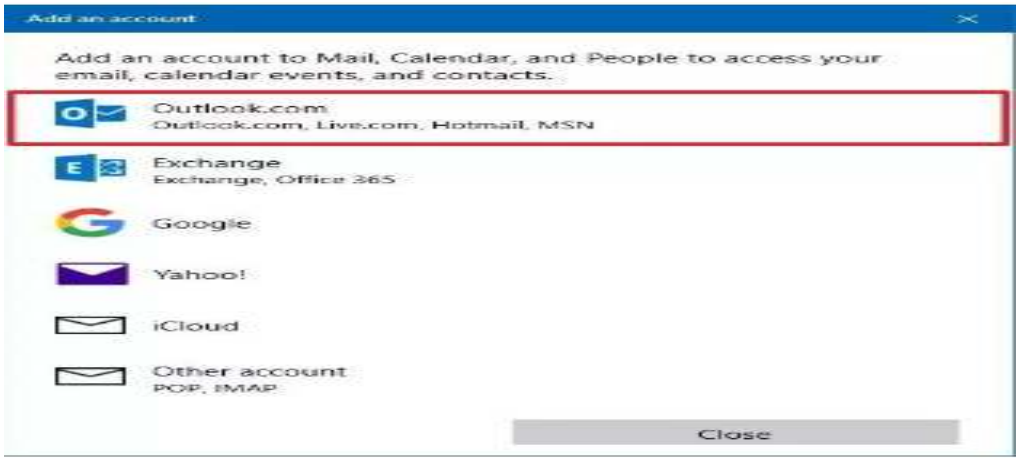
Operation Sheet 3

- **Operation Title: Adding a new E-mail Account**
- **Purpose:** To practice and demonstrate the knowledge and skill required in **Adding a new E-mail Account**
- **Instruction:** you have given 20min and demonstrate to your trainer
- **Tools and requirement:**
  - Personal Computer
- **Precautions:** take under consideration any required Safety measures during work
- **Procedures used to accomplishing the task**

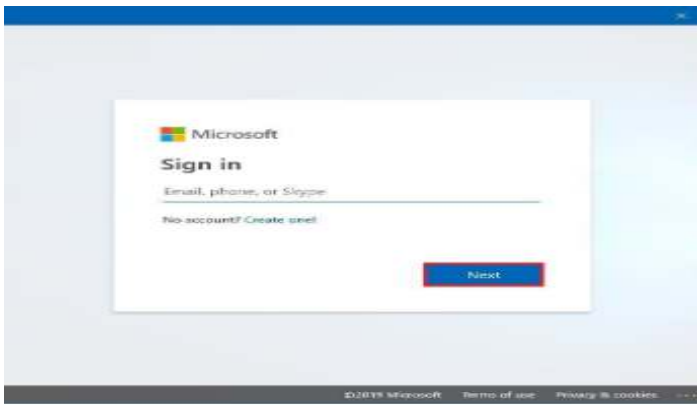
Step 1. Open **Settings**.
Step 2. Click on **Accounts**.
Step 3. Click on **Email & accounts**.
Step 4. Click the **Add an account** button to include a new email account to allow the Mail, Calendar, and People apps to access your emails, calendar, and contacts.



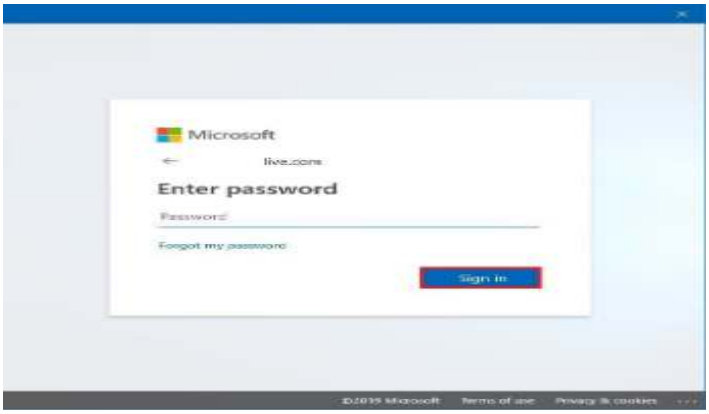
Step 5. Select your service provider — for example, Outlook.com.



Step 6.Type your email account information.
Step 7.Click the **Next** button.



Step 8. Type your account password.
Step 9. Click the **Sign-in** button.



Step 10. Click the **OK** button.
Step 11. Click the **Done** button.

Lap Test 1

Task 1. Create Local and administrator user account respectively

Task 2. Change the Local Account to Administrator User Account

Task 3. Change your account Picture, Name and Password

Task 4. Display legal message on start up

Task 5. Add a new E-mail account

Unit Two: Detect and remove destructive software

This unit is developed to provide you the necessary information regarding the following content coverage and topics:

- common types of destructive software
- virus protection
  - Selecting anti-virus software
  - Installing and updating anti-virus software
  - Describing advance system protection
- Configuring software security setting
- Scheduling anti-virus software
- Reporting and removing detected destructive software

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Define and identify common types of destructive software
- Access virus protection
  - Select anti-virus software
  - Install and updating anti-virus software
  - Describe advance system protection
- Configure software security setting
- Run and/or scheduling anti-virus software
- Report and remove detected destructive software

2.1. Common types of destructive software

What is a destructive software program?

- Destructive malware is malicious software with the capability to render affected systems inoperable and challenge reconstitution.
- Most destructive malware variants cause destruction through the deletion, or wiping, of files that are critical to the operating system's ability to run.
- Malware is short for malicious software and used as a single term to refer to virus, spy ware, worm etc.

- Malware is designed to cause damage to a stand-alone computer or a networked pc. So wherever a malware term is used it means a program which is designed to damage your computer it may be a virus, worm or Trojan.

- are programs that travel from one computer to another, using various methods, such as programs that are not what they appear to be. Shareware downloaded from the Internet is a popular method for spreading virus code.

Common types of destructive software

Destructive Software may include but ins not limited to:

- Viruses.
- File viruses.
- System sector viruses.
- Macro viruses.
- Worms.
- Trojans.
- Logic bombs.
- Spyware.

