Chapter 6
Computer Viruses

Computer Viruses

Objectives

Main objectives:

1. Learn about the types of risks that threaten computers and data.
2. Learn about viruses in terms of mechanism of action and how to infect and deal with viruses.
3. Learn about data protection methods

Sub-Objectives

After studying this chapter, the student isexpected to master the following knowledge and skills:

1. Learn about the different types of risks that threaten computers and data
2. Learn about computer viruses and list their types.
3. Learn ways to protect data on computers and networks.
4. Learn the working mechanisms of viruses.
5. Learn to categorize different types of viruses.
6. Learn the methods of infection with viruses.
7. Learn the most common viruses
8. Learn ways to prevent viruses and how to get rid of them.
9. Learn the ethics of using a computer to protect data.

6 -1 Introduction to Computer Viruses

In the recent period with the development of computers and networks, the risks to the computer have increased, and among these types of risks are malicious programs and computer viruses. The virus is a program that was developed by programmers and is intended to harm or control the computer. The damage to the computer varies, including what destroys the computer by damaging the hard disk, including what damages part of the data.

Definition of a computer virus: a program that has the ability to spread between different computers by hiding itself in an application file or program, and it aims to infect the computer with specific undesirable damages.

Computer viruses are so called by this name because they resemble vital viruses, which are the microorganisms that transmit diseases to humans, including:

- Viruses always disappear behind another file, and when the infected programis run, the virus is run.
- Viruses are present in a basic place on the computer, such as the disk and memory-operating sector, and infect any file that is running while in the hard disk or memory, which increases the number of infected files.
- Sometimes the biological virus and the computer virus change their shapes to make them difficult to detect and overcome.

Skill 6 - 1
Knowing about the types of risks that threaten computers and data.

6 -2 Types of Computer and data threats

Almost, the computer on the Internet is not free of threats and risks, including hacking, spyware, hackers, and malware.

The risk is a threat to information inside the computer with a security vulnerability. Figure 6- 1 shows the types of risks that threaten the computer and data. This chapter will present some of these types.

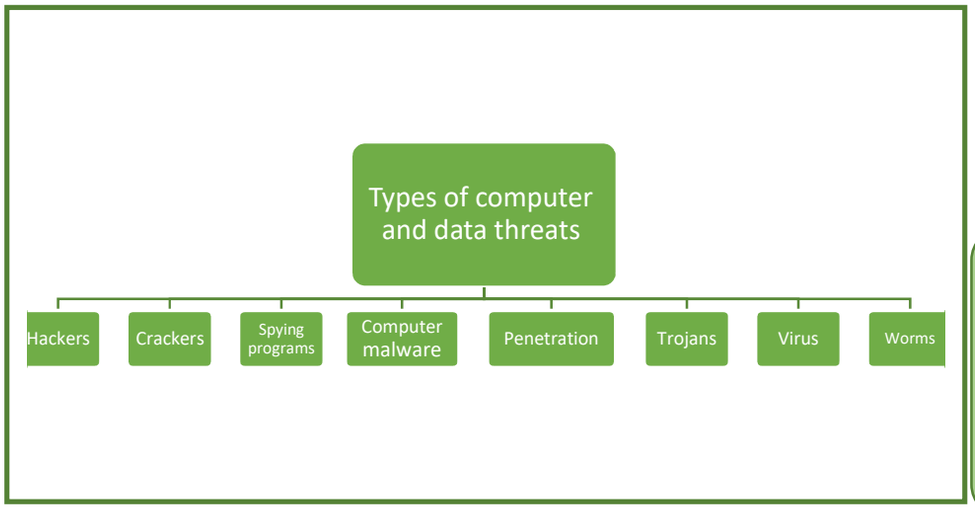


Figure 6-1: Types of risks to computers and data

6 -2- 1 Penetration

Penetration is the ability to enter information inside the computer illegally. The main reason for the penetration is the use of the Internet, with gaps in the system's protection system.Among the most important drivers of penetration:

- Obtaining money by stealing bank information.
- Obtaining personal information for the purpose of blackmail.
- Get secret email spy codes on personal messages.
- Obtaining the password for a website in order to destroy it or change its content.

Types of Penetration:

The types of penetration in terms of the method used are divided into three types:

- Penetration of servers of companies or government agencies by penetrating the firewalls that are usually placed to protect them.
- Hacking personal devices and tampering with the information, they contain.
- Exposing data during its transmission and identifying its code if it is encrypted. This method is used to reveal credit card numbers and to reveal bankcard numbers ATM.

