የሥራ እና ክህሎት ሚኒስቴር
MINISTRY OF LABOR AND SKILLS

Web Development and Database Administration

Level - I

Based on March, 2022, CURRICULUM Version 1

Module Title: Protect Application or System Software

Module code: EIS WDDBA1 05 0322

Nominal duration: 30Hour

September, 2022

Addis Ababa, Ethiopia

Contents

Acknowledgment

Ministry of labor and skills wish to extend thanks and appreciation to the many representatives of TVET instructors and experts who donated their time and expertise to the development of this Short-Term program Teaching, Training and Learning Materials (TTLM).

Acronym

UAC - User Account Control

SIDs - security identifiers

OS – Operating System

GPO – Group Policy Object

ISP – Internet service providers

USB – Universal Serial Bus

ZIP –Zone Improvement Plan

RAR– RoshalARchive

Introduction to the Module

This learner’s guide is prepared to help you achieve the required competence in “Web Development and Database Administration”. This will be the source of information for you to acquire knowledge and skills required to Protect Application or System Software.

This module covers the units :

- Ensure user accounts are controlled
- Detect and remove destructive software
- Identify and take action to stop spam
- Perform workplace duties following written notices

Learning Objective of the Module

- Ensure user account are controlled
- Detect and identify destructive software, spam.
- To perform workplace duties with notices

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” given at the end of each unit and
5. Read the identified reference book for examples and exercise

Unit one: user accounts control

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

- Modifying default user settings to conform security policy
- Modifying previously created user settings to update security policy
- Ensuring legal notices displayed at logon
- Accessing information service

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:

- Document and report client requirements
- Meet client requirements in line with organizational requirements.

1.1. Modifying default user settings to conform security policy

1.1.1. Introduction on user access control

User access control (UAC) is defined as the capacity of an organization and its systems to allow or deny a user or an object access to its systems and resources. A user can be restricted from accessing a program, database or file. An object in this definition represents passive entities such as a system or a process. Systems and processes under the UAC are also restricted from accessing other processes and programs.

User Account Control (UAC) helps prevent malware from damaging a PC and helps organizations deploy a better-managed desktop. With UAC, apps and tasks always run in the security context of a non-administrator account, unless an administrator specifically authorizes administrator-level access to the system. UAC can block the automatic installation of unauthorized apps and prevent inadvertent changes to system settings.

UAC allows all users to log on to their computers using a standard user account. Processes launched using a standard user token may perform tasks using access rights granted to a standard user. For instance, Windows Explorer automatically inherits standard user level permissions. Additionally, any apps that are started using Windows Explorer (for example, by double-clicking a shortcut) also run with the standard set of user permissions. Many apps, including those that are included with the operating system itself, are designed to work properly in this way.

Other apps, especially those that were not specifically designed with security settings in mind, often require additional permissions to run successfully. These types of apps are referred to as legacy apps. Additionally, actions such as installing new software and making configuration changes to the Windows Firewall, require more permissions than what is available to a standard user account.

When an app needs to run with more than standard user rights, UAC allows users to run apps with their administrator token (with administrative groups and privileges) instead of their default, standard user access token. Users continue to operate in the standard user security context, while enabling certain apps to run with elevated privileges, if needed.

1.1.2. Components of User Access Control

The UAC comprises three main components. Each of these components are governed by a set of UAC policies forming management policy. The three components are:

- **Identification and authentication** are two processes that determine who or what, if at all, has access to any of the systems and resources. Without proper identification and authorization, policies dictate that absolutely no access to the system or resource is granted. Without a valid passport, unique to an individual, the visa is not granted.
- **Authorization** determines what an authorized user or object can access and the scope of that access. As a non-immigrant you can shop at any mall or store but you do not have right to access the free national health care system as a national would.
- **Accountability** identifies and establishes exactly what the user or the process did within the system once access was granted.

1.2. User Access Control Policies

These policies detail the specifics which are used in enforcing the restrictions by the user access controls on the systems.

A. Identification Policies

1. User access—users must reveal their identity to the system. This means that the user needs to tell the system who he/she is. This is done by using a username.

2. Object access—the system must identify the object requesting access to the system using a matching identifier previously stored within its database. Identification is achieved by the use of identifiers such as computer names, MAC addresses, IP (Internet Protocol) addresses, or Process Identification (PI) numbers.

Required identification policies must:

- uniquely identify the user or object. The identifying parameter must be unique to that individual or process alone. There cannot be two people with the same username, e.g. "jackie27," existing on the system.
- not identify the users based on the relative importance (designation) with respect to the organization.
- not be a commonly used or shared account name such as "user", "process", "admin", "sysadmin" or "root."

B. Authentication Policies

Required authentication policies must:

- be based on something known and personal to the user such as a secret password or unique identification number. This should be information known only by the owner of the account. Passwords must be set according to the management's password policies. Stricter password policies dictate the contents of the password and they must not contain groups or letters or words identical to the user name. For example, the user name "Jackie27" will not be permitted to have a password "Jackie279." This is considered to be a very weak password. Password policies also dictate the minimum number of characters with addition security rules including the mandatory use of a number and a capital letter.
- be based on an authenticating piece of hardware used to unlock the account; such as a smart card or token which is always in sole possession of the owner.
- be based on some physical characteristic or biometric identification. Science has established that no two people are perfectly identical. As such, characteristics such as fingerprints, iris recognition, and voice recognition have become internationally accepted characteristics for authentication.

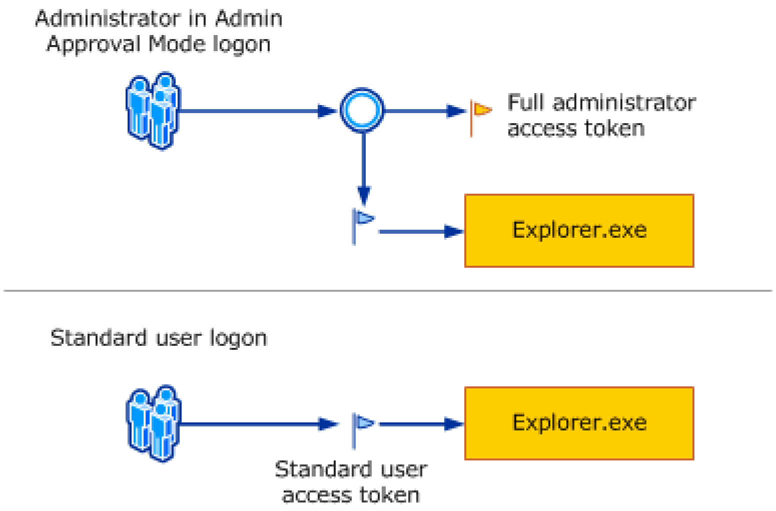
1.3. User account control process and interaction

User Account Control (UAC) is a fundamental component of Microsoft's overall security vision. UAC helps mitigate the impact of malware.

Each app that requires the administrator access token must prompt for consent. The one exception is the relationship that exists between parent and child processes. Child processes inherit the user's access token from the parent process. Both the parent and child processes, however, must have the same integrity level. Windows protects processes by marking their integrity levels. Integrity levels are measurements of trust. A "high" integrity application is one that performs tasks that modify system data, such as a disk partitioning application, while a "low" integrity application is one that performs tasks that could potentially compromise the operating system, such as a Web browser. Apps with lower integrity levels cannot modify data in applications with higher integrity levels. When a standard user attempts to run an app that requires an administrator access token, UAC requires that the user provide valid administrator credentials.

1.4. Logon process

The following shows how the logon process for an administrator differs from the logon process for a standard user.


Administrator in Admin Approval Mode logon
Full administrator access token
Explorer.exe
Standard user logon
Explorer.exe
Standard user access token

By default, standard users and administrators access resources and run apps in the security context of standard users. When a user logs on to a computer, the system creates an access token for that user. The 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 is used to start apps that do not perform administrative tasks (standard user apps). The standard user access token is then used to display the desktop (explorer.exe). Explorer.exe is the parent process from which all other user-initiated processes inherit their access token. As a result, all apps run as a standard user unless a user provides consent or credentials to approve an app to use a full administrative access token.

A user that is a member of the Administrators group can log on, browse the Web, and read e-mail while using a standard user access token. When the administrator needs to perform a task that requires the administrator access token, Windows 10 or Windows 11 automatically prompts the user for approval. This prompt is called an elevation prompt, and its behavior can be configured by using the Local Security Policy snap-in (Secpol.msc) or Group Policy.

1.5. The UAC User Experience

When UAC is enabled, the user experience for standard users is different from that of administrators in Admin Approval Mode. The recommended and more secure method of running Windows 10 or Windows 11 is to make your primary user account a standard user account. Running as a standard user helps to maximize security for a managed environment. With the built-in UAC elevation component, standard users can easily perform an administrative task by entering valid credentials for a local administrator account. The default, built-in UAC elevation component for standard users is the credential prompt.

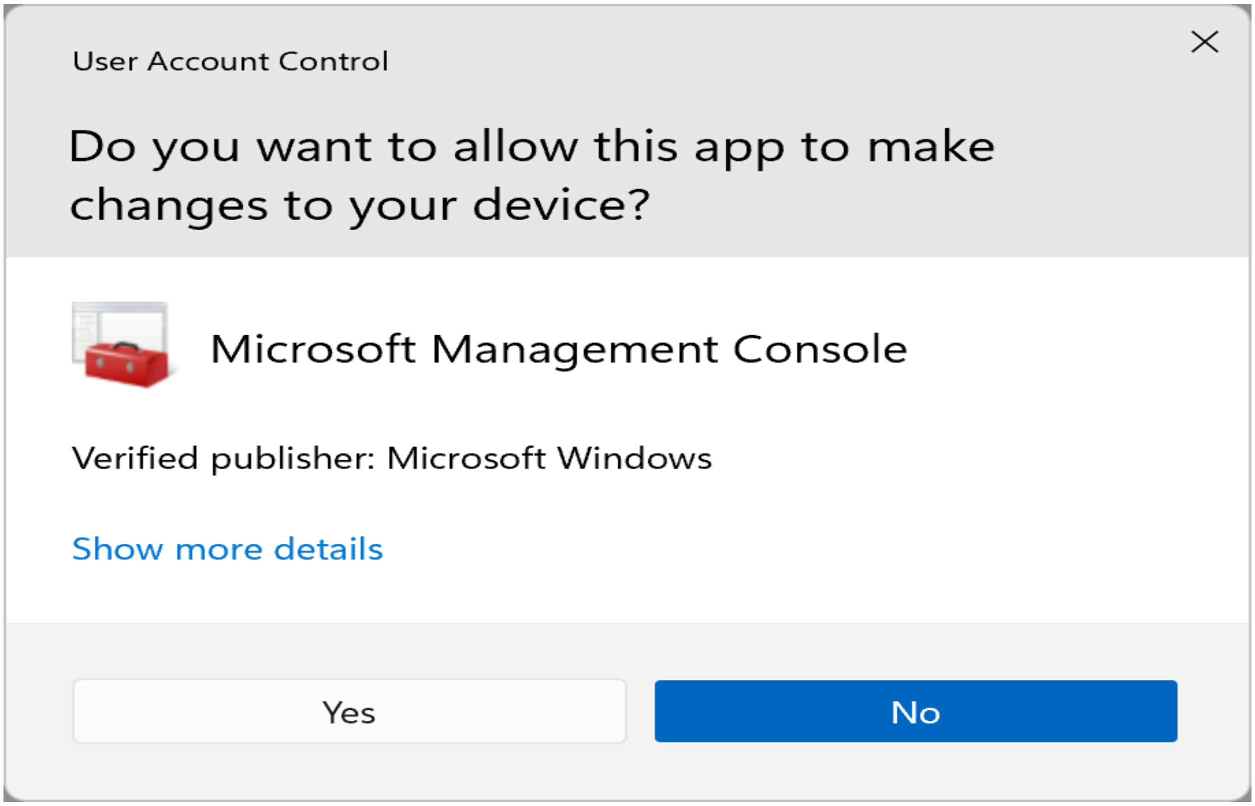
The alternative to running as a standard user is to run as an administrator in Admin Approval Mode. With the built-in UAC elevation component, members of the local Administrators group can easily perform an administrative task by providing approval. The default, built-in UAC elevation component for an administrator account in Admin Approval Mode is called the consent prompt.

