When users go online, their personal information may be exposed in a number of different ways. For this reason, Internet security procedures should be understood and practiced by anyone who accesses the Internet.

Common Threats Faced by Users

The most well-known threats to Internet security are computer viruses. A virus is a self-replicating program that infects a device and makes a number of undesirable changes