Damages caused by Viruses

- A virus can damage programs, delete files and reformat or erase your hard drive, which results in reduced performance or even crashing your system entirely.
- Hackers can also use viruses to access your personal information to steal or destroy your data.

Harmful program

Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network or server. Types of malware include computer viruses, worms, Trojan horses, ransomware and spyware.

Virus work on a computer in the ways of

- Executes when an infected program is executed. Therefore, only executable files can be infected – by definition, a virus infects other programs with copies of itself or may simply clone itself or may damage other programs and data.

- Trojans contain malicious code, that, when triggered, cause loss, or even theft, of data.

- The main purpose of a worm is to self-replicate and propagate across the network. A virus is a type of malicious software that needs a user to spread.

- A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.
- It often uses a computer network to spread itself, relying on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers.

2.2. Virus protection

- Virus protection software is designed to prevent viruses, worms and Trojan horses from getting onto a computer as well as remove any malicious software code that has already infected a computer.
- Most virus protection utilities now bundle anti-spyware and anti-malware capabilities to go along with anti-virus protection.

2.2.1. Anti-virus Selection

We recommend the best products through an independent review process, and advertisers do not influence our picks. We may receive compensation if you visit partners we recommend. Read our advertiser disclosure for more info.

Data breaches were up 68% in 2021 compared to the previous year. Personal information such as Social Security numbers, birth dates, bank account information, and credit card numbers is at risk. That data is then available on the dark web and can be used to ruin your financial life. In fact, the personal information of people with a high credit score can sell for relatively little on the dark net.

Cyberattacks on companies are also costly. The costs for compromised records, mitigating an attack, downtime, and repairs, and more accounted for a total cost of $4.24 million in 2021.2 Installing the right antivirus software at home or your business is one step you can take to ensure you don't become a future statistic. Current antivirus software has moved beyond detecting viruses to providing malware and other attack protections. With hundreds of antivirus software solutions available, it can be hard to decide which is best for you.

The 6 Best Antivirus Software of 2022

- Best Overall: Bitdefender Antivirus Plus
- Best for Windows: Norton 360 With LifeLock
- Best for Mac: Webroot SecureAnywhere for Mac
- Best for Multiple Devices: McAfee Antivirus Plus
- Best Premium Option: Trend Micro Antivirus+ Security

- Best Malware Scanning: Malwarebytes and also you can use other antivirus soft wares for your PC Example *Avast Antivirus Software*.

2.2.2. Antivirus software Installation

- Installing Antivirus application is no different to any other program or app.
- First, check if you have any antivirus software installed (besides Windows Defender).
- Open the Settings app and click on Apps. Look through the list an uninstall any packages, since they can cause problems.
- Windows Defender will be disabled automatically when you install other security software, but here's how to turn on or off Windows Defender off manually.
- Next decide which antivirus you want to use – feel free to pick one from our list of the best free antivirus – then download it from the maker's website.

2.3. Configuring software security setting

Computer security

Although we cannot always avoid threats, we can certainly take steps to minimize the associated risk. This applies not only to our lives, but also to our computers. We can take steps to ensure that we protect our computers and keep them secure, and minimize the threats they face on a daily basis.

Threats to the Computer

If you use the internet and email, share files with others or allow others to use your computer, then it is essential that you keep your computer secure to prevent harm. This is because computer criminals (also known as 'hackers') are constantly writing viruses and other forms of malicious software in an attempt to access your computer and steal your personal information, or to cause your computer to stop working as it should. For all the benefits and advantages of the internet, internet security is still a major issue. For the most part it's because users are generally not educated on what they can do to keep their computer secure when using the internet.

☞ ***Keeping Computer Secure by configuring the following settings***

There are a number of things you can do in Windows 7 to ensure your computer stays secure.

- **Windows Firewall**

Hackers attempt to gain access to your computer by looking for vulnerabilities in your computer's security. This is where the firewall comes in. A firewall is a software program or hardware that checks incoming information (such as from websites) and blocks malicious software or attempts by hackers to gain access to your computer through a network or the internet. A firewall will also stop you from spreading viruses to other computers.

- **Virus Software Viruses**

worms and Trojan horses (all types of programs designed to infect computers) are created by hackers in an attempt to erase information on your computer or to cause it to stop functioning as it should. Viruses can also be spread from computer to computer without the user being aware they are spreading a virus (such as through email and files on your computer). Installing anti-virus software and keeping it up-to-date is a must for internet users.

- **Maintain Spyware Protection**

Spyware programs are designed to collect information about you, such as websites you visit, or they may display pop-up advertisements and the like. You are not usually aware that spyware has been installed on your computer, but if odd toolbars appear on your web browser, your default home page changes, or your computer starts running slower, there's a chance it's spyware. Spyware can be installed on your computer through free software that you download and install, and/or websites you visit.

- **Back Up Your Data**

Make sure you regularly back up the data on your computer. If a virus or other type of malicious software does somehow find its way onto your computer, you can then restore your computer's data and settings to an earlier time, that is, before the virus infected your computer.

- **Playing It Safe**

Although Windows does its best to keep your computer secure, it really does come down to you being aware of the types of threats that exist, how they can end up on your computer, and what you need to be aware of and can do to ensure that your computer and valuable data stays safe.

2.4. Scheduling Anti-virus

Configure antivirus scan options with antivirus settings

Antivirus gives you complete control over how antivirus scans run on targeted devices, and which options are available to end users. For example, depending on the purpose or scheduled time of an antivirus scan, you may want to show the Antivirus client on end user devices, allow the end user to perform antivirus scans, view and restore quarantined objects, download virus definition file updates on their own, and so on. You can do this by creating and applying antivirus settings to a scan task.

