**How to Protect Your Computer from the Cyber Attacks?**

The increasing amount of cyber hackers have also increased the threats to the data and information stored in the Computer system. The Cyber attacks can be of several types and can be from any corner of the world, but there are definitely certain ways to safeguard the exposure that your computer has from the cyber attacks.

The computer systems which we use now-a-days are far advanced, modern and hence secured than that of the one which we used decades back. There are several inbuilt tools and anti-virus installed with the windows package which are said to be a savior from all sorts of the cyber attacks but they are not as secured as said. There are always loop holes from which the attack takes place and the system software can’t even respond before which the data has been gone to other systems.

**The vulnerability analyzers**

There are several software available now-a-days which check the vulnerability of your computer system and get you some of the better results with which you can take measures to protect and safeguard your computer from all sort of cyber attacks. These vulnerability assessors are not any sort of anti-virus programs but these are the analyzers that check some of the settings which are regarded as the space for the hackers or any foreign substance to get into your system and that can steal or damage the information stored.

**Common forms of Cyber Attacks**

As stated by the Microsoft after extensive research by their R&D wing they have said to find some of the key forms of the network attacks that affect your system.

*Overhearing or Eavesdropping*

Most of the network communication takes place in an unsecured or a ‘cleartext’ format which enables the hacker or the attacker who already has got the access to the data paths of you network to “Eavesdrop” or read the traffic. The biggest security threat that most of the administrator face in an enterprise is the ability of the eavesdropper to monitor the network, by which he can track the in and out of your entire networking system and can easily trace the information shared.

*Password-Based Threats*

There are several older applications that do not protect the identity information of your system and hence it is exposed to the hackers to gain access by pretending itself as a valid user. When the hacker gets a valid user account, he has the equivalent authority as the valid user has and hence if he uses the real administrator rights he also can make accounts for the later access.

*The Sniffer Attack*

Sniffer is basically an application which has the capacity to read and capture the network packets and the data exchanges. A sniffer gets you the complete view of the data inside the network packets in case they are not encrypted. Even tunneled packets can be broken and the data stored inside can be read if not encrypted.

With the help of a sniffer, an attacker can:

* Crash or corrupt the network and gain the information stored.
* Read all the information and data files stored in your communication packets.

**How to protect the system from the attacks?**

Hackers are on their move to hack but there are also ways to safeguard your systems from getting affected due to the cyber attacks.

*Tighten up the security*:

Never try to be bold and handle things of your own. You need to concentrate on your work without worrying about the firewall updates. If you have a big set or an enterprise, you can hire professionals that keep a back up of all your data and automatically update the virus protection and malware software.

*Careful browsing*: Whenever you use internet, keep an eye on the internet pages that you visit. Virus can be anywhere and attack can be from any corner. By downloading wrong files you can invite the cyber attack. Keep a close check basically while dealing with banking and financial transactions.

*There are also several tools available that when installed gives you an immediate notice when finds a vulnerability in your system which could be a reason for an attack and it also gives suggestions to get rid of the loop being created knowingly or by default.*