1.5.1 The consent and credential prompts

With UAC enabled, Windows 10 or Windows 11 prompts for consent or prompts for credentials of a valid local administrator account before starting a program or task that requires a full administrator access token. This prompt ensures that no malicious software can be silently installed.

i. The consent prompt

The consent prompt is presented when a user attempts to perform a task that requires a user's administrative access token. The following is an example of the UAC consent prompt.



User Account Control

Do you want to allow this app to make changes to your device?

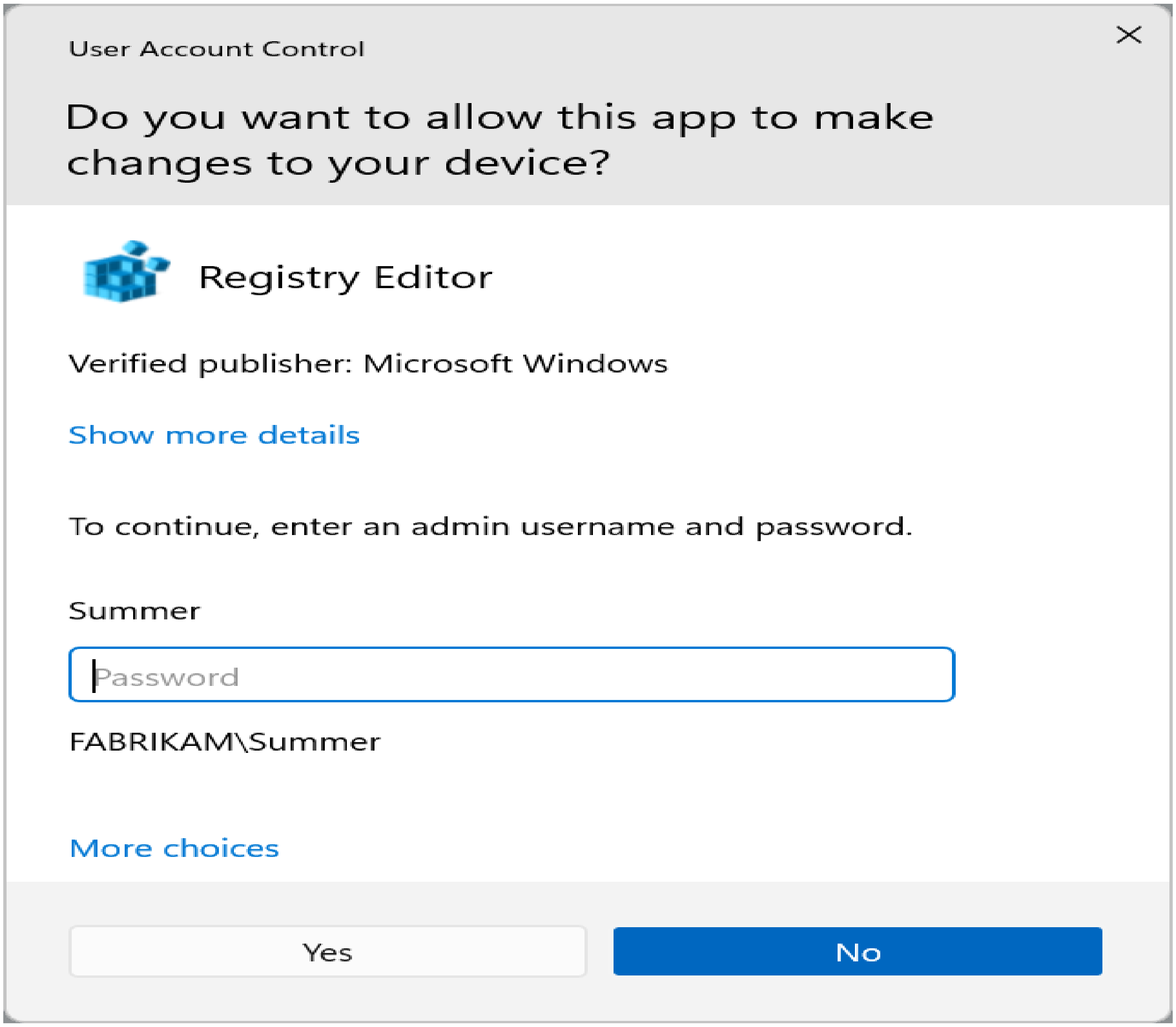
Microsoft Management Console

Verified publisher: Microsoft Windows

ii. The credential prompt

The credential prompt is presented when a standard user attempts to perform a task that requires a user's administrative access token. Administrators can also be required to provide their credentials by setting the User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Modepolicy setting value to prompt for credentials**.**

The following is an example of the UAC credential prompt.



User Account Control

Do you want to allow this app to make changes to your device?

Registry Editor

Verified publisher: Microsoft Windows

Show more details

To continue, enter an admin username and password.

Summer

Password

FABRIKAM\Summer

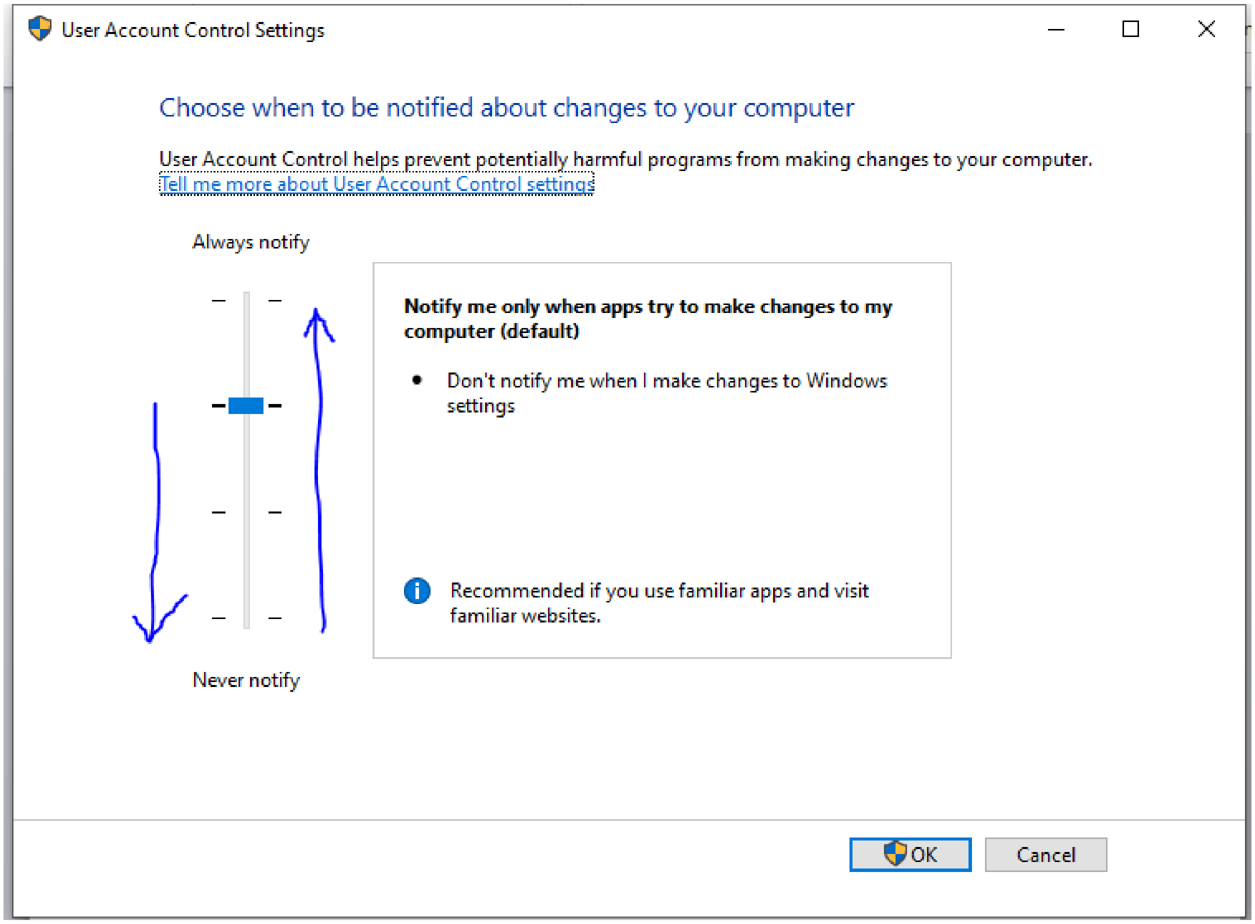
More choices

iii. UAC elevation prompts

The UAC elevation prompts are color-coded to be app-specific, enabling for immediate identification of an application's potential security risk. When an app attempts to run with an administrator's full access token, Windows 10 or Windows 11 first analyzes the executable file to determine its publisher. Apps are first separated into three categories based on the file's publisher: Windows 10 or Windows 11, publisher verified (signed), and publisher not verified (unsigned). The following diagram illustrates how Windows determines which color elevation prompt to present to the user.