6 -2- 2 Spyware

Spyware is software that aims to collect personal information about an individual or organization without their knowledge, which may cause data theft and slowdown in the computer. The stolen data can be passwords, for example. Methods of infection with spyware:

- Through electronic chat sessions.

- Through the Email.
- When downloading programs or files from untrusted sites.
- By using infected volumes.

6 -2- 3 Hackers

Hackers are ComputerExperts, who access hacked information, and they are intruders who challenge the security of network systems but the vast majority of them do not have sabotage motives.

6- 2- 4 Crackers

Crackers are people who are computer professionals or experts but who do illegal or legal activities, such as making a program for the purpose of theft, or making a program to obtain information in illegal ways.

Skill 6 - 2
Knowing about the types of malicious programs and their characteristics

6 -2- 5 Malicious Computer Programs

Malware is a small program that is insert into the computer system to damage it or destroy it. The risk may be simple to a defect that cannot be repaired except by scanning computer data, and they are several types, including viruses, worms, and Trojan horses. Figure 6 -1 shows these malicious types in terms of malware.

1. Worms: They are programs that reproduce themselves but do not contaminate other programs. They were made for the purpose of sabotaging or stealing data from computers during connection to the Internet, which is fast spread and difficult to get rid of.

Among the types of worms:

- Mail worms: They are attached to the message content and most types of these worms require the user to open the attached file in order to infect the device.
- File-sharing software worms: They spread by placing themselves in the sharing folders so that they spread among other computers.
- Internet worms: They transmit over the TCP / IP protocol.

Among its characteristics:

- Fast spread across networks.
- Diffused as an email attachment.
- It sends a copy of itself to other computers.
- It has remote execution capability.

- It has the ability to log in remotely.

2. Virus: Virus is a small program, which is programmed with the purpose of damaging the computer, moving from one computer to another, and also copies itself inside the device, interferes with the computer's operating system, and is programmed by professional programmers to ruin it, and damage to computers, or to achieve financial gains.

3. Trojan Horse: It is part of a program that is intentionally hidden inside a desired program section. When the user runs one of these programs, he activates the Trojan horse and does certain job that was designed for him. The Trojan horse can perform malicious or benign actions.

Most Trojans share the following characteristics:

- It has the ability to disappear.
- It works from a distance to steal data.
- It has powerful frauds. She has an unspoken skill to defraud.
- Automatic connection of computers via the network.
- Has the ability to self-repair.

Skill 6 - 3
Knowing about Data Security and advice to consider.

6.3 Data protection

The rapid spread of the computer and the Internet has created many problems related to how to protect data and provide the necessary security for it from viruses, malware, hackers, and others.

Owning the latest security technologies alone is not sufficient to guarantee comprehensive protection for programs, devices and data, but there is a set of preventiveprocedure,and things that all computer users must knowin order to be safe from viruses and hackers.

6 -3 -1 Elements of information security

Basic principles of information security Information security and protection depend on a set of basic principles that must be observed during the taking of procedures and measures necessary to protect information. The elements of information security are as follows:

1. Secrecy: means ensuring that information on the computer system is only accessible to authorized users.

2. Integrity: means ensuring that the information content is correct and has not been modified.
3. Continuationof availability: means the availability of the information system for authorized users.
4. Protect computers and protect computer networks from potential hazards.

6 -3 -2 Computer protection

Computer protection is a set of procedures to protect computer data and equipment. Computer protecting achieved by:

- Using a strong password.
- Using a firewall.
- Using antivirus software.
- Installing antivirus software.
- Updating antivirus software on a daily basis.
- Running an antivirus program on a daily basis.
- Updating the operating system constantly.
- Backing up files: backup important data to an external disk.

6 -3 -3 Protection of the internet

When a computer connects to the Internet, it is at risk. The risk includes stealing information, publishing information, or any other harm. Personal protection on the Internet is divide into two parts:

- Safety.
- Security.

Safety: It is the provision of protection to ensure the safety of the user himself from exploitation, extortion, violation or abuse. Security is the provision of protection to ensure the security of information, data and personal privacy. It includes file and hardware protection.

Internet Protection: A set of procedures to protect data within the Internet, including:

- Use of secure networks.
- Use trusted sites.
- Network Security: Ensure a strong password.
- Avoid websites that provide pirated material.
- Keep personal information secure.
- Do not use an open Wi-Fi network: Do not use an open Wi-Fi network. A malicious person can access data through the device.

Skill 6 - 4
Knowing the mechanisms of viruses.

