10 Important Computer Terms to Remember

Published on Thursday, March 09, 2017

Virus:

It is a computer code that can make multiples of it and spread from one computer system to another system. A virus has the capacity to corrupt or delete data on your system and it can utilise an email program to spread the virus to other computers.In the worst case scenario, it can even delete
everything on your hard disk. The purpose of it is to disrupt the operation of the computer or the program.

Antivirus Software:

Antivirus Software is used to scan the hard disk to remove the virus from them. Some of the famous anti – viruses available are Avast, Norton, Avira, Kaspersky, AVG, etc.

Malware:

Malware is the short form of malicious software. This software is used to disrupt the operations of a system, gather information, or gain access to private computer systems. It can appear in the form of executable code, scripts, active content, and other software.

Computer Worm:

A worm is a malware program which creates multiples of its self to spread to other systems. Worms often use a computer network to spread itself. The rely on security failures on the computer which they have targeted to access it.

Trojan horse:

Trojan horse is a program that promises to remove viruses from your computer system but instead introduces viruses onto your computer. The term Trojan is taken from the Greek story of the Trojan War.

Authorization:

Authorization is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular. More formally, "to authorise" is to define an access policy.

Authentication:

When a single piece of data or a person is checked to confirm whether it is of true value, the act is known as authentication. The identity of an entity is confirmed by cross-checking the documents which prove their identity and on achieving successful results access is granted. Authentication often involves verifying the validity of at least one form of identification.

Hacker:

Hacker is a one who with the help of his or her computer knowledge takes control of the computer systems of others to obtain valuable information or to do damage.

Phishing:

The attempt to obtain information like usernames, passwords or details of credit card and sometimes money (indirectly) by promising to be a trustworthy entity in an electronic communication is popularly known as phishing.

Spoofing Attack:

A set of actions in which a person or program projects itself as something else successfully by providing false data and by doing so gaining an unfair advantage is known as spoofing attack.