Here's how to turn User Account Control (UAC) on or off in Windows 10 and later:

1. Type **UAC** in the search field on your taskbar. (If the search field isn't visible, right-click the **Start** button and choose **Search**.)
2. Click **Change User Account Control settings** in the search results.
3. Then do one of the following:
   - To turn UAC *off*, drag the slider down to **Never notify** and click **OK**.
   - To turn UAC *on*, drag the slider up to the desired level of security and click **OK**.
4. You may be prompted to confirm your selection or enter an administrator password.
5. Reboot your computer for the change to take effect.



User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify

Never notify

Notify me only when apps try to make changes to my computer (default)

- Don't notify me when I make changes to Windows settings

Recommended if you use familiar apps and visit familiar websites.

 The UAC settings.

- **Always notify**.

  The UAC prompt is shown when apps try to install software or make changes to your computer and when you try to change Windows settings. The Desktop is dimmed when a UAC prompt is shown.

- **Notify me only when apps try to make changes to my computer.**

  This is the default setting for UAC. UAC prompts aren't shown when you try to make changes to Windows settings. The Desktop is dimmed when a UAC prompt is shown.

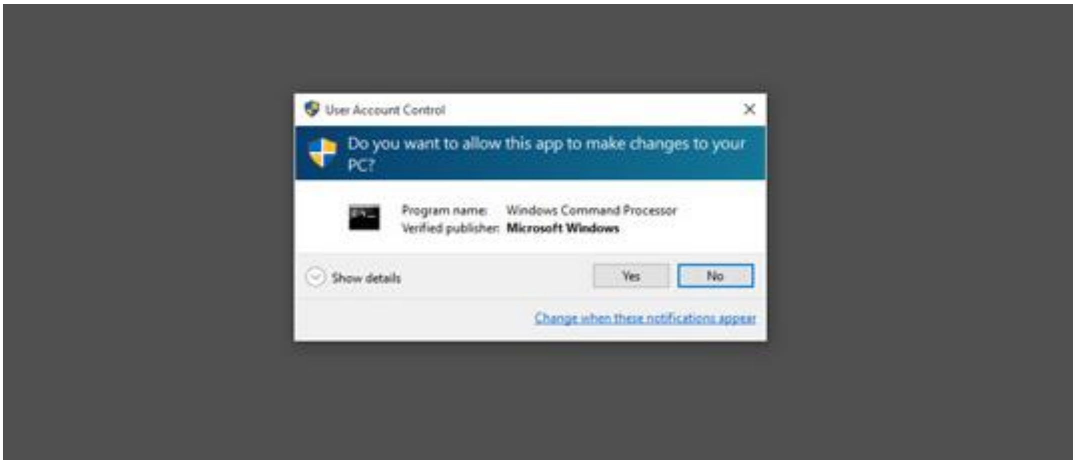
- **Notify me only when apps try to make changes to my computer (do not dim my desktop).**

  UAC prompts are not shown when you try to make changes to Windows settings, but the Desktop isn't dimmed when a UAC prompt is shown.

- **Never notify.**

Desktop apps in Windows 10 don't run with administrator permissions and consequently can't make automatic changes to an operating system. When a desktop app wants to make system changes (such as modifications that affect other user accounts, modifications of system files and folders, or installation of new software), Windows 10 issues what's called a UAC confirmation dialog box, where users can confirm whether they want those changes to be made.

If the user clicks No, the changes won't be made. If the user clicks Yes, the app receives administrator permissions and makes the system changes it's programmed to make.



User Account Control

Do you want to allow this app to make changes to your PC?

Program name: Windows Command Processor
Verified publisher: Microsoft Windows

1.6. Configure security policy settings in window 10

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).
  - **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; installation of drivers; sign-in prompts; and so on.
- **Windows Firewall with Advanced Security.** Specify settings to protect the device on your network by using a stateful firewall that allows you to determine which network traffic is permitted to pass between your device and the network.
- **Network List Manager Policies.** Specify settings that you can use to configure different aspects of how networks are listed and displayed on one device or on many devices.
- **Public Key Policies.** Specify settings to control Encrypting File System, Data Protection, and BitLocker Drive Encryption in addition to certain certificate paths and services settings.

- **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.
- **IP Security Policies on Local Computer.** Specify settings to ensure private, secure communications over IP networks by using cryptographic security services. IPsec establishes trust and security from a source IP address to a destination IP address.
- **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.

1.7. Using appropriate utilities to check strength of passwords and its complexity rules

1.7.1. Best Practices for Password Strength

Before you use password strength checkers, you need to understand a critical aspect of identity and access management: password best practices. After all, what good is a password validation tool if you don’t know how to compose a strong password?

Critically, most password strength checkers judge credentials based on two key factors: strength and complexity. The longer the password, the more time a cracking program requires to uncover it. A password of twelve characters proves far more secure than a password of eight characters. Therefore, your enterprise should mandate minimum passwords of at least ten characters and allow for longer ones.

As for complexity, most users know the general requirements: include letters both upper and lower case, numbers, and punctuation. However, most identity and password experts recommend not using sequences in your passwords; hackers’ cracking programs can identify patterns easily and exploit them. Plus, using phrases and sentences often proves easier to remember and stronger for cybersecurity.

Other password security best practices include:

- **Don’t Allow Repeated Passwords**

Often, this proves easier said than done; many employees feel overwhelmed by the number of passwords they must remember to perform their jobs. Regardless, employees should never repeat passwords in either their professional or personal lives. More importantly, they should never cross-use their credentials.

The more a password appears across the web, the more likely it ends up in hackers' hands through other breaches. With these, hackers can conduct largely successful credential stuffing attacks.

- **Don't Allow The Sharing of Passwords**

This remains a persistent problem across enterprises of all sizes. Employees can and will share their passwords with others; often they do so to facilitate business processes and efficiencies. Of course, this leads to more insider threats and a loss of control over users' access. Put severe penalties in place for sharing passwords.

Additionally, forbid employees from writing down their passwords, either on physical paper or in document applications. That almost always leads to significant issues in the long term.

- **Don't Incorporate Personal Information into Your Passwords**

Stereotypically, birthdays often end up in users' passwords. However, this precept extends further than that. Social media research and other kinds of open personal information allow hackers to conduct significant research on their targets with minimal effort. Obviously, this allows them to inflict subtler social engineering and phishing attacks.

Less obviously, hackers can use this information to guess users' passwords. Usually, users create passwords they can remember easily which means drawing on their interests.

- **Remember Password Expiration Policies Don't Work**

Although many cybersecurity and identity management providers only now recognize the futility of password expiration policies. In fact, they can actually cloud your identity security protocols, as it creates more long term confusion.

Instead, identity management experts believe it better to mandate strong passwords and secure them rather than constantly expire them.

Secure Privileged Access Accounts as Well

All of the precepts described above apply equally to privileged users and regular ones. In fact, they may apply more to the former; hackers tend to target privileged access credentials more than regular ones because of the network power they wield.

At the same time, privileged users are subject to the same identity foibles as their regular counterparts.

1.7.2. Password Strength Checkers and Validation Tools

Of course, you should only use password strength checkers which you can trust. Obviously, a trustworthy validation tool should *never* store your passwords in any capacity; they should only process your passwords in the browser. Again, you should never input your password into sites you don’t trust.

Another important note is that almost all of these password strength checkers and validation tools call themselves educational tools; they provide non-binding advice and exist primarily to help users understand what they need to improve their passwords.

Therefore, you should use these password strength checkers as intended—to demonstrate why typical passwords don’t suffice in modern identity management. Provide them to your employees to help them determine how best to write strong passwords and push them away from weaker ones. Additionally, you can use them to help you formulate your own password policies.

We cultivated a clear list of password vaults we believe to be secure. However, you should do your own evaluation of these sites to ensure your users’ credentials’ safety.

Utilities to check strength of passwords and its complexity rules

A. Comparitech Password Strength Test

The Comparitech Password Strength Test provides a strong baseline for other password strength checkers. For example, the test can demonstrate how long hackers need to crack the inputted password.

This test evaluates passwords based on complexity, length, and can determine whether the password appears in the list of most commonly used passwords. As a bonus, this test hashes the passwords automatically, which isn’t always the case.

B. My1Login Password Strength Test

Much like the password checker above, the My1Login Password automatically hashes the password inputted; this helps establish trust with the validation tool. Also, it too gives an estimate on the time needed to crack the password.

However, My1Login offers much more conservative timeframe estimates. A super complex password labeled as 13 sextillion years to crack only requires hackers two years to crack, according to this tool. If anything, this could be a sobering reminder of the relative security of passwords.

C. Thycotic Password Strength Checker

The Thycotic Password Strength Checker can also recognize the most common passwords and warns against them. Further, it can identify dictionary words, recognizes repeated patterns of characters, and suggest ways to improve password strength.

D. LastPass: How Secure Is My Password?

From one of the most prominent of password managers, we wanted to include LastPass to emphasize the potential of password management. Such tools when paired with other identity and access management solutions can help employees deal with the myriad password demands of their day-to-day business processes.

1.8. Identify Security Gaps

1.8.1. 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 10 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).

Smart Card

Windows 10 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 smartcard 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.

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.

Self-check-1

Directions: Answer all the questions listed below.

1. User Access Control is defined as ___________

A. the tools with which users access the controls of the systems within an organization.

B. the components with which users access the controls of a system's resources and database.

C. the capacity of a user to allow or deny a system or an object access its organization.

D. the capacity of an organization and its systems to allow or deny a user or an object access its systems and resources

2. UAC comprises of three main components: _______________

A. Authenticity & Authoritarianism, Authorization and Accountability

B. Identification & Authentication, Authorization and Accountability

C. Identification & Authentication, Authorization and Accountancy

D. Identification & Authentication, Impassibility and Accountability

3. Consider the following password policy: Password must be at least 8 characters long, contain a capital letter, a special character, a numeric character and no similar username phrases. Which of the following is considered a strong acceptable password for the username: Herod45 under this policy

E. A. herod76 B. claire*5647 C. Yasmany@12 D. 3456yelloW68

Directions: Answer all the questions listed below.

1. ___________________ is the process of verifying the identity of people who are attempting to access the network or system.

2. ____________________ are rules that administrators configure on a computer or multiple devices for protecting resources on a device or network.

3. __________________________ prompts are color-coded to be app-specific, enabling for immediate identification of an application's potential security risk.

Unit Two: Detect and remove destructive software

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

- Defining and identifying common types of destructive software
- Selecting and installing virus protection and scheduling compatible with current operating system
- Describing advanced systems of protection
- Establishing maintenance practices
- Installing software updates on a regular basis
- Configuring software security settings to prevent from infecting computer
- Running and/or scheduling virus protection software
- Reporting detected destructive software
- Removing destructive software

This guide 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
- Describe advanced systems of protection
- Configure software security settings to prevent from infecting computer
- Report detected destructive software
- Remove destructive software

2.1. Destructive Software

2.1.1. What is destructive software's

Destructive software isreferred toasmalware (malicious software) and the term includes viruses, worms, logicbombs,rootkits, Trojan horses, adware, key stroke loggers and spyware. Malware is software designed to in filtrate a computer system without the owner's informed consent; hostile, intrusive, or annoying software.