6- 4 Mechanisms of Viruses

The mechanism of virus work is divide into four main stages: the passive stage, the launch phase, the spread phase, and the implementation phase. Figure 62- shows these mechanisms of virus work.

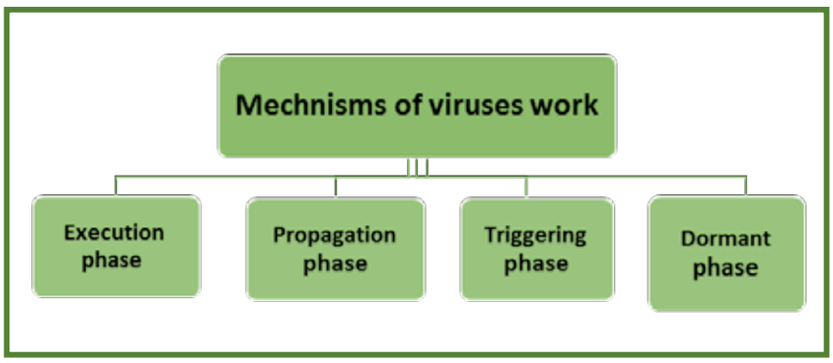


Figure 6-2: Mechanisms of viruses

After the virus program can infect a device, it enters the dormant phase in which the virus is inactive, but not all viruses have this stage.

Then, if certain conditions areavailable, such as a specific time or operation of a specific application, the virus begins in the triggering phase, where the virus is hidden in another program and is active with it, to perform the function for which it was made.

Most viruses pass through the latency stage immediately after infection, the damage does not appear on new infected programs, allowing the virus the time necessary to copy itself without noticing it.

Then the propagation phase iscoming, where the virus launches and adds its code to the original program and modifies its instructions so that the implementation moves to the virus code and when the infected executable is run, at which point the virus is active and the device is infected. The infected program becomes a source of infection and infects other programs.

In the execution phase, the virus is spread through files and the computer system.

Skill 6 - 5

Classify the viruses according to the target or hiding strategy.

6.5 Classificationof viruses

Viruses are classified into several categories.

- In terms of rapid spread, there are:
  - Fast-spreading, and
  - Slow-spreading viruses.
- In terms of timing of activity, there are:
- Viruses that are active at specific times, and Perpetualviruses.
- In terms of the location of infection, viruses infect a specific part of the computer, such as the operating sector virus.
- In terms of the size of the damage, there are destructive viruses for devices, such as the virus, that harm memory random access in the computer.
- There are harmless viruses that do not harmful for work.
- Depending on the target, which is a variety of viruses, each with specific features and attributes, such as macro viruses that infect documents in a Microsoft Office package.
- According to the hiding strategy such as encrypted viruses.

Generally, viruses classified into two classes, either by target or cache strategy. They classified into a variety of viruses categories, each one with specific attributes and characteristics.Figure 63- shows these types.

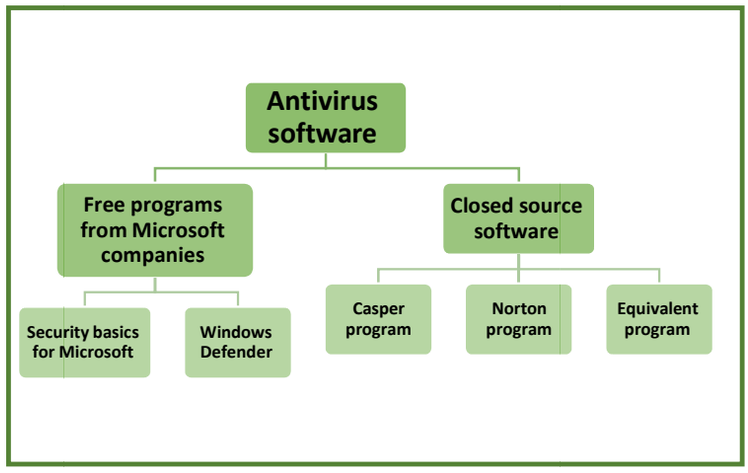


Figure 6-3: Types of anti-viruses

6.5.1 Classification of viruses by purpose

Viruses classified according to the goal into three types.

1. **File Infector Viruses:** This type of virus attaches itself as a file in any executable program, infects the executable in the volume and it inserts the infected code into an executable file, and it is spread across disks or across the network.

2. **Boot Sector Viruses:** These are viruses that infect the basic boot program on the disk (Boot Sector), and destroy its contents, which leads to the inability of the computer to boot or run and is considered one of the most dangerous types as it leads to the computer stopping work.