With antivirus settings, you can configure the following options:

- Whether the Antivirus icon appears in device system trays (providing end user access to antivirus scanning, quarantine and backup viewing, and file handling tasks)
- Real-time email scanning
- End user right-click scans
- CPU usage
- Owner (to restrict access)
- Scheduled antivirus scans
- Quarantine/backup folder size
- Restoring infected and suspicious objects
- Specifying which files, folders, and file types to scan
- Scan exclusions
- Whether to use heuristic analysis for detecting suspicious files
- Whether to scan for riskware
- Real-time file protection (including which files to scan, heuristics, and exclusions)
- Downloading virus definition file updates (pilot test versions, scheduled downloads, end user download permission, and direct downloads from the security content serve

2.5. Removing detected destructive software

Removing a computer virus or spyware can be difficult without the help of malicious software removal tools. Some computer viruses and other unwanted software reinstall themselves after the viruses and spyware are detected and removed. Fortunately, by updating the computer and by using malicious software removal tools, you can help permanently remove unwanted software.

For more information about how to remove a computer virus and spyware, see the following article in the Microsoft Knowledge Base: 2671662 - Microsoft resources and guidance for removal of malware and viruses

1. **Install the latest updates from Microsoft Update**

Note A computer virus may prevent you from accessing the Microsoft Update website to install the latest updates. We recommend that you set the Automatic Updates service to run automatically so that a computer is not missing any important updates

2. Use the free Microsoft Safety Scanner

Microsoft offers a free online tool that scans and helps remove potential threats from your computer. To perform the scan, go to the Microsoft Safety Scanner website.

3. Use the Windows Malicious Software Removal Tool

For more information about the Microsoft Malicious Software Removal Tool, see the following article in the Microsoft Knowledge Base:

890830 - Remove specific prevalent malware with Windows Malicious Software Removal Tool

4. Manually remove the rogue security software

If the rogue security software can't be detected or removed by using Microsoft Safety Scanner or the Windows Malicious Software Removal Tool, try the following steps:

5. Run Microsoft Defender Offline

Microsoft Defender Offline is an anti-malware tool that helps remove difficult to eliminate viruses that start before Windows starts. Starting with Windows 10, Microsoft Defender Offline is built in. To use it follow the steps in this article: Help protect my PC with Microsoft Defender Offline.

Self-check 1

Instruction II. Choose the correct answer from the given alternatives

1. Malware term is used it means a program which is designed to damage your computer it may be

   A. Virus
   B. worm
   C. Trojan.
   D. All
   E. None

2. Destructive Software may include but ins not limited to:

   A. Viruses.
   B. File viruses.
   C. System sector viruses.
   D. All
   E. None

3. _____is a standalone malware computer program that replicates itself in order to spread to other computers

   A. Trojan
   B. Worm
   C. Software
   D. All
   E. None

Instruction I: Write True if the statement is correct and False if the statement is incorrect

1. Malware is designed to cause damage to a stand-alone computer or a networked pc.
2. Malware, or malicious software, is any program or file that is intentionally harmful to a computer.
3. Virus is a computer program that executes when an infected program is executed
4. Trojans contain malicious code, that, when triggered, cause loss, or even theft, of data
5. Installing Antivirus application is different to any other program or app.
6. Windows Defender will be disabled automatically when you install other security software
7. Virus protection software is designed to prevent viruses, worms and Trojan horses
8. Most virus protection utilities now bundle anti-spyware and anti-malware capabilities

Instruction II. Matching

A	**B**
1. Best Overall	A. Bit defender Antivirus Plus
2. Best for Windows	B. Norton 360 with Life Lock
3. Best for Mac	C. Web root Secure Anywhere for Mac
4. Best for Multiple Devices	D. McAfee Antivirus Plus
5. Best Premium Option	E. Trend Micro Antivirus+ Security
	F. Internet
	G. Cyber

Operation sheet 1

Operation Title: Avast Antivirus Installation

Tools and Equipment:

i. **Computer**
ii. **Antivirus software**

Precaution: Use required safety guidelines

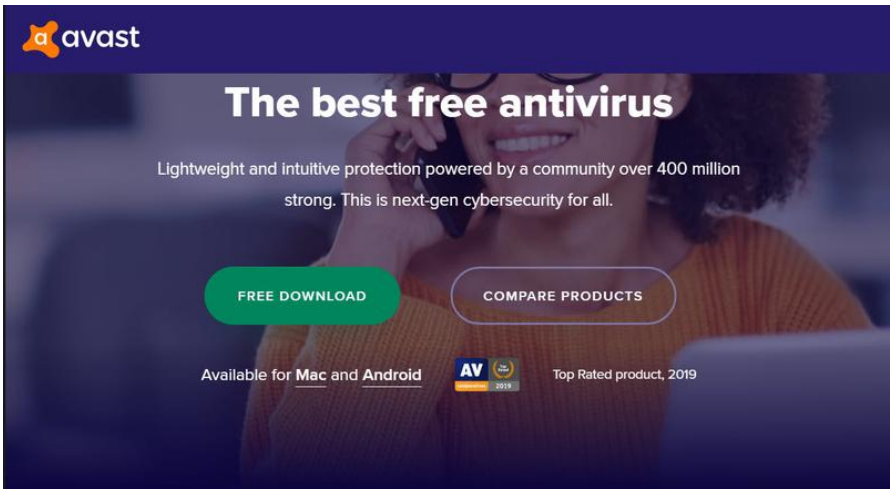
Procedures:

Step 1: Use CD/ Flash disk

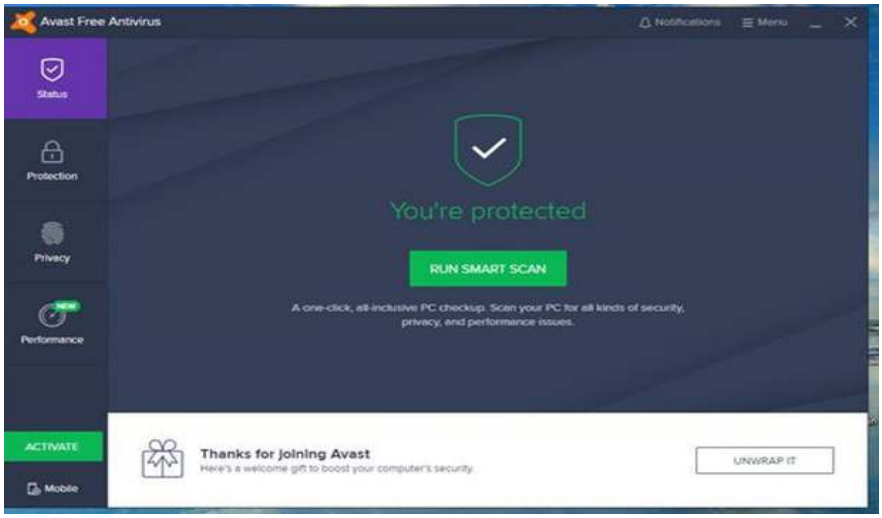
Step 2: Open the inserted Removable disk