Data-stealing malware isa 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, screens crapers, spyware, adware, backdoors and bots. Malware's most common path way from criminals or malicious developers to users is through the Internet: primarily by email and the Worldwide Web.

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

2.1.2. The Common Types of Destructive Software

The common types of destructive software are:

- **Virus**

A **computer virus** is a piece of malicious code that has been designed to replicate itself when introduced into any computing environment (its host). This host could be another computer program, the computer's operating system partition, a document, or a removable drive. The virus may be knowingly or unknowingly spread by the user or administrator of the infected system. Once the virus has successfully infiltrated the system, it may replicate itself in a way that adversely affects the system's available space and performance. It also may infect other programs or software installed on the host, causing system disruptions, instability, unauthorized modifications, or disability of core functions and processes. Viruses can also copy, delete, or encrypt files. Some viruses lay dormant, waiting to be triggered by some user or system action. Others are activated immediately and commence the corruption of system programs and software in the various ways described above.

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.

2.1.3. Virus Origin, History and Evolution

History of Viruses

One of the most recognized terms in the world of cyber security is *computer virus*. Like any dangerous biological virus brings alarm to a scientist, the term computer virus brings fear to the administrators or users of any computer system. Viruses are never a pleasure. So where did viruses come from? Where and when did they start? How did they grow to become as menacing as they are today?

1940-1966: The Birth of Replicating Automata

Replicating Automata is a mechanism that has the ability of self-multiplication. Its birth came from mathematical and intellectual curiosity and not from malicious intent. This thought was initiated in the 1940s and subsequently published in a 1966 paper by mathematician John von Neumann. In this paper, he documented the possibilities of developing a piece of code that could copy itself, infect its host just like a biological virus, and cause any number of threats to the host system.

1971: The Creeper Program

In 1971, Bob Thomas of BBN created the very first virus, the **Creeper Program**. It was the first actual test of the Replicating Automata concept to see whether it was possible. He was successful and it worked. On each new host it infiltrated, it replicated itself, infected the hard drive, and tried to remove itself from its previous host.

1974: The Rabbit Virus

In 1974, the **Rabbit Virus** was developed. This time malicious intent was ingrained in its code. The virus replicated itself within its host and caused system disruptions that adversely affected overall system performance. This continued until complete system failure or crash was achieved.

1975: The First Trojan

In 1975, John Walker, a computer programmer, created the first Trojan. A **Trojan** is a computer virus that cannot replicate itself but instead, propagates itself by attaching to user programs, files, or games that are transmitted or exchanged. It is then executed primarily through end-user activity. Around this time, there were a number of popular games called **Animal Games**. These games used a set of questions to decipher what animal a user was thinking of. John Walker created a version of this game that became very popular among his friends and colleagues. With no internet and smart devices at that time, it was distributed using magnetic tapes. Walker used this avenue to distribute the *Pervade* virus embedded in the game. Once the virus was installed on the host, it proceeded to snoop around and copy itself to all the directories on the existing host's file system. Although this was done without the host's knowledge or permission, its effects were not destructive.

1986: The Brain Boot Virus

In 1986, there was a computer store in Pakistan run by two brothers: Basit and Amjad Farooq. In their mounting frustration from people illegally copying their software, they developed a piece of malicious code called the **Brain Boot Virus** which would alter the boot sector of any floppy disk used to copy their software. This became known as the first PC virus, due to the increased development and use of the personal computer at that time.

Computer viruses and attacks have proliferated across the internet in recent years, as more people are becoming accustomed to using the World Wide Web as a vehicle of communication and file exchanging. Computer viruses were first termed simple ‘bugs' when systems were found to be crashing or incurred various technical problems. In the early 1940s, this wasn't a problem that could spread to other computers so easily since networking and linking computers through a large-scale computer communication system was not developed.

As more people became comfortable with developing programs and computer software on their own, it also became easier to share files and results with other people. Programmers and developers began to save information and code on disks, package it as software, and send it out to other users for small fees or free of charge. Opening these files and running the programs on independent computer was more acceptable without any scanning or checking; instead, at this time, computers were potentially vulnerable to a variety of threats and conditions**.**

The rise of hackers in the early 1980s became paramount as the U.S. government discovered various security breaches and Trojan horse programs attacking the country's important computer networks. In 1983, Fred Cohen of the University of Southern California termed the concept of a ‘computer virus' as any program that could modify other programs and possibly self-replicate. Virus defense techniques were then initiated by his research and other computer experts.

As computer networks evolved and established into the personal and business sector during the early 1990s, more people realized the need for the best antivirus software and shielding networked computers from potential threats. The increase in computer users also resulted in an increase of hackers and computer programmers who could develop and release malicious software, programs, and code. Antivirus software companies began developing counterattacks and highly secure software systems as early as 1995**,** and the Internet boom that followed shortly thereafter resulted in multiple downloads of secure software.

In 1999, the ‘Melissa' virus was one of the first sets of viruses that reached epic proportions of computer damage. At this time, thousands computer users began taking more control and installing antivirus software and suite packages to protect themselves from infection. Between 2001 and 2003, several “famous” worms and viruses were released to the public in a variety of forms; some were attached to frequently-downloaded images, while others were sent as e-mail attachments from suspicious third parties. The Code Red worm, the Nimda virus, and the Klez worm were just a handful of vicious viruses that spread throughout some of the top companies and personal computers at record speeds. In 2004, the MyDoom email worm damaged millions of computers by persuading people to open the e-mail attachment through a social engineering initiative.

The History of Computer viruses has had a parallel history with the boom of the Internet, and as more people are using the World Wide Web to stay connected, threats and security risks are on the rise. E-mal attachments, visiting suspicious websites and downloading free software all pose various risks depending on the security level of the computer. Norton antivirus programs can scan a computer user's system periodically, detect viruses and other threats, and help to eliminate and remove them from the system. The same programs can also prevent viruses and other forms of Internet based threats to infect the system with its real-time protection.

2.1.4. 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.

- **Electronic Mail (Email) Virus**

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.

2.2. Virus Infection, Removal and Prevention

2.2.1. 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 auto run 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.

2.2.2. Virus Infection Symptoms

Common symptoms of a virus-infected computer include

- A computer program disappears from its memory, especially if there is no known removal of the program.
- Unfamiliar music or sounds unexpectedly starts playing through the speakers.
- Icons appear on the desktop unrelated to any programs that are currently being installed, or new icons seem to appear when no software has been installed.
- An antivirus program will not run, or a new one will not install properly or at all.
- Previously installed antivirus programs will suddenly disable and can not be restarted.
- Files that have been recently opened suddenly have more than one extension, such as .exe, .vbs, .gif, or .jpg.
- Dialog boxes and menus seem to be distorted or different.
- Unusual error messages will pop up.
- Items are not printing correctly.
- Disk drives or disks become inaccessible.
- An application or applications are not working correctly.
- The computer isn’t running as well as usual, or the computer reboots on its own.
- The computer restarts continuously.
- The computer locks up frequently or stops responding.

- The computer seems to be losing processing speed.

Take caution with symptoms

All of these symptoms may be caused by viruses, worms, or Trojan horses; however, it's not the only thing that may be causing some of the individual symptoms. Some of the symptoms may be because of faulty hardware or software. Or, they may be caused by overburdening the processes (running too many programs at once) or the disk space (too many files on the computer). Or, an older computer just may be wearing down with age, and/or not keeping up with newer software and operating system.

2.2.3. Preventing viruses

There are several steps a person can take to make sure these symptoms do not appear on their computer. These include:

- **Modify behavior** – Most cybercriminals depend upon the ignorance of novice computer users to perpetrate their crimes. Become educated on how cyber attacks can happen. Never open an e-mail from an unfamiliar sender, and never forward on any chain-type e-mails. Never give away login and password information, even if it seems to be coming from a reliable source. And if a claim on a Web site sounds too good to be true, it probably is – and is probably hiding a cybercriminal.
- **Use reputable antivirus software** – As mentioned before, even the best antivirus software programs are fallible. However, they're still the best method of preventing malware attacks. They're also hand if malware does pass through, especially if it comes with removal and backup systems.
- **Keep computers update** – Make sure that all software, especially operating system software and your preferred Internet browser, contain the most up-to-date patches and updates. These are usually published to keep computers safe from the latest known threats.

Having a multi-point plan that involves various layers of protection is the best way to stave off attacks of viruses and other forms of malware.

2.3. Selecting and installing virus protection and scheduling

2.3.1. Installing virus protection

Installing virus protection or antivirus 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.

Based on research, these are the best antivirus:

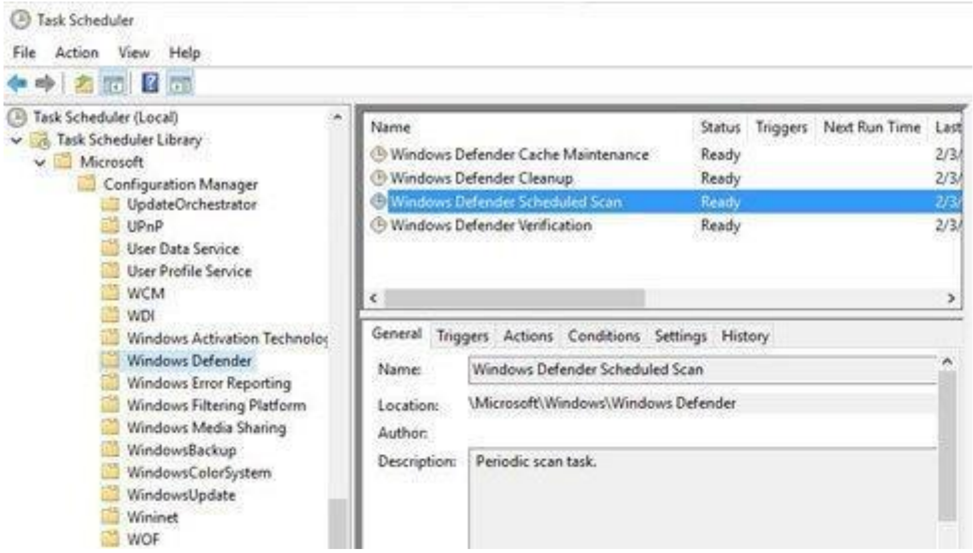
1. **Norton 360** – Best antivirus for individual PC and Mac users. Delivers well-regarded internet security that can include ID theft protection with LifeLock.
2. **TotalAV** – Best antivirus for web browsing protection. Actively scans for suspicious websites and monitors for criminal use of your private information.
3. **Intego Antivirus** – Best web protection for Mac users. The company is a rarity, focusing its services and builds primarily on OSX and iOS devices.
4. McAfee Total Protection – Offers well-respected protection for individuals or families.
5. **VIPRE Antivirus** – Consistently scores above more well-known brands in independent testing lab analyses.
6. **Bitdefender Internet Security** – Maintains consistently reliable performance and includes a webcam protection tool.