3. **Macro Viruses:** They are rapidly spreading among users especially that it is able to spread in all ways such as mobile and compact discs, email and free programs, they are viruses that infect application programs such as word processing macros and laziness macros.Macro virusesare characterized by many forms to comply with all files.

4. **Denial-of-Service(DoS**) attackDenial of service attacks are not a modern method, but the Internet has made them deadly and means that a group of computers attacks a single server with a very large set of commands that outperform the server's ability to Treatment in order to block the service.

From the types of DoS attacks:

- Attacks that exploit the Bug in TCP / IP build
- Attacks that exploit the default TCP / IP specifications
- Attacks that block traffic to your network so that no data can access or leave it.

To protect the computer from DoS, use (Dos.deny), which is a system designed to detect and respond to DDOS and prevent it from affecting the performance of servers or sites that use this system.

6.5.2 Classification of viruses according to the concealment strategy:

1. **Encrypted Virus:** A virus that uses encryption to hide itself from antivirus software. Encrypted viruses create a random encryption key that is difficult to detect by antivirus software.

2. **Stealth Virus:** designed to hide itself from an antivirus program, and it works on a strategy to hide itself in files where it displays a clean copy when scanning files, and works to change the properties of the hidden file.

3. **Polymorphic Virus:** a virus that is difficult to detect due to its transformation

with every infection, and it works on a strategy to use encryption to maintain itself.

4. **Metamorphic Virus**: transforms and rewrites itself at every repeat, making it more difficult to detect, and working on a strategy that changes its software, and reassembles itself into an executable form.

Skill 6 - 6

Knowing ways of transmitting viruses and their symptoms..

6- 6 Modes of transmission and symptoms of viruses

Most viruses today are transmitted using the Internet unless protection systems such as firewalls and virus protection programs are used, secondly storage media such as optical disks and mobile memory and thirdly in mail messages.

The computer virus is transmitted according to the method of spreading into two types: the direct infection virus and the indirect infection virus:

1. Direct Infector: When a program or file infected with a virus of this type is execute, that virus actively searches for one or more files to transmit the infection to it, and when one of the files becomes infected, it loads it into memory and runs it.

2. Indirect Infector: When an infected program or file is execute with a virus of this type, that virus will transfer to the computer's memory and settle in it, and the original program will be executed and the virus will infect every program that is loaded into memory after that. Until the computer is cut off and restarted.

Among the most important methods of infection with viruses are

- Open attachments from unknown and virus-infected emails.
- Download free programs from malicious websites.
- Anonymous ads online.
- Use of mobile volumes: Volumes such as portable and optical disks transmit viruses if inserted into an infected device.

Skill 6 - 7
Count the symptoms of infection with viruses.

6- 7 Symptoms of Infection with Viruses

When running the program infected with viruses, it may infect the rest of the files with it on the computer, and the virus needs intervention from the user in order to spread, of course the intervention is to run it after it was brought from the mobile disk or compact lending or via e-mail or the Internet.

The most common symptoms of computer virus infection are

- The computer slows down without any reason.
- The computer system contains less available memory.
- Creation of unknown programs or files.
- Some programs or files are lost.
- Some files are damaged.
- Restarting the computer in unusual ways.
- Some files or programs do not run correctly automatically.
- Display strange messages, music or sounds.
- Change the name of the hard drive or volume name.
- Inability to deal with some terminals such as CD and printers.
- The entire system collapses and the device is unable to operate.

Skill 6 - 8
Knowing ways to prevent viruses.

6 -8 Methods of virus protection

To protect the computer from the risk of infection with viruses, the following steps should be followed:

1. Install antivirus software.
2. Keep your antivirus software updated on a daily basis.
3. Scheduled checks should be done regularly with antivirus software.
4. Make a backup copy of the important data periodically to take advantage of it when the computer is infected can be retrieved.
5. Update the operating system.
6. Do not use an infected flash memory.
7. The Internet use is regulated.

6 -9 VirusesMonths

The emergence of viruses began to spread in the mid-eighties of the last century and since that time, it has evolved and started spreading abundantly, and at the end of the 90th the number of famous viruses reached thousands of viruses and it is increasing every day. Among the most famous viruses that spread quickly are:

1. Melissa Virus

Melissa Virus was the first virus to be transmitted via e-mail, and this matter was very frightening, as the prevailing belief at that time was that viruses could only be used if a user opened one of the files carrying the virus and attached to an e-mail.