Step 3: Open / double click its setup

Step 4: the following window is displayed/ if you have an internet connection click on ***free downloads***



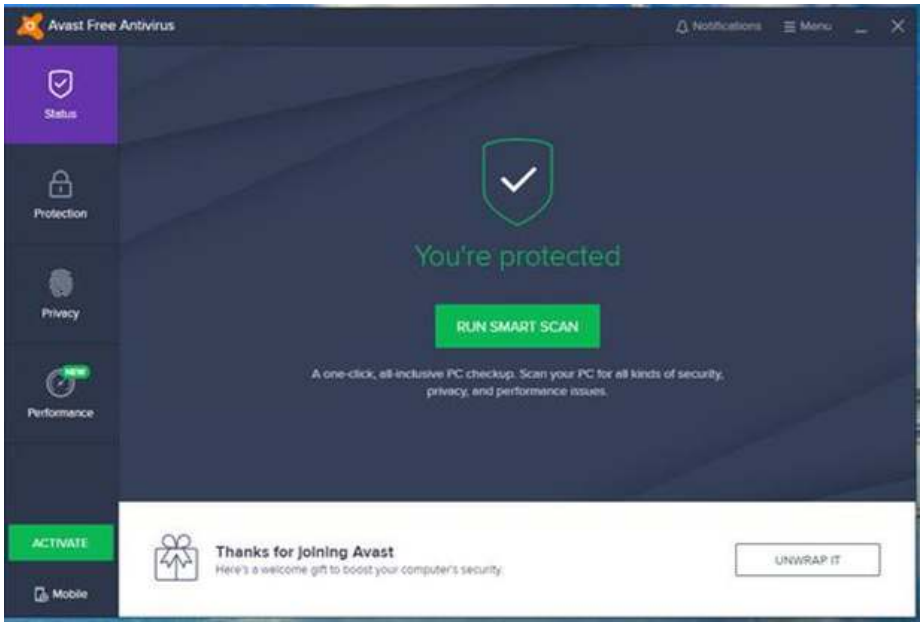
Step 5: Next, you'll be presented with a window telling you that the software wants to make changes to your system, this is a normal part of the process, so click **Accept** and then an **Install** option should appear.



☞ Before you get things underway, check for any tickboxes on the screen, as free versions can often ask to additionally install secure web browsers, software from partners or for permission to share your details with advertisers. These aren't necessarily bad things, but be sure you know what you're agreeing to before you click **Install**.

☞ When the program has finished its installation process you'll usually be asked a few questions regarding upgrading to other related products, but you can always do this later on or not at all.

Step 6: The last step is to run a full scan of your PC so that the new software can check that you don't already have any naughty programs lurking on your system.



Operation sheet 2

Operation Title: Updating Avast Antivirus

Tools and Equipment:

1. **Computer**
2. **Antivirus software**

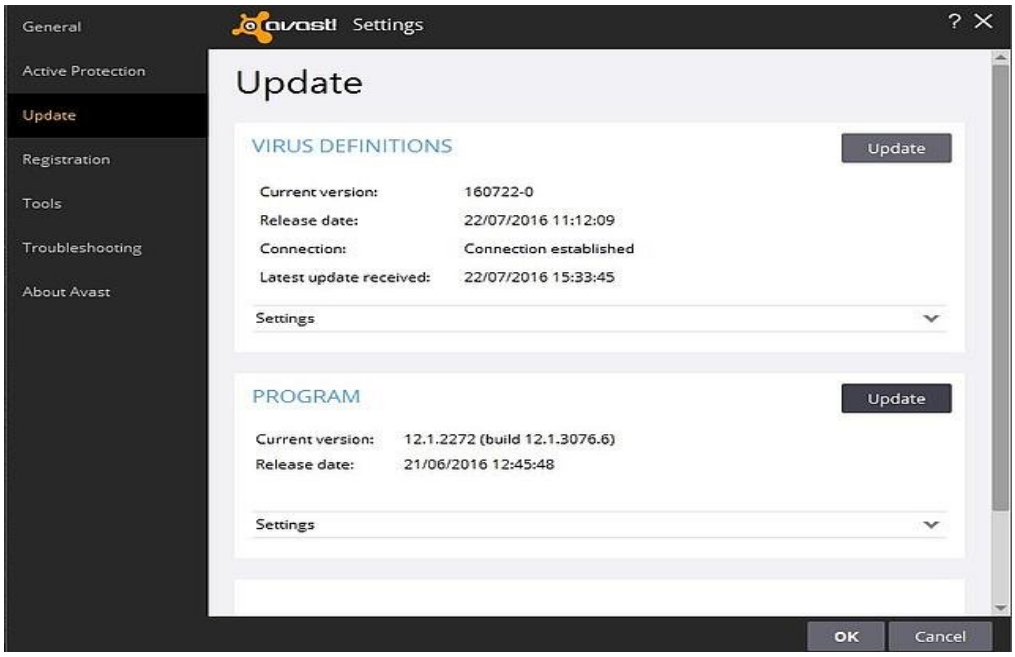
Precaution: Use required safety guidelines

Procedures:

Step 1: Open Avast Antivirus

Step 2: Click on Settings

Step 3: Select Update and click on Update (next to Program).