7. **Kaspersky Lab Internet Security** – Best selection of features. Includes a secure, encrypted browser for online shopping.
8. **Panda Antiviru**s – Among the only providers with an “unlimited devices” option for extensive device protection.
9. **ESET Internet Security** – Provides a highly-awarded internet security tool for every major operating system.
10. **Avira Antivirus** – Blocks phishing attacks on social media and email.
11. **Avast** – Analyzes app behavior for potential malicious activity
12. **AVG Internet Security** – Actively used by over 200 million people worldwide.
13. **Trend Micro** – Well-respected brand with a significant focus on business endpoint protection.
14. **Sophos** – Multi-device coverage with free option
15. **Webroot** – Incredibly feature-rich for the offered price.
16. **Comodo Internet Securit**y – No frills antivirus scanning and real-time protection

2.3.2. Schedule a scan in Microsoft Defender Antivirus

Microsoft Defender Antivirus regularly scans your device to help keep it safe. We try to do this while you're not using your device so it doesn't interfere with your work. You can also schedule Microsoft Defender Antivirus to scan at a time and frequency that you choose.

1. In the search box on your taskbar, enter **Task Scheduler** and open the app.
2. In the left pane, expand **Task Scheduler Library**>**Microsoft**>**Windows**, and then scroll down and select the **Windows Defender** folder.
3. In the top center pane, double-click **Windows Defender Scheduled Scan**.



Name	Status	Triggers	Next Run Time	Last
Windows Defender Cache Maintenance	Ready			2/3/
Windows Defender Cleanup	Ready			2/3/
Windows Defender Scheduled Scan	Ready			2/3/
Windows Defender Verification	Ready			2/3/

Name: Windows Defender Scheduled Scan
Location: \Microsoft\Windows\Windows Defender
Author:
Description: Periodic scan task.

4. In the **Windows Defender Scheduled Scan Properties (Local Computer)** window, select the **Triggers** tab, go to the bottom of the window, and then select **New**.
5. Specify how often you want scans to run and when you'd like them to start.

Self-check-2

Test 1

Directions: Answer all the questions listed below.

_______1. What is a computer virus?

A. A virus is John Walker code that has been designed to replicate files in the computing environment.

B. It is an infective digital agent that typically consists of nucleic acid bytes in the transport layer of the computing network and is able to multiply itself within the host causing disruptions.

C. A virus is Basit and Amjad Farooq code that has been designed to replicate the brain boot files in the computer.

D. It is malicious code that had been designed to replicate itself in its host causing system disruptions, instability, unauthorized modifications, or disability of core functions and processes.

_______2. The beginning of computer viruses stemmed from _____.

A. The Replicating Automata concept
B. The Bob Thomas theroem
C. The Basit and Amjad Farooq paper
D. The Onel de Guzman concept

______3. The first computer virus developed was the _____.

A. Creeper Program
B. Replicating Automata
C. Love Letter Virus
D. Brain boot Virus

Test 2

Directions: Matching Column A with the Column B.

ColumnA

______ 1. Logic Bomb

______ 2. Rootkit

______ 3. Adware

______ 4. KeyLogger

______ 5. Spyware

______ 6. Boot Sector Virus

______ 7. File Virus

______ 8. Macro Virus

ColumnB

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

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

C. A virus that attacks files on your computer and also attacks entire programs.

D. A virus that is designed to attack a boot sector, causing your PC to refuse to start at all

E. Typeover’s that are written specifically to infect Microsoft Office documents

F. Software that loads itself onto a computer and tracks the user's browsing habits

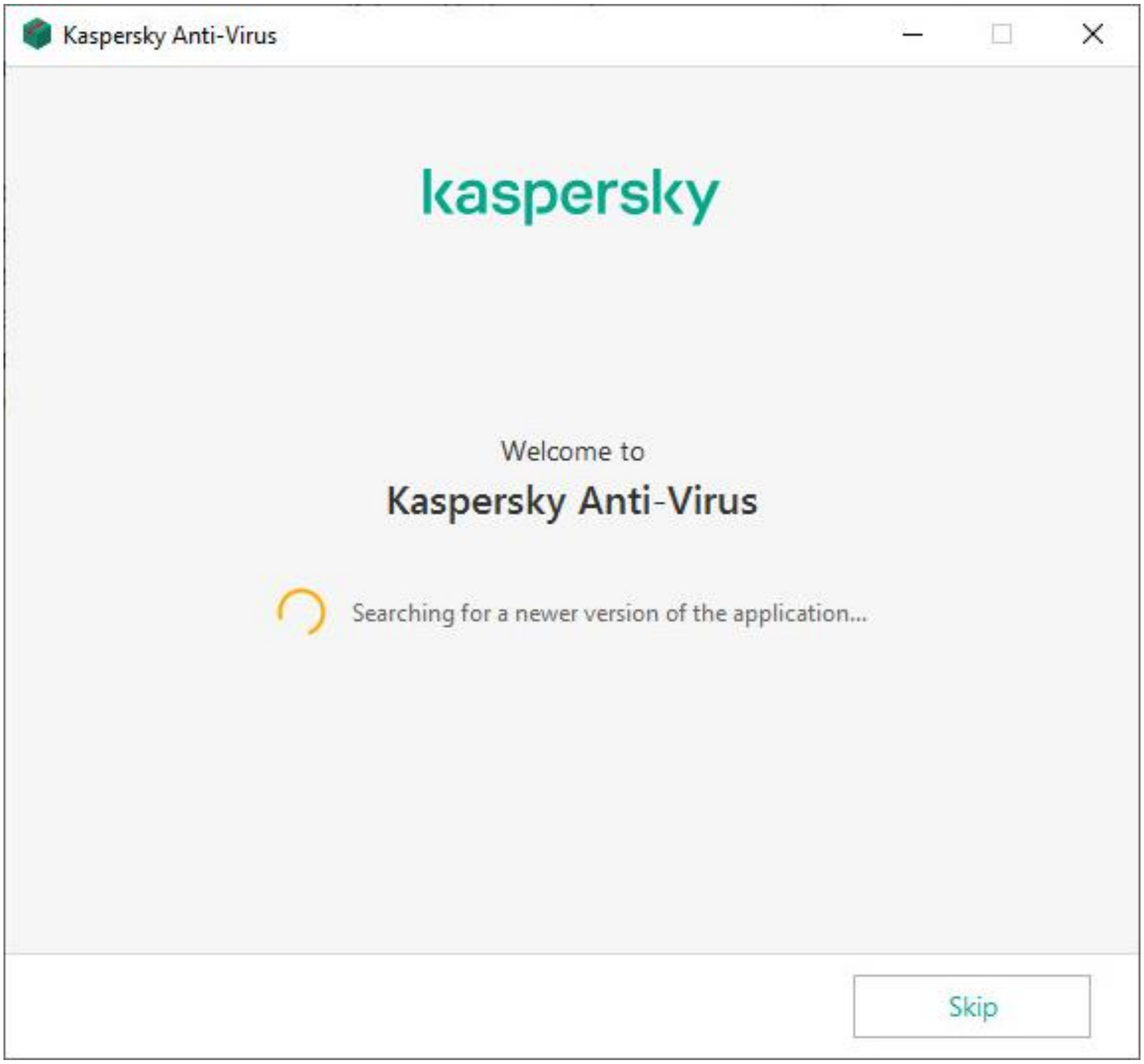
G. Practice of tracking the keys struck on a keyboard, typically in a covert manner

H. Setofinstructionsinsertedintoaprogramthataredesignedtoexecuteorexplode if a particular condition is satisfied

Operation sheet 2.1: Installing kaspersky anti-virus

- **Operation title: Installing Kaspersky anti-virus**
- **Purpose:** To Install anti-virus
- **Instruction:** Download the Kaspersky antivirus and install on your computer

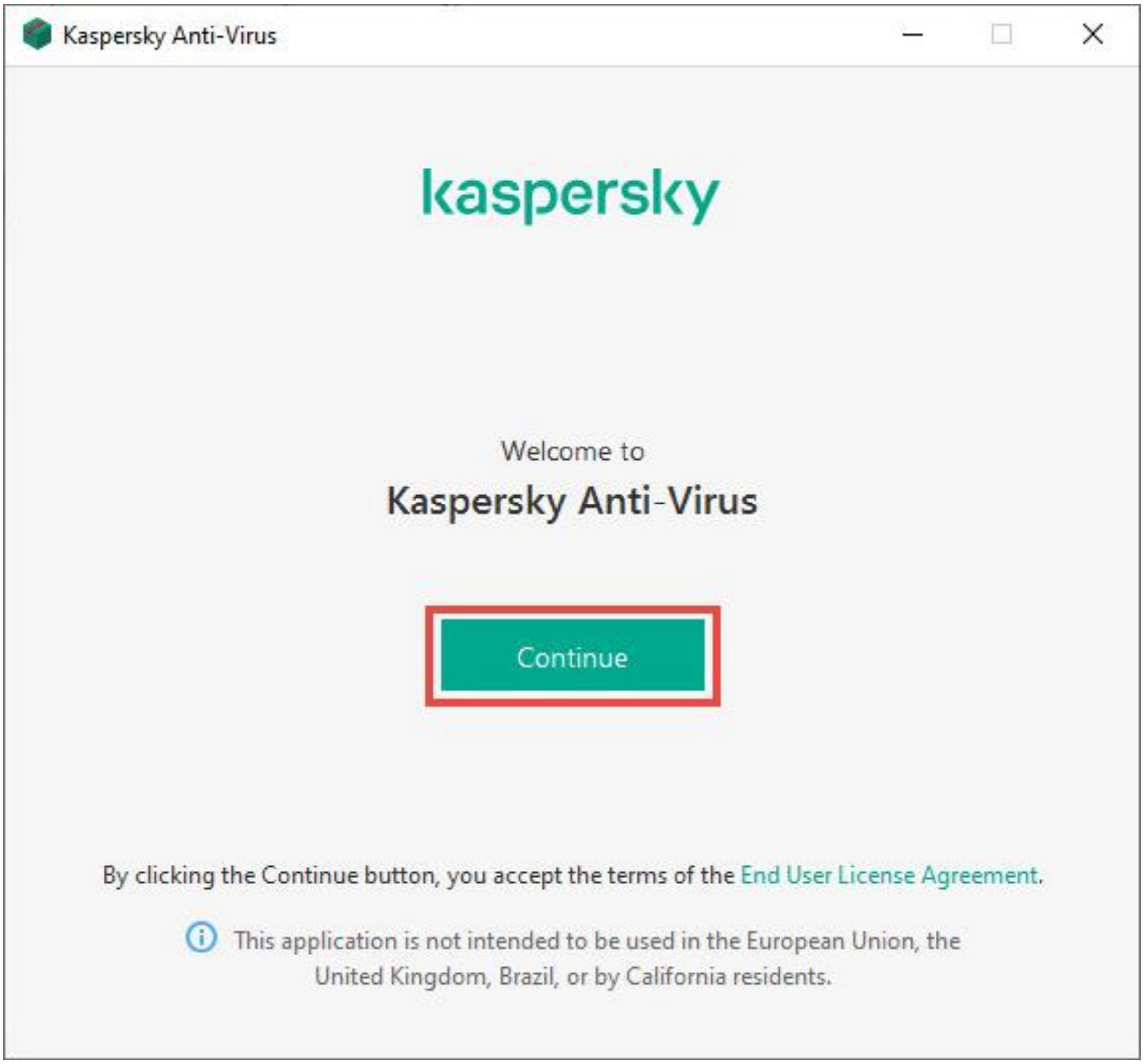
1. Download the Kaspersky Anti-Virus installer from the Kaspersky website, or via the link in the email you received from the online store.
2. Run the downloaded installer.
3. Wait until the wizard finds the latest version of the application or click **Skip** to install the current version.