2. Melissa Virus

One of the fastest viruses that spread in 1999. It is acunning type of viruses, specializing in email infection. It spreads by sticking to text programs as an attachment in the email message and once the user opens the file attached to the message only the virus begins to work as it can access the list of the user's private message begin to sends the same message to the first fifty addresses without your knowledge and continues to spread.

3. SoBig Virus

An anonymous email message that crashes computers when they open. This virus disrupted Newsweek when it first appeared in 2003.

4. Sasser Virus (SASR)

In May 2004, the virus infected 3.17% of the worldwide computers that run Windows operating system through the internet. This virus causes a delay in executing the commands that are given to the device and also closes the machine and reopens it.

5. Love Virus

A destructive computer worm that is spreading rapidly hit computers in 2000, exploiting a vulnerability in the Windows system and a weak e-mail system, but it specializes in infecting Microsoft Outlook's email management program and is characterized by its rapid spread

6. MyDoom Virus

A type of virus that attaches to an e-mail as a text file and re-sends itself to other e-mail addresses, as it spreads through music files, movies, and games over the Internet.The virus introduces a program that allows hackers and hackers to enter the computer and register everything that was printed starting from the

password to credit card numbers. This virus infected about millions of computers when it appeared in 2004.

6 -10 Antivirus software

Many anti-virus programs are available and can be used to fight viruses, worms, and Trojans. The antivirus program examines the computer for new viruses that have been infected and then clean these viruses to ensure that no more harm is done to the computer.Anti-virus programsbecomes useless facing new viruses unless the programsare updated from the company's producing website. Antivirus programs are divide into free programs from Microsoft, such as the basics of Microsoft's security and Microsoft's security, and closed source (non-free) programs such as Casper, Norton and McAfee. Here and later Microsoft anti-virus software are introduced. Figure 64- shows the classification of these programs.

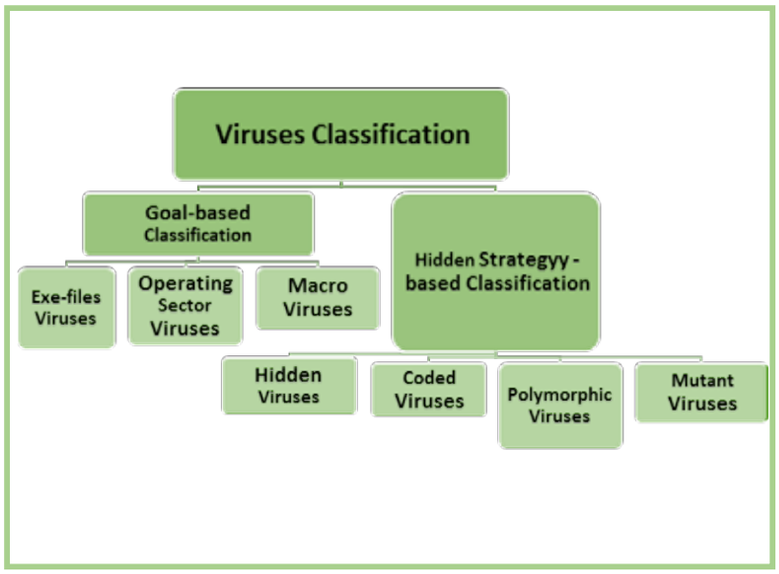


Figure 6-4: Antivirus software

6 -10 -1 Mechanism of Antivirus Working:

The following steps explain how antivirus work and how to get rid of viruses:

1. A virus is created and launched.
2. The virus infects a few computers and is sent to the antivirus company.
3. The antivirus company records a signature of the virus.
4. The company includes the new signature in its database.
5. When an antivirus scan is performed, the virus is detected, and the virus risk is reduced.

6 -10 -2 Microsoft antivirus software

A free software from Microsoft and provides computer protection from viruses, spyware and malicious files, and it includes two programs:

- Security basics for Microsoft Windows 7 and Windows 7.
- Windows Defender, which works with Windows 8 and above.

Skill 6 - 9
Identify and use Microsoft Security Essentials.
Microsoft Security Essentials.

Firstly: Microsoft Security Essentials

Microsoft Security Essentials is a free anti-virus program for devices running the Windows operating system. The anti-virus program was produced by Microsoft. Its mission is to protect the computer from the dangers of viruses, malware, and hacker attacks.

1. Features of the protection program - Microsoft Security Essentials

- A free program is downloaded directly from Microsoft, easy to use, and works very efficiently on the Windows operating system without stopping to keep the system protected from any threat.
- Provides a quick scan of the computer.
- Provides a complete scan of all files and programs.
- Provides a custom examination that includes the part to be examined.
- Fast and provides instant reports in case of danger to the device.
- The update process is done automatically.