Operation sheet 3

Operation Title: Configuring Avast software security setting

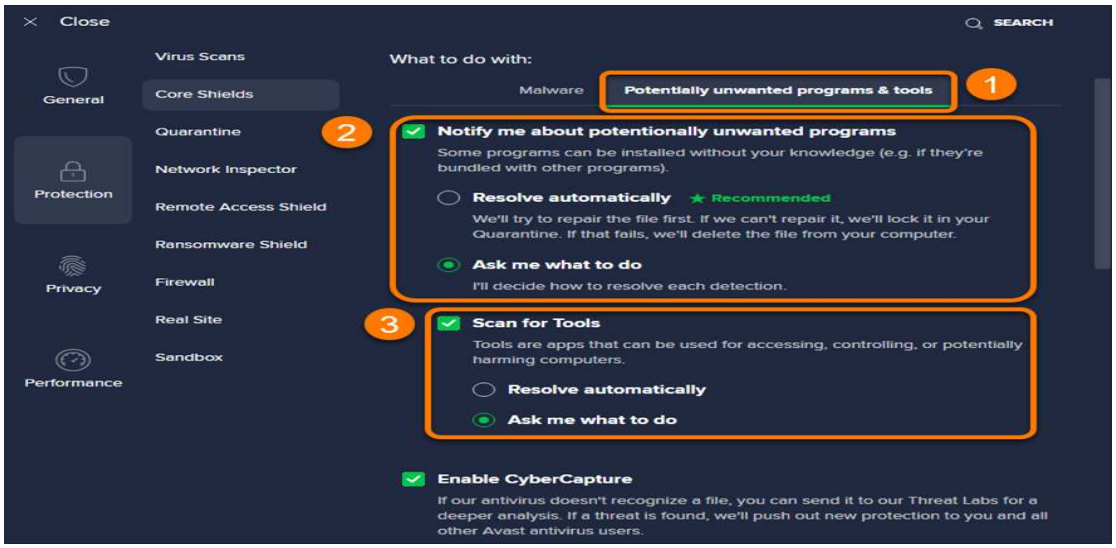
Tools and Equipment:

1. **Computer**
2. **Antivirus software**

Precaution: Use required safety guidelines
Procedures:
Step 1: Select the **Potentially unwanted programs & tools** tab.

Step 2: The default setting is for Avast Antivirus to notify you each time a potentially unwanted program is installed on your PC. When **Notify me about potentially unwanted programs** is ticked, you can select from the following actions:

Step 3: Resolve automatically or **Ask me what to do**:
Step 4: Optionally, tick the box next to **Scan for Tools**
Step 5: Resolve automatically or **Ask me what to do**:



Operation sheet 4

Operation Title: scheduling anti-virus software

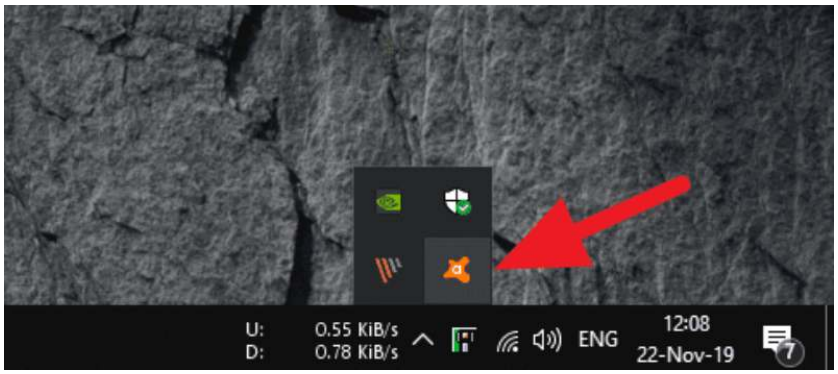
Tools and Equipment:

1. **Computer**
2. **Antivirus software**

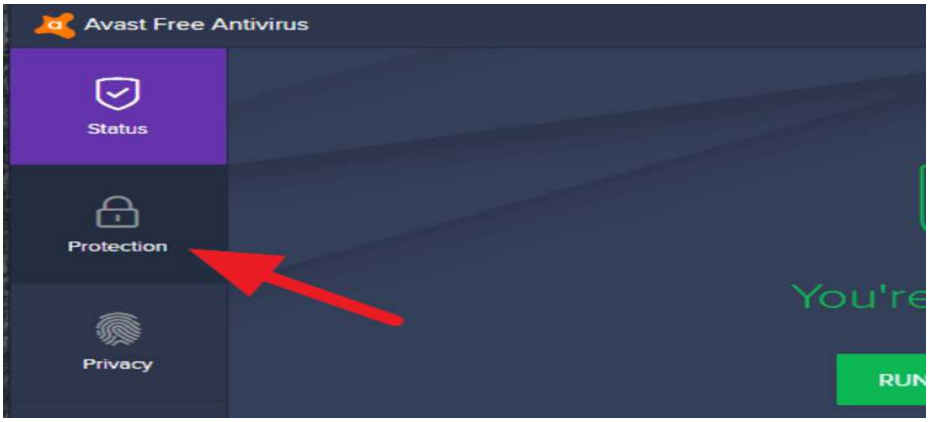
Precaution: Use required safety guidelines

Procedures:

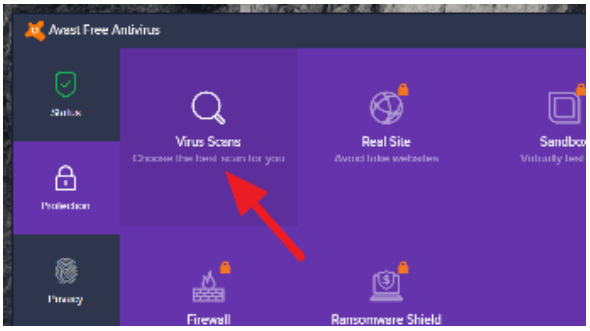
Step 1: Go to the system tray and click on the Avast icon to run the program. Basically, you can use other ways to run the antivirus.



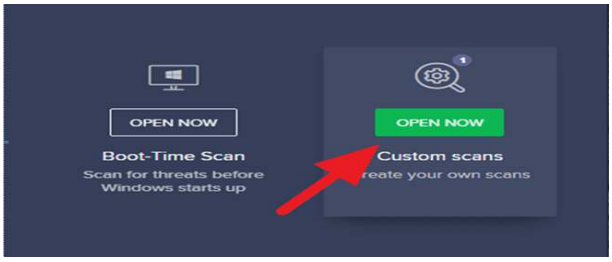
Step 2: Click the **Protection**.