Welcome to
Kaspersky Anti-Virus

Searching for a newer version of the application...

4. Click the link to review the License Agreement. If you agree to its terms, click **Continue**.



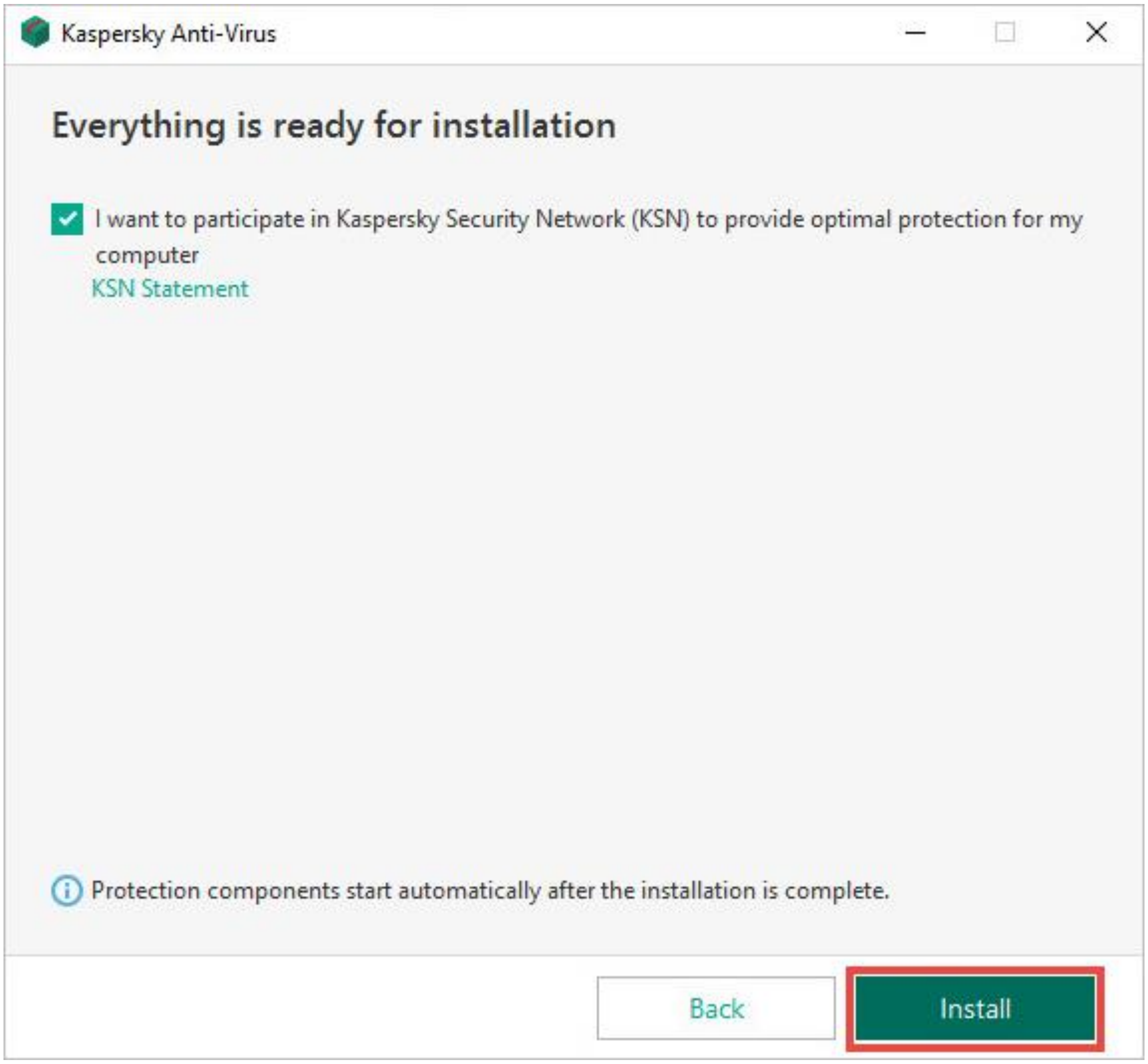
Welcome to

Kaspersky Anti-Virus

By clicking the Continue button, you accept the terms of the End User License Agreement.

This application is not intended to be used in the European Union, the United Kingdom, Brazil, or by California residents.

5. Click the link to review the KSN Statement. If you want to participate in Kaspersky Security Network, leave the corresponding checkbox selected.
6. Click **Install**.



Kaspersky Anti-Virus

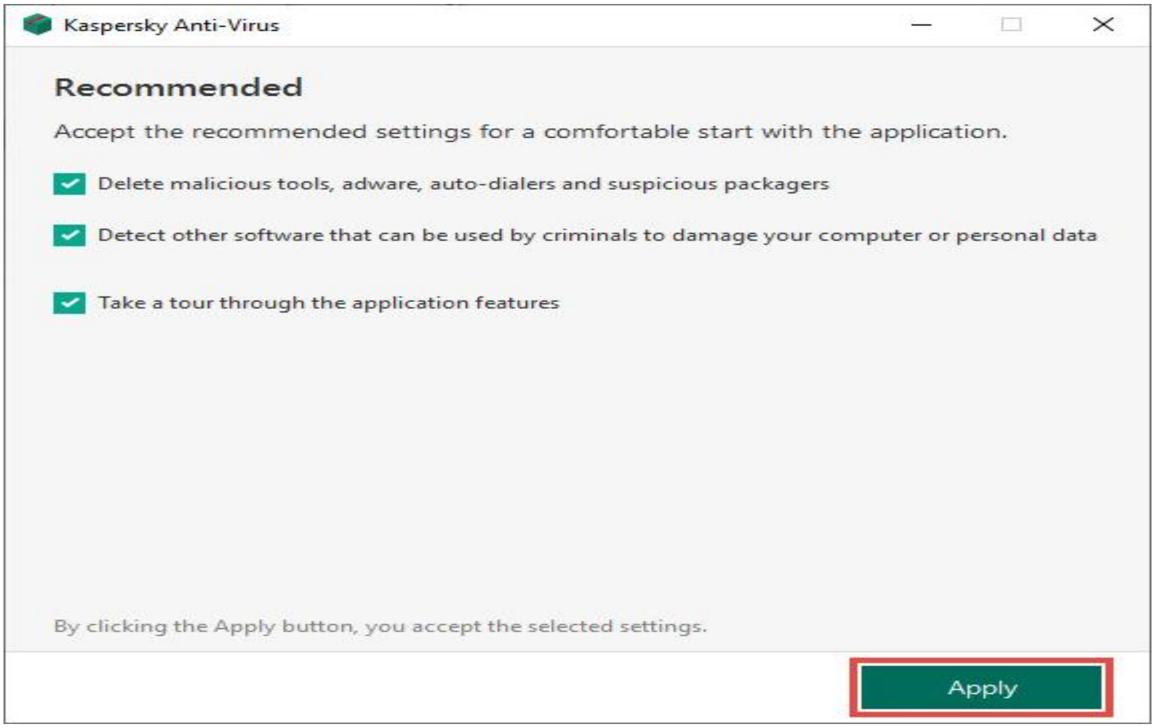
Everything is ready for installation

☑ I want to participate in Kaspersky Security Network (KSN) to provide optimal protection for my computer

KSN Statement

Protection components start automatically after the installation is complete.

7. Wait for the installation to complete. Make sure settings you want to apply are selected and click **Apply**.



Kaspersky Anti-Virus

Recommended

Accept the recommended settings for a comfortable start with the application.

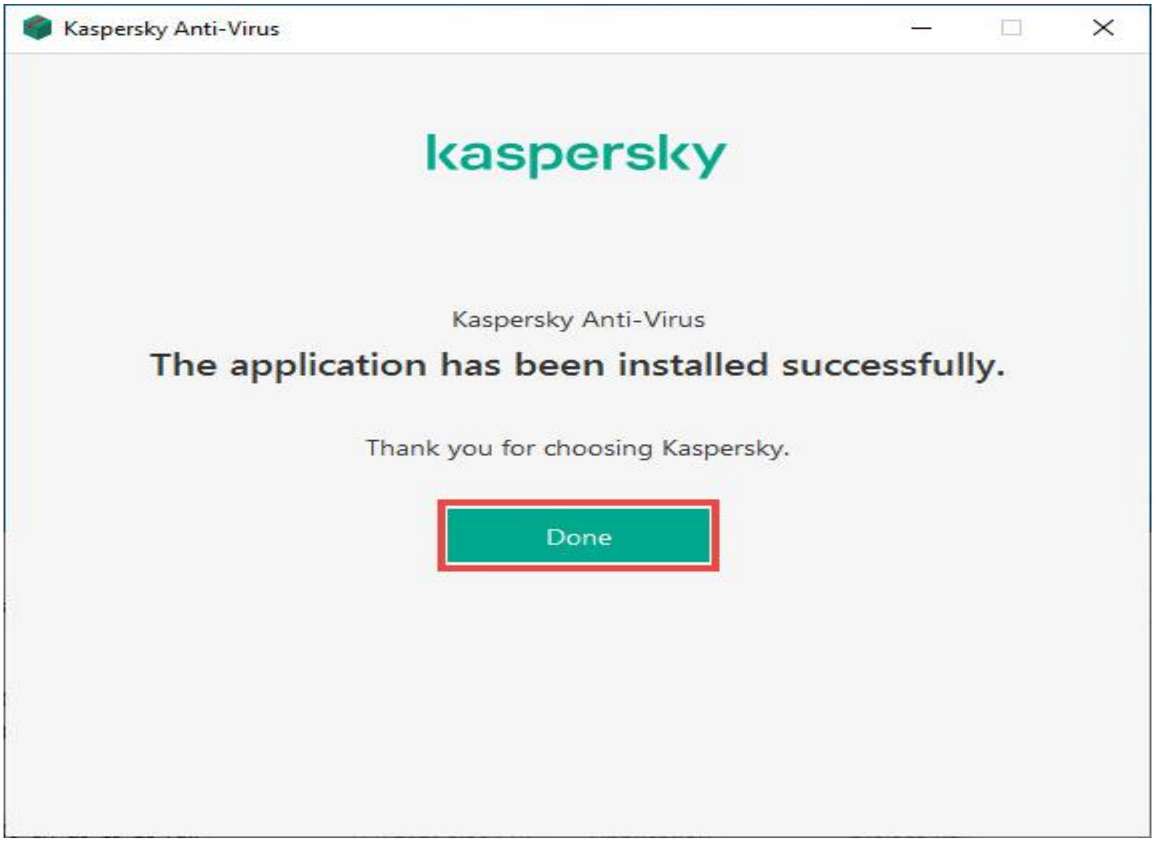
☑ Delete malicious tools, adware, auto-dialers and suspicious packagers

☑ Detect other software that can be used by criminals to damage your computer or personal data

☑ Take a tour through the application features

By clicking the Apply button, you accept the selected settings.