2. Check the system

The Security Basics program provides Microsoft Scan options with Quick Scan, Full Scan, and Custom Scan. Figure 66- shows the scan options.

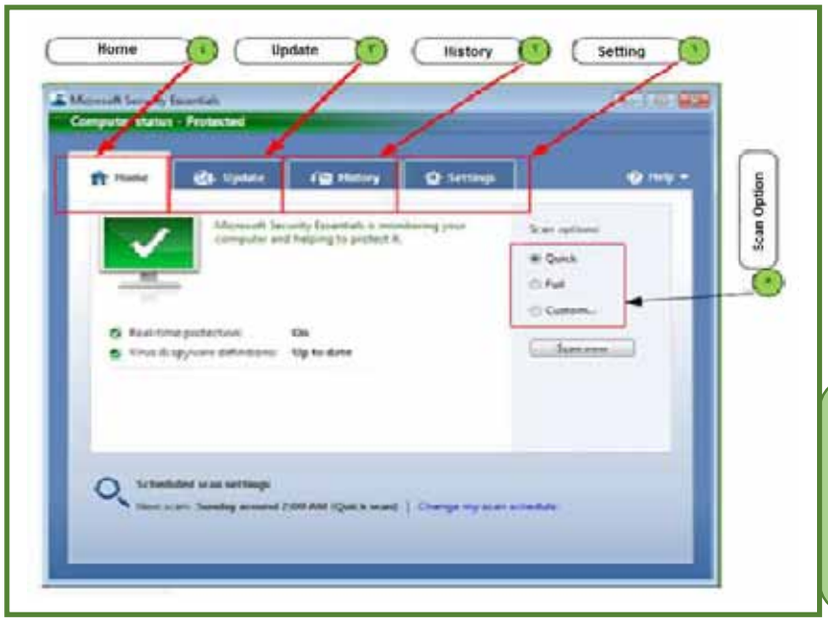
- Quick Scan: Quick Scan searches the places on your computer's hard drive that are most likely infected by malware.
- Full scan of the device: The full scan searches for all files on the hard disk and in all programs currently running, but it may cause the computer to slow down until the scan is complete.
- Custom Scan:Here you can choose the part of the data to be scanned.

3. The home page of the Microsoft Security Essentials program

It contains the settings icon for the system and an icon that shows the history of the checks that were performed on the system, and it contains search options, which are fast, full or custom searches, it contains icons that display the security status of the computer in the form of a green, yellow or red icon,

a . Green icon

This means that the computer's security condition is good, when the computer faces a lower threat, it will turn from green to yellow. Figure 6.5 shows that the symbol is green, which means that safety conditions are good.



:Figure 6-5

Microsoft Security Home Page

b. Yellow icon

Means that the situation is not protected, and that protection must be run in real time, or a system scan must be performed, whether it is fast, complete, or ad hoc. Figure 6- 6 shows the yellow icon and the user should scan for and remove viruses.

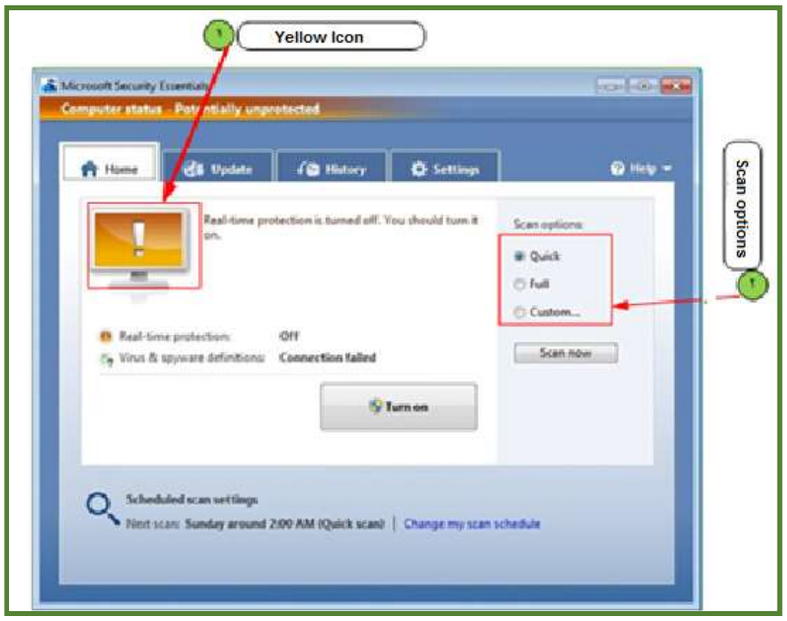


Figure 6-6:

The status is not protected in Microsoft Security

c. Red icon

The appearance of red means that the computer is in a very dangerous stage and that the program must be run to remove the danger. Figure 67- shows the red symbol meaning that the computer is in great danger and the computer must be checked and the threat removed.