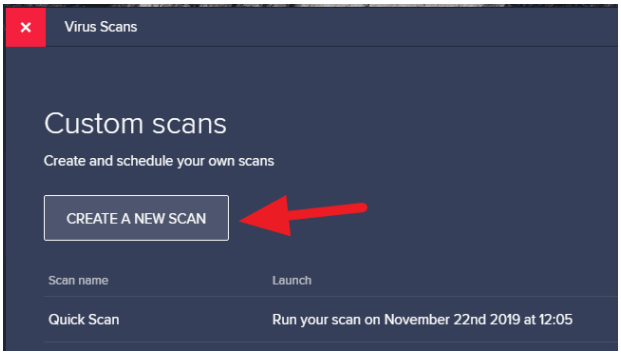
Step 3: Select **Virus Scans**.



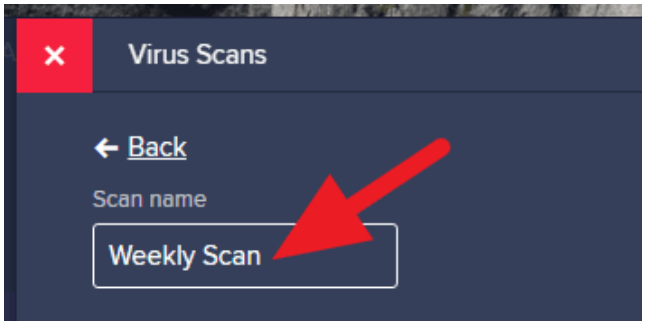
Step 4: Next, select **Custom scans**.



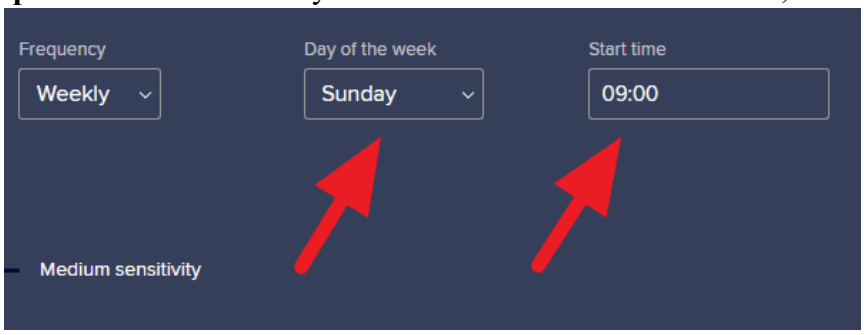
Step 5: Click **Create a New Scan** button.



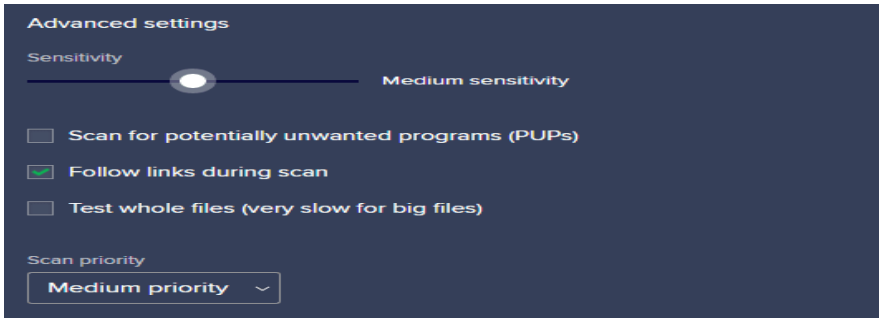
Step 6: Give a name to the scan profile, so it will be easily distinguished by other scan profiles.



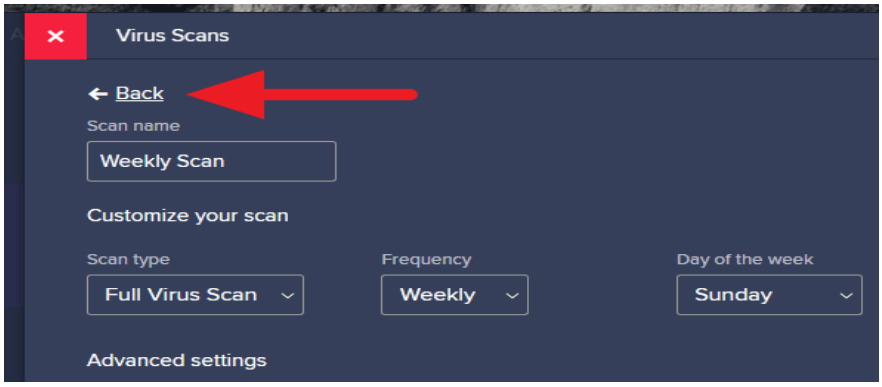
Step 7: Select the exact day or date and **Start time**. Remember, Avast uses the 24-hour format.



Step 8: You can tune the **advanced settings**. But if you don't understand, the default setting is fine.



Step 9: Go **Back** to save the scan profile.



Step 10: The scheduled scan has been created and will perform the scan on the selected date.

Operation sheet 5

Operation Title: Manually removing the rogue security software

Tools and Equipment:

1. **Computer**
2. **Antivirus software**

Precaution: Use required safety guidelines

Procedures:

Step1. Note the name of the rogue security software. For this example, we'll call it **XP Security Agent 2020**.
Step2. Restart your computer.
Step3. When you see the computer's manufacturer's logo, repeatedly press the F8 key.
Step4. When you are prompted, use the arrow keys to highlight **Safe Mode with Networking**, and then press Enter.
Step5. Click the **Start** button and check whether the rogue security software appears on the Start menu. If it's not listed there, click **All Programs** and scroll to find the rogue security software's name.
Step6. Right-click the name of the rogue security software program, and then click **Properties**.
Step7. Click the **Shortcut** tab.
Step8. In the **Properties** dialog box, check the path of the rogue security software program that is listed in **Target**. For example, **C:\Program Files\XP Security Agent 2020**.
Step9. Click **Open File Location**.
Step10. In the **Program Files** window, click **Program Files** in the address bar.
Step11. Scroll until you find the rogue security software program folder. For example, **XP Security Agent 2020**.
Step12. Right-click the folder, and then click **Delete**.
Step13. Restart your computer.
Step14. Go to the Microsoft Safety Scanner website.
Step15. Click the **Download Now** button, and then click **Run**.
Step16. Follow the instructions to scan your computer and help remove the rogue security software**.**

