Electronic Intrusion

It is the attempt by one or more unauthorized persons to enter (**access**) electronically to a computer or network via the Internet for the purpose of perusal, theft, sabotage and disruption using specialized programs.

Types of electronic Intrusion

The electronic penetration with respect to method used can be divided into three:

1. **The servers or main devices of companies, institutions, or government agencies** by penetrating the firewall, whose protection is set using simulation for the purpose of deception (Spoofing) it is a term used for impersonation to enter to the system, as the data packets contain address of the sender and the address of receiver, any these addresses are seen as acceptable and valid addresses by programs and network devices.
2. **Personal devices:** tampering with their information it is considered one of the common methods because of the inexperience with most of the users of these devices on one hand and the ease of learning and multiplicity of hacking software on the other.
3. **Data:** through exposure and identification of the data during its transmission and trying to open encryption if the data is encrypted. This method is used in the detection of credit card numbers and secret numbers of bank cards.

Sources of electronic Intrusion

1. **Intentional Sources:** that come from external parties trying to enter a device illegally, with a purpose that may differ according to the target device. An example of a common source :
   - ❖ Professionals and Amateurs : for the purpose of espionage without harming the computer.
   - ❖ Hacking communication network and its devices: for eavesdropping or free calls.
   - ❖ Hacking to post a specific program or to break a program to decode its source code (Crackers)
   - ❖ External enemies and competitors.
   - ❖ Professional criminals: in the field of computers and the internet

2. **Unintentional Sources:** that arise because of loopholes in computer software that may expose the device to the same problems that result from the deliberate dangers.

The most common security risks

a. **Viruses:** are programs designed to spread to computers in a wrong way and without the user's permission, and lead to sabotaging or disrupting the work of the computer or damaging files and data. And it will talk about viruses and their types extensively.

b. **Spywares:** are programs designed to collect personal information such as websites that the user visits, record their data and passwords for electronic account, as well as can obtain important matters for the user such as the credit card number without his knowledge

c. **Adware files**: its programs designed for advertising and changing general settings on computers, such as changing the browser's home page and showing some advertising windows while you connect to the internet and browse websites

d. **Lack of experience in dealing with some programs:** with the increase in the use of the internet by the general public who is not specialized, and their use and dealings with more advanced software for serving internet applications on an ongoing basis and without sufficient experience on

how to deal with these programs, it may open a loophole in the computer that enables others to penetrate the device.

e. **General Errors:** such as miss-choosing a password or writing it on a piece of paper, which enables others to read it , or leaving the computer open, allowing others (especially unauthorized or foreigners) to access computer files or change some settings.