Malware

Malware stands for two words **Malicious software** to infiltrate or destroy a computer system without the user's knowledge. Once installed, the malware can be difficult to remove. Depending on the degree of the software, its damage can range form slight inconvenience (some unwanted advertising windows while the user is working on the computer, connected or not connected to the network) to being irreparable requiring reformatting the hard drive, an example of malicious software are **viruses:** Computer viruses are small, external programs deliberately designed to change the properties of the files they infect, and they execute some commands either to delete, modify, or sabotage according to the goals they disguise, and it is stored inside the computer by one of the transmission methods to inflict damage on it and control it.

Damage caused by computer Malware:

1. Reducing the level of computer performance
2. Shutting down the computer and restarting itself automatically every few minutes or it fails to work after restarting
3. Unable to access the hard and compact drives(storage units) and the massage "unable to save storage units" appears.
4. Delete files or change their contents
5. Problems appeared in the installed applications and changes in application windows, menus and data
6. Frequent appearance of error massages in more than one application.
7. Disclose important personal information and secrets

Characteristics of computer Malware

1. The ability to replicate and spread, Replication
2. Connect itself to another program called the host
3. It can transfer from an infected computer to anther healthy one.

Malware components

This program is scientifically composed of four main parts that perform the following:

1. **The Replication Mechanism** allows the virus to copy itself
2. **The Hidden Mechanism** the virus it hidden from discovery
3. **The Trigger Mechanism** allows the virus to spread
4. **The Payload Mechanism** execute the virus when activated

Types of Malware

Malware are divided into three types:

1. **Virus** : an executable program (com, exe, bat, pif , scr) it works separately it aims to cause a defect in the computer, and its danger ranges according to the task for which it is designed , some are simple others dangerous, and it is transferred by copying files from a computer containing infected files to another via CD and flash memory.
2. **Worm :** it spreads only over networks and the internet, taking advantage of a list of e-mail addresses (such as the **Messenger** application), when the computer is infected the malicious program searches for addresses of people registered in the address list and sends itself to everyone on the list, causing it to spread quickly across the network.
3. **Trojan horse:** a virus whose working mechanism is an attachment to some programs, i.e. it is become a part of a program without the user's knowledge. This program was called the Trojan horse because it recalls the famous story of the Trojan horse. the Greek soldiers hide inside it and were able to storm the city of Troy and defeat its army

The most important steps needed to protect from Hacking

As long as the device maintains the computer against these files completely, it is very difficult to connect to the internet, but the computer can be protected by a large percentage and reduce the risk of infection by malware by following the following step:

1. **Use protected operating systems** of viruses such as Unix and Linux systems and their derivatives. These systems have been built in such a way that on external program can enter them except with the clear and explicit consent and knowledge of the user, and the basic system files are protected from any change or tampering , even by unintentional error.
2. **Install anti-virus programs** such as (Norton, Avira , McAfee Kaspersky) and anti-spyware program such as AVG anti-Spyware with recent versions and update eversion
3. **Maintain copies of important software** such as the windows operating system, the office package and a copy of the user's files.
4. Do not open any message or file **attached to an email coming from unknown person** to the user, or files with unknown extensions.
5. **Install Password** on the computer and the user's wireless network and change it every period, and only allow trusted users to connect and use the computer.
6. **Do not keep any personal information inside the computer** (such as private massages, photographs, important files and important information such as account numbers or credit card), store it in external storage media.
7. **Do not to run game software** on the same computer that contains important data and software, because it is one of the most frequently used programs between people and that is infected with viruses
8. **Making backup copies** of important and necessary files **and** stop the file sharing feature unless necessary.
9. **User knowledge about**: identifying viruses, ways they spread, how to protect from them, and the consequences of infection by them . this is done through continuous communication by visiting sites that are concerned with protection from viruses.

10. **Disengaging the connection between the computer and the modem** or the telephone line upon completion of the work . this prevents malicious programs that try to communicate from entering the computer.
11. **Activate the firewall :** the firewall checks the information coming from and out of the internet. It identifies the information received from dangerous sites or that arouse suspicion , and works to stop them . if the user sets up the firewall correctly, intruders will not be able to access these devices.

Risk computer on Health

Sitting for long periods in front of computer wrong sitting in front of a computer screen, and exposure to rays from this screen that affects the eyes, eyesight and skin. The best protection is to ensure the correct position of sitting in front of the computer while maintaining the screen position appropriately so that the user does not raise or lower his head to the computer many times.

- **physical and psychological Short-range effects**, including tension and eye muscle fatigue, and psychological anxiety.
- **Physical and psychological effects far reaching ,** which takes a longer period to appear, including muscle, joint and spin pain , a state of insomnia , psychological anxiety, psychological and social separation from the real world, living in a virtual environment , and imaginary relationships for those who are addicted to the internet. And the best prevention for this is to stop working with the computer from time to time , extend the legs and ankles , and do some light exercise to speed up blood flow and limit the hours of working with the computer at night.