8. Click **Done**



Kaspersky Anti-Virus

Kaspersky Anti-Virus

The application has been installed successfully.

Thank you for choosing Kaspersky.

Lap Test -2

Instructions: Given necessary templates, tools and materials you are required to perform the following tasks

1. Install & Use kaspersky Antivirus

   A. Install kaspersky antivirus

   A. Auto Scan Schedule – Weekly every Monday and Friday at 4:00 AM

   B. Scan your storage drive

Unit Three: How to Identify and taking action to stop spam

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

- Defining and identifying common types of spam
- Taking Appropriate action to protect unauthorized access of spammers
- Configuring and using Spam filters
- Reporting and documenting Spams to identify the security threats and perform recommended action

This guide 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 spam
- Protect unauthorized access of spammers
- Configure using spam filter
- Report and document spams to identify the security threats

3.1.Definition of Spam

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.

3.2.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.

A. Phishing emails

Phishing emails are a type of spam cybercriminals send 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."

B. 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.

C. 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.

D. 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.

E. Malspam

Short for “malware spam” or “malicious spam,” 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, crypto miners, 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.

F. 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.

3.3. How can I stop spam?

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.

- **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 cybersecurity 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.

3.4. Configuring and using Spam filters

3.4.1. What is a spam filter?

A spam filter is a program used to detect unsolicited, unwanted and virus-infected emails and prevent those messages from getting to a user's inbox. Like other types of filtering programs, a spam filter looks for specific criteria on which to base its judgments.

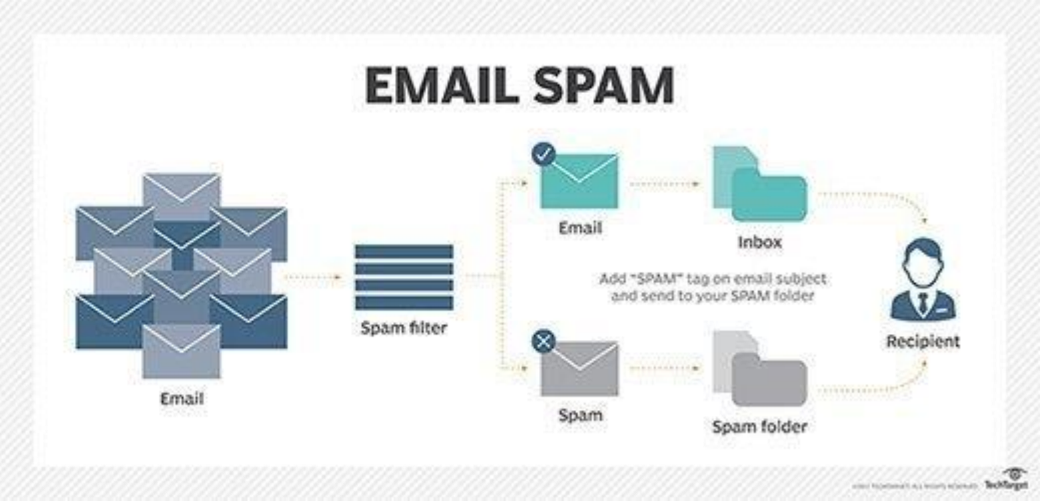
Internet service providers (ISPs), free online email services and businesses use email spam filtering tools to minimize the risk of distributing spam. For example, one of the simplest and earliest versions of spam filtering, like the one that was used by Microsoft's Hotmail, was set to watch out for particular words in the subject lines of messages. An email was excluded from the user's inbox whenever the filter recognized one of the specified words.

This method is not especially effective and often omits perfectly legitimate messages, called *false positives*, while letting actual spam messages through.

More sophisticated programs, such as Bayesian filters and other heuristic filters, identify spam messages by recognizing suspicious word patterns or word frequency. They do this by learning the user's preferences based on the emails marked as spam. The spam software then creates rules and applies them to future emails that target the user's inbox.

For example, whenever users mark emails from a specific sender as spam, the Bayesian filter recognizes the pattern and automatically moves future emails from that sender to the spam folder.

ISPs apply spam filters to both inbound and outbound emails. However, small to medium enterprises usually focus on inbound filters to protect their network. There are also many different spam filtering solutions available. They can be hosted in the cloud, hosted on servers or integrated into email software, such as Microsoft Outlook.

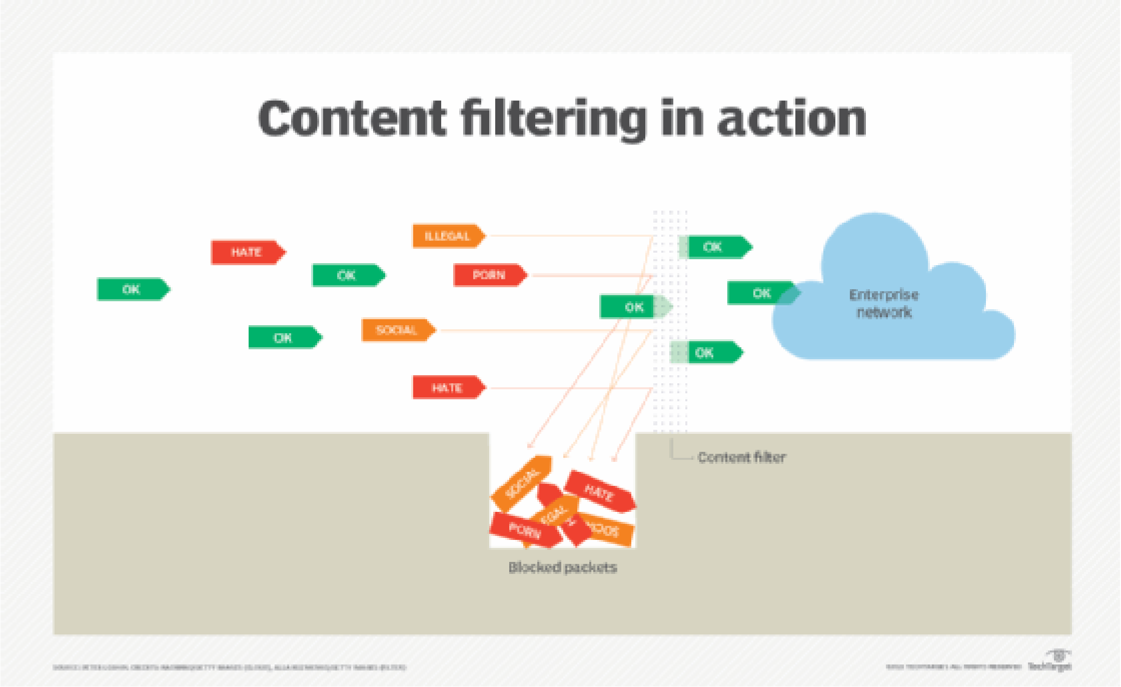


3.4.2. What are the different types of spam filters?

There are many different types of spam filters. The most frequently used filters include the following:

- **Blocklist filters.** Blocklist filters block spam emails from senders that have been added to a comprehensive spammers list. Blocklist filters are updated frequently to keep up with spammers who change their email addresses relatively quickly. However, if spammers switch their email domain, the email might be able to trick the system and penetrate the filter until it is identified once again as spam.
  Enterprises often create their own blocklist filter to protect their business interests. For example, they can block headhunters who seek to poach their top talent for the benefit of other companies, including direct competitors. They can also block emails deemed to waste their employees' time, e.g., emails with special offers.
- **Content filters.** Content filters examine the contents of each email and use that information to decide whether it is spam or not. These filters tend to work because spam email content is often predictable, offering deals, promoting explicit content or targeting basic human feelings, such as desire and fear. Those types of spammers tend to use target words, like *special offer* or *discount*, several times, which may trigger the filter. Some organizations also use content filters to examine emails for inappropriate language and block them accordingly.

- **Header filters.** Header filters analyze email headers to determine if they originated from a legitimate source. This includes IP addresses recognized as often used by spammers and data indicating that an email was part of multiple emails sent at once to preselected recipients.
- **Language filters.** Spammers often target people worldwide and, sometimes, send emails from geographic areas where the language is different from the recipient's native language. Language filters help block those messages, but if a business has a global customer base, it runs the risk of customer queries from another country going straight to the spam folder. As such, it always helps to check the spam folder when expecting such messages from global customers.
- **Rule-based filters.** Rule-based filters enable users to establish specific rules and apply them to all incoming emails. Whenever content matches one of the rules, it automatically forwards the email to a spam folder. The rules can be specific words or phrases in the message or header. This type of filter is often popular with users who receive unwanted emails associated with memberships because rule-based filters can also target particular senders.



Reporting and documenting Spams

Spam reporting, more properly called abuse reporting, is the action of designating electronic messages as abusive for reporting to an authority (e.g. an email administrator) so that they can be dealt with. Reported messages can be email messages, blog comments, or any kind of spam.

Acceptable spam report rate

An acceptable spam report rate is a metric set for how many of a company's marketing or status emails are reported as spam, also known as "junk mail," or unsolicited bulk messages sent through email.

Self-check-3

Directions: Answer all the questions listed below.