Lap Test

Task 1: Install any available Antivirus
Task 2: Update the installed anti-virus
Task 3: Configuring Avast software security setting
Task 4: scheduling anti-virus software
Task 5: remove the destructive software

Unit Three: Identify and take action to stop spam

This unit is developed to provide you the necessary information regarding the following content coverage and topics:

- common types of spam
- Protecting unauthorized spammer
- Configuring and using spam filters
- Reporting and documenting spams
    - Identifying security threats
    - Performing recommended action

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Define and identify common types of spam
- Protect unauthorized spammer
- Configure and using spam filters
- Report and document spams
    - Identify security threats
    - Perform recommended action

3.1. Common types of spam

Spam definition

Spam is any kind of unwanted, unsolicited digital communication that gets sent out in bulk. Often spam is sent via email, but it can also be distributed via text messages, phone calls, or social media.

What does spam stand for?

Spam is not an acronym for a computer threat, although some have been proposed (stupid pointless annoying malware, for instance). The inspiration for using the term "spam" to describe mass unwanted messages is a Monty Python skit in which the actors declare that everyone must eat the food Spam, whether they want it or not. Similarly, everyone with an email address must unfortunately be bothered by spam messages, whether we like it or not.

Types of spam

Spammers use many forms of communication to bulk-send their unwanted messages. Some of these are marketing messages peddling unsolicited goods. Other types of spam messages can spread malware, trick you into divulging personal information, or scare you into thinking you need to pay to get out of trouble.

Email spam filters catch many of these types of messages, and phone carriers often warn you of a "spam risk" from unknown callers. Whether via email, text, phone, or social media, some spam messages do get through, and you want to be able to recognize them and avoid these threats. Below are several types of spam to look out for.

Phishing emails

Phishing emails are a type of spam cybercriminals sends to many people, hoping to "hook" a few people. Phishing emails trick victims into giving up sensitive information like website logins or credit card information.

Adam Kujawa, Director of Malwarebytes Labs, says of phishing emails: "Phishing is the simplest kind of cyberattack and, at the same time, the most dangerous and effective. That is because it attacks the most vulnerable and powerful computer on the planet: the human mind."

Email spoofing

Spoofed emails mimic, or spoof, an email from a legitimate sender, and ask you to take some sort of action. Well-executed spoofs will contain familiar branding and content, often from a large well-known company such as PayPal or Apple. Common email spoofing spam messages include:

- A request for payment of an outstanding invoice

- A request to reset your password or verify your account
- Verification of purchases you didn't make
- Request for updated billing information

Tech support scams

In a tech support scam, the spam message indicates that you have a technical problem and you should contact tech support by calling the phone number or clicking a link in the message. Like email spoofing, these types of spam often say they are from a large technology company like Microsoft or a cybersecurity company like Malwarebytes.

If you think you have a technical issue or malware on your computer, tablet, or smartphone, you should always go to the official website of the company you want to call for tech support to find the legitimate contact information. Remote tech support often involves remote access to your computer to help you, and you don't want to accidentally give that access to a tech support scammer.

Current event scams

Hot topics in the news can be used in spam messages to get your attention. In 2020 when the world was facing the Covid-19 pandemic and there was an increase in work-from-home jobs, some scammers sent spam messages promising **remote jobs that paid in Bitcoin**. During the same year, another popular spam topic was related to **offering financial relief for small businesses**, but the scammers ultimately asked for bank account details. News headlines can be catchy, but beware of them in regards to potential spam messages.

Advance-fee scams

This type of spam is likely familiar to anyone who has been using email since the 90s or 2000s. Sometimes called "Nigerian prince" emails as that was the purported message sender for many years, this type of spam promises a financial reward if you first provide a cash advance. The sender typically indicates that this cash advance is some sort of processing fee or earnest money to unlock the larger sum, but once you pay, they disappear. To make it more personal, a similar type of scam involves the sender pretending to be a family member that is in trouble and needs money, but if you pay, unfortunately the outcome is the same.

Malspam

Short for "malware spam" or "malicious spam," malspam is a spam message that delivers malware to your device. Unsuspecting readers who click on a link or open an email attachment end up with some type of malware including ransomware, Trojans, bots, info-stealers, cryptominers, spyware, and keyloggers. A common delivery method is to include malicious scripts in an attachment of a familiar type like a Word document, PDF file, or PowerPoint presentation. Once the attachment is opened, the scripts run and retrieve the malware payload.

Spam calls and spam texts

Have you ever received a robocall? That's call spam. A text message from an unknown sender urging you to click an unknown link? That's referred to as text message spam or "smishing," a combination of SMS and phishing.

If you're receiving spam calls and texts on your Android or iPhone, most major carriers give you an option to report spam. Blocking numbers is another way to combat mobile spam. In the US, you can add your phone number to the National Do Not Call Registry to try to cut down on the amount of unwanted sales calls you receive, but you should still be alert to scammers who ignore the list.

3.2. Protecting unauthorized spammer

While it may not be possible to avoid spam altogether, there are steps you can take to help protect yourself against falling for a scam or getting phished from a spam message:

Learn to spot phishing

All of us can fall victim to phishing attacks. We may be in a rush and click a malicious link without realizing. If a new type of phishing attack comes out, we may not readily recognize it. To protect yourself, learn to check for some key signs that a spam message isn't just annoying—it's a phishing attempt:

1. Sender's email address: If an email from a company is legitimate, the sender's email address should match the domain for the company they claim to represent. Sometimes these are obvious, like example@abkljzr09348.biz, but other times the changes are less noticeable, like example@paypa1.com instead of paypal.com.
2. Missing personal information: If you are a customer, the company should have your information and will likely address you by your first name. A missing personal greeting alone isn't enough to spot a phishing email, but it's one thing to look for, especially in messages that say they are from a company with whom you do business. Receiving an email that says your account has been locked or you owe money is cause to worry, and sometimes we rush to click a link in order to fix the problem. If it's phishing, that's exactly what the sender wants, so be careful and check if the email is generic or addressed specifically to you.
3. Links: Beware of all links, including buttons in an email. If you get a message from a company with whom you have an account, it's wise to log in to your account to see if there is a message there rather than just clicking the link in the message without verifying first. You can contact the company to ask if a suspicious message is legitimate or not. If you have any doubts about a message, don't click any links.
4. Grammatical errors: We all make them, but a company sending out legitimate messages probably won't have a lot of punctuation errors, poor grammar, and spelling mistakes. These can be another red flag to indicate that the email could be suspect.
5. Too-good-to-be-true offers: Many phishing messages pretend to be from large, well-known companies, hoping to ensnare readers who happen to do business with the company. Other phishing attempts offer something for free like cash or a desirable prize. The saying is often true that if something sounds too good to be true it probably

is, and this can be a warning that a spam message is trying to get something from you, rather than give you something.

6. Attachments: Unless you are expecting an email with attachments, always be wary before opening or downloading them. Using anti-malware software can help by scanning files that you download for malware.

You can read even more about phishing emails and how to spot them on the Malwarebytes Labs blog.

Report spam

Email providers have gotten pretty good at filtering out spam, but when messages make it through to your inbox, you can report them. This is true for spam calls and text messages, as many carriers give you the ability to report spam as well. You can also choose to block the sender, often in the same step as reporting the message.

Reporting spam can help your email provider or phone service carrier get better at detecting spam. If legitimate emails get sent to your spam filter, you can report that they should not be marked as spam, and that also provides useful information on what should not be filtered. Another helpful step is to add senders you want to hear from to your contacts list proactively.

Use two factor-authentication (2FA)

With two-factor or multi-factor authentication, even if your username and password are compromised via a phishing attack, cybercriminals won't be able to get around the additional authentication requirements tied to your account. Additional authentication factors include secret questions or verification codes sent to your phone via text message.

Install cybersecurity

In the event that you click a bad link or download malware sent to you via spam, good cyber security software will recognize the malware and shut it down before it can do any damage to your system or network. With products for home and business, Malwarebytes has got you covered wherever technology takes you.

3.3. Configuring Spam Filter

- Spam Filter detects spam emails based on the reputation score of the sender's IP address. The sender's address is the address of the host that connects to the SMTP server to deliver an email message, not an address within the email header.

- An email is classified as spam if the sender's reputation is below the spam threshold, or is classified as suspected spam if the sender's reputation is between the spam threshold and suspected spam threshold. An email is not classified as spam if the sender's reputation is above the suspected spam threshold.

In Microsoft 365 organizations with mailboxes in Exchange Online or standalone Exchange Online Protection (EOP) organizations without Exchange Online mailboxes, inbound email messages are automatically protected against spam by EOP. EOP uses anti-spam policies (also known as spam filter policies or content filter policies) as part of your organization's overall defense against spam. For more information, see Anti-spam protection.

Admins can view, edit, and configure (but not delete) the default anti-spam policy. For greater granularity, you can also create custom anti-spam policies that apply to specific users, groups, or domains in your organization. Custom policies always take precedence over the default policy, but you can change the priority (running order) of your custom policies.

You can configure anti-spam policies in the Microsoft 365 Defender portal or in PowerShell (Exchange Online PowerShell for Microsoft 365 organizations with mailboxes in Exchange Online; standalone EOP PowerShell for organizations without Exchange Online mailboxes).

The basic elements of an anti-spam policy are:

- **The spam filter policy**: Specifies the actions for spam filtering verdicts and the notification options.
- **The spam filter rule**: Specifies the priority and recipient filters (who the policy applies to) for a spam filter policy.

The difference between these two elements isn't obvious when you manage anti-spam polices in the Microsoft 365 Defender portal:

- When you create an anti-spam policy, you're actually creating a spam filter rule and the associated spam filter policy at the same time using the same name for both.
- When you modify an anti-spam policy, settings related to the name, priority, enabled or disabled, and recipient filters modify the spam filter rule. All other settings modify the associated spam filter policy.
- When you remove an anti-spam policy, the spam filter rule and the associated spam filter policy are removed.

In Exchange Online PowerShell or standalone EOP PowerShell, you manage the policy and the rule separately. Every organization has a built-in anti-spam policy named Default that has these properties:

- The policy is applied to all recipients in the organization, even though there's no spam filter rule (recipient filters) associated with the policy.

- The policy has the custom priority value **Lowest** that you can't modify (the policy is always applied last). Any custom policies that you create always have a higher priority.
- The policy is the default policy (the **IsDefault** property has the value True), and you can't delete the default policy.

To increase the effectiveness of spam filtering, you can create custom anti-spam policies with stricter settings that are applied to specific users or groups of users.

3.4. Documenting Spams

In order for us to help, we will need to use the following process if you receive a spam email:

1. Forward the email to SFS.SpamBox@wolterskluwer.com
2. DELETE the spam email from EMC
3. Continue with the next contact

Self-Check 1.

Instruction I: Write True if the statement is correct and False if the statement is incorrect

1. Spam is any kind of unwanted, unsolicited digital communication that gets sent out in bulk
2. Spammers use many forms of communication to bulk-send their unwanted messages.
3. Phishing emails are a type of spam cybercriminals send to many people, hoping to "hook" a few people.
4. malspam is a spam message that delivers malware to your device

Instruction II. Choosing

1. ____ Specifies the actions for spam filtering verdicts and the notification options.
   A. The spam filter policy
   B. Virus
   C. Phishing
   D. All
   E. None

2. _____Specifies the priority and recipient filters (who the policy applies to) for a spam filter policy
   A. Email spoofing
   B. Malspam
   C. The spam filter rule
   D. All
   E. None

3. Common email spoofing spam messages include:
   A. A request for payment of an outstanding invoice
   B. A request to reset your password or verify your account
   C. Verification of purchases you didn't make
   D. Request for updated billing information
   E. all

4. _____ can help your email provider or phone service carrier get better at detecting spam.
   A. Spam
   B. Reporting spam
   C. Virus
   D. All
   E. None