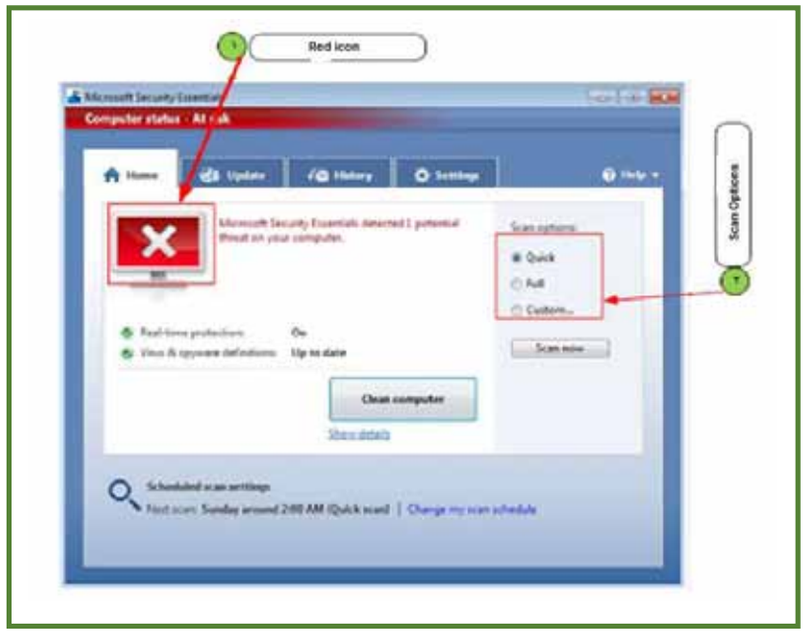


Figure 6-7:

The situation is in danger in Microsoft Security

Skill 6 - 10
Defining and Using Windows Defender

Secondly: Windows Defender Program

Windows Defender is an alternative to the Microsoft Security Essentials program that works to achieve protection for computers running Windows newer than Windows 8. As it is considered Windows Defender is one of the necessary and important programs that in turn protect files and get rid of harmful programs.

1. Windows Defender program features

- Provides periodic updates.
- Provides complete computer protection from viruses and spyware.
- Cleans the computer from malware and useless files.
- Effective protection while surfing the Internet.
- Easy to use user interface.
- The user interface supports multiple languages.
- Compatible with all modern Windows versions of Windows 8 and above.
- The program is free and available to all Windows users.

2. The main screen of the Windows Defender program

The main screen of the Windows Defender program contains a set of icons that indicate the security status of the computer in the form of a green, yellow, or red icon, depending on the case. Figure 6 -8 shows these elements.

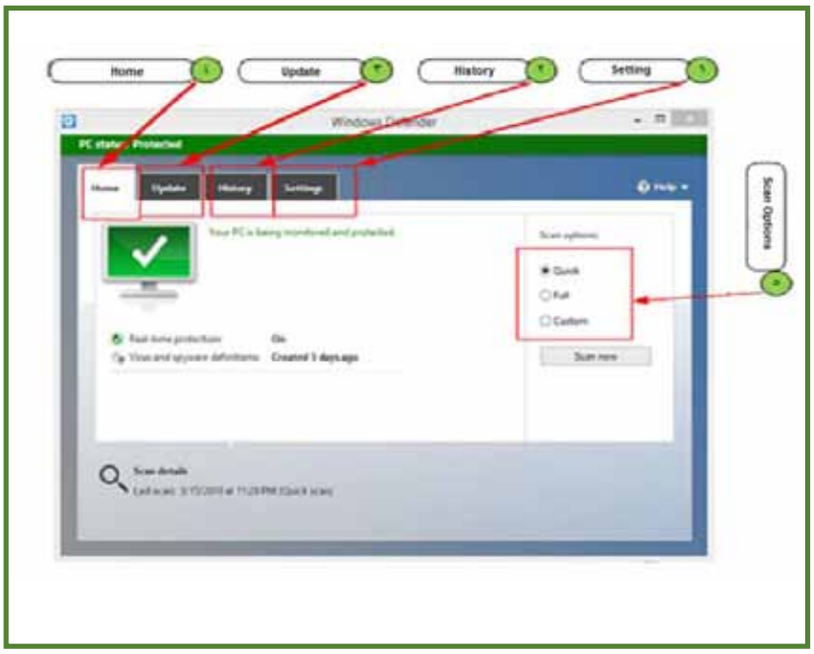


Figure 6-8 Basics of Windows Defender

1. How to use Windows Defender

There are several scanning methods provided by Windows Defender. Figure 6- 9 shows this.