1. List and explain different types of spam filters.

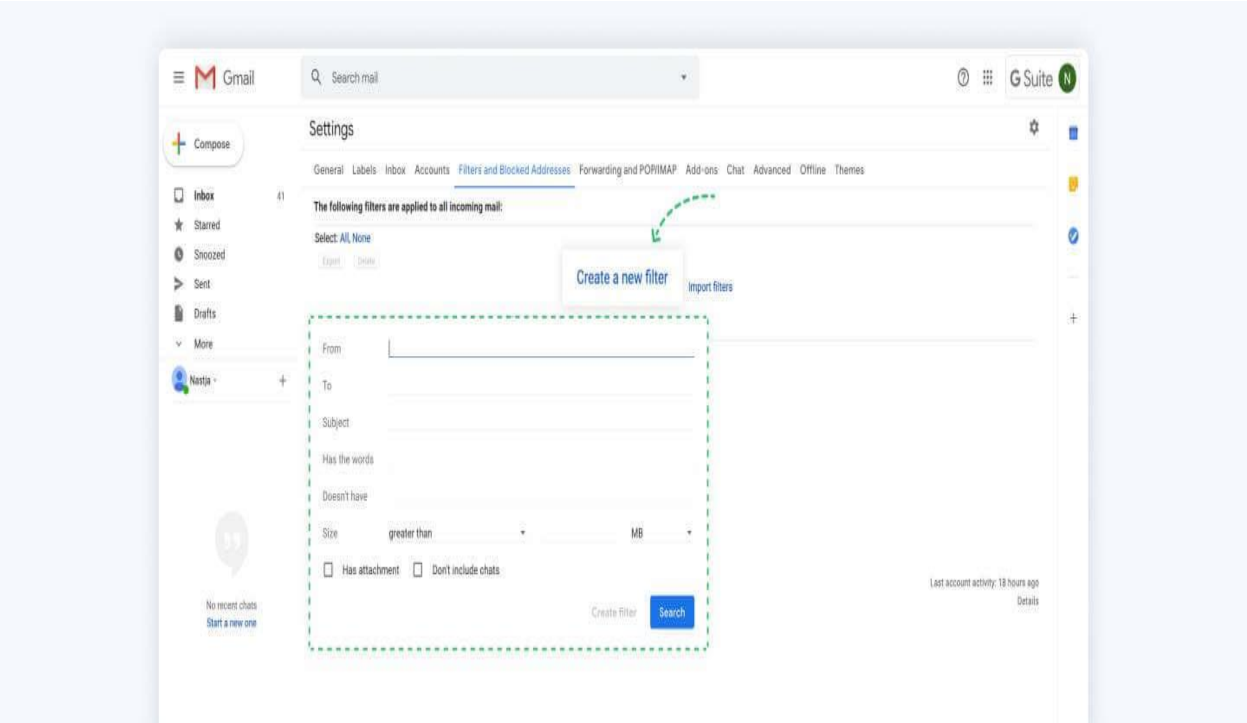
2. List and explain two types of Spam at least.

3. How can I stop spam?

Operation sheet 3.1: Set spam filter on Gmail

- **Operation title: Setting spam filter on G-mail Account**
- **Purpose:** To Set spam filter on gmail
- **Instruction:** perform the following task by follow the procedure below.
- **Equipment, Tools & materials:** Gmail account , internet connection
- **Procedure:**

1. Setting your spam filter in Gmail
2. Log in to your Gmail account
3. First, click on the Settings icon that looks like a gear.
4. Then, navigate to “Filters and Blocked Addresses.”
5. Choose “Create New Filter.”
6. Click in the “From” section, and type in the email address from the sender that you want to keep out of your spam folder.
7. Finally, click “Create Filter,” and you will now be able to view messages from this sender without navigating to the spam folder.



The following filters are applied to all incoming mail:

Operation sheet 3.2 Setting Windows local Security policy

- **Operation title:** Procedures of setting local security policy
- **Purpose:** To practice and demonstrate the knowledge and skill required to set window security policy
- **Instruction:** follow the procedure and complete the task

Note: You will need to be an administrator to open the Local Group Policy Editor.

The Local Group Policy Editor is a Microsoft Management Console (MMC) snap-in that gives a single user interface through which all the Computer Configuration and User Configuration settings of Local Group Policy objects can be managed. The Local Security Policy settings are among the security settings contained in the Local Group Policy Editor. An administrator can use these to set policies that are applied to the computer. In this project, you will view and change local security policy settings.

1. Click **Start**.
2. Type **secpol.msc** into the Search box and then click **secpol**.

Note: You may be prompted at this point for an administrator password or confirmation.

3. First create a policy regarding passwords. Expand **Account Policies** in the left pane and then expand **Password Policy**.
4. Double-click **Enforce password history** in the right pane. This setting defines how many previously used passwords Windows will record. This prevents users from “recycling” old passwords.
5. Change **passwords remembered** to **4**.
6. Click **OK**.
7. Double-click **Maximum password age** in the right pane. The default value is 42, meaning that a user must change his password after 42 days.
8. Change days to 30. After changing it to 30, take a screenshot and paste it below this step. Make sure your VM number in the top left is visible in the screenshot or no credit will be given for this step.
9. Click **OK**.

10. Double-click **Minimum password length** in the right pane. The default value is a length of 8 characters.
11. Change **characters** to **10**.
12. Click **OK**.
13. Double-click **Password must meet complexity requirements** in the right pane. This setting forces a password to include at least two opposite case letters, a number, and a special character (such as a punctuation mark).
14. Click **Enabled**.
15. Click **OK**.
16. Double-click **Store passwords using reversible encryption** in the right pane. Because passwords should be stored in an encrypted format this setting should not be enabled.
17. If necessary, click **Disabled**. After clicking disabled, take a screenshot and paste it below this step. Make sure your VM number in the top left is visible in the screenshot or no credit will be given for this step.
18. Click **OK**.
19. In the left pane, click **Account lockout policy**.
20. Double-click **Account lockout threshold** in the right pane. This is the number of times that a user can enter an incorrect password before Windows will lock the account from being accessed. (This prevents an attacker from attempting to guess the password with unlimited attempts.)
21. Change **invalid login attempts** to **5**.
22. Click **OK**.
23. Note that the Local Security Policy suggests changes to the **Account lockout duration** and the **Reset account lockout counter after** values to 30 minutes.
24. Click **OK**.
25. Expand **Local Policies** in the left pane and then click **Audit Policy**.
26. Double-click **Audit account logon events**.
27. Check both **Success** and **Failure**. After checking the settings, take a screenshot and paste it below this step. Make sure your VM number in the top left is visible in the screenshot or no credit will be given for this step.
28. Click **OK**.

29. Right-click **Security Settings** in the left pane.
30. Click **Reload** to have these policies applied.
31. Close all windows.

Lap Test -3

Instructions: Given necessary templates, tools and materials you are required to perform the Following tasks

1. .Turn on your Windows Defender Firewall
2. Turn on User Account Control

Unit four: Perform workplace duties following written notices

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

- Reading and interpreting written notices and instructions in accordance with organizational guidelines
- Following routine written instruction in sequence
- Giving feedback to workplace supervisor

This guide 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:

- Read and interpreting written notices and instruction
- Follow routine written instruction in sequence
- Give feedback

4.1.Receiving and Following Instructions

Receiving Instructions from someone else, especially if they are speaking to you:

- Stop whatever else you are doing
- Focus on the person speaking
- If you can, make notes about the details
- When the person has finished, tell them what you understood from their instructions to make sure you have understood them correctly

The instructions were not heard correctly due to:

- Too much noise around – ask to move to a quieter place
- The person not speaking loudly or clearly enough – ask them to speak up

Not enough detail was given:

- Ask for more information– don’t assume you know what they mean

The meaning was unclear:

- Check the outcome and the purpose of the task

4.2. Written Information Sources

In the workplace, written information can take the form of:

- Letters
- Memos
- Informal Notes
- Faxes
- E-mails
- Text Messages
- Workplace Signs
- Instruction Manuals

The following points should help you to follow written instructions in a more effective way.

- Read through all the instructions or steps before beginning the task. This will give a clear picture of what the whole tasks involves
- If diagrams are provided take the time to look at them carefully. As you work through the task check the diagrams to make sure that your work matches the example given.
- If you are not sure of the meaning of any words or terms take the time to find out the correct meaning. Ask your workplace supervisor if you guess correctly you may find that you cannot complete the task or that the finished task is not done properly.
- Avoid the temptation to try to complete the task before reading all the instructions. Although the job may take a little longer, it will save time in the long run as you may avoid mistakes.

Following Spoken Instructions

- Spoken instructions are generally received face to face or via the telephone. The following points should help you follow spoken instructions in a more effective way.
- When following spoken instructions, it is absolutely essential that you listen. Avoid jumping to conclusions or assuming that you know how to complete the task. Use all your listening skills to ensure that you receive the message accurately.
- Ask questions if you are uncertain about particular steps. Sometimes people are afraid to ask questions because they think they will look stupid. Remember questioning shows that you are keen and interested and it is always better to ask questions rather than make a mistake.
- Be sure that you understand all he words or terms being used.
- If you are receiving instructions over the telephone, always write down the information accurately.
- Repeat the instructions back to the instructor to be sure that you have fully understood all the details.
- It often helps if you can complete the task once with the instructor. This will give you a chance to ask questions and check other things as you work through the job.

Self-Check 4

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

______ 1. In the workplace, written information can take the form of:

A. Letters

B. Memos

C. Informal Notes

D. All

______ 2. ________ Instructions are generally received face to face or via the telephone.

A. Spoken

B. Written

C. A and B

D. None

Reference

https://www.techtarget.com/searchsecurity/definition/spam-filter

https://study.com/academy/practice/quiz-worksheet-history-of-computer-viruses.html

https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/how-user-account-control-works

https://support.kaspersky.com/15407#block1

https://edu.gcfglobal.org/en/basic-computer-skills/how-to-update-your-software/1/

https://www.studocu.com/row/document/adama-science-and-technology-university/management-information-system/protect-application-or-system-software/19989898

https://www.malwarebytes.com/cybersecurity/business/what-is-endpoint-protection

https://www.techtarget.com/search/query?q=reporting%20spam&type=definition&pageNo=1&sortField=

Participants of this Module (training material) preparation

No	Name	Level	Field of Study	Organization/ Institution	Mobile number	E-mail
1	Abel G/Egziabher	A	Computer Science	MOLS	0911776728	Ab.smart99@gmail.com
2	Endalew Kassa	A	IT	Debremarkos PTC	0913305454	crouchkecho@gmail.com
3	Frew Atkilt	A	Network & Information Security	Bishoftu PTC	0911787374	Frew_at@gmail.com
3	Getnet Alemu	B	IT	Nefasmewucha PTC	0922550906	Getnetalemu783@gmail.com
4	Remedan Mohammed	A	ICT	Harar PTC	0913478937	remedanm77@gmail.com