v Full scan, custom scanand quick scan.

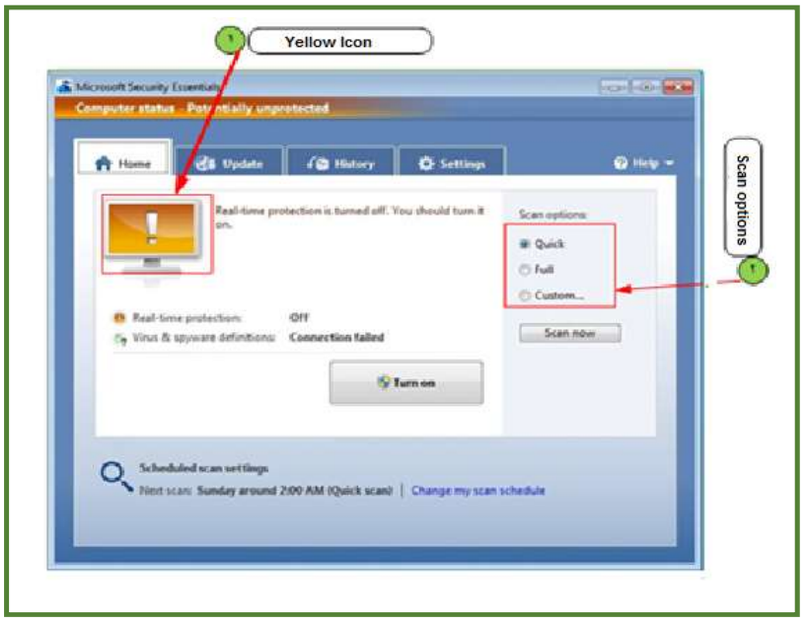


Figure 6-9:

The status is not protected in Windows Defender

a. Green icon

Green icon shown in Figure 68-, means that the computer security condition is good, up to date, and works in the background to help protect the computer from malware and other harmful threats.

b. Yellow icon

Means that the condition is potentially unprotected and some actions can be taken, such as turning on real-time protection or performing a system scan as shown in Figure 6- 9.

How Microsoft programs to remove viruses

To get rid of viruses the program does the following

- Step 1: Scan for viruses.
- Step 2: remove the virus and get rid of it, and if that is not possible, we use the "Format" device.

Skill 6 - 10

Learn about computer ethics and the most important commandments of computer ethics.

6- 11 Computer Ethics

Computer ethics is the way to deal with computers, it concerned with the moral and legal aspect. Computer ethics is used to describe the ethical principles that govern the process of computer use, which include ethical issues such as intellectual property rights (copyright, copyrights, patents) facing today's computer and information-based society.

The ethics of using a computer are many and varied, three main things that a computer user must know while dealing with it, including:

o Ethics of using a computer between a person and himself.

Among the ethics that must be characterized by the individual in this case is not to do things that negatively affect him, such as wasting time, and seeing the privacy of others.

o Ethics of using a computer between a person and a third party.

When working on a computer and the Internet, one should respect individual property, not steal other people's business, preserve the privacy and secrets of others, and not to others.

o Ethics between the user and the device.

It means maintaining the computer and complying with the laws that were put in place to benefit from its use.

Among the commandments of computer and Internet ethics, there are many ethics that a computer user must have.

- It is not permissible to use a computer to harm others.
- It is not permissible to spy on other people's data.
- It is not allowed to use the computer to carry out theft and fraud.
- It is not permissible to use a computer for forgery in documents or data.
- It is not permissible to use other people's computer resources without their permission or authorization.
- The computer should be used with interest and respect of the privacy of others.
- Commitment to confidentiality, pledges, agreements and labor laws.
- It is not permissible to copy other people's software and use their files without approval or without paying for these programs unless they are free.
- It is not permissible to use the Internet to send messages that are harmful to others, to interfere with their files, and to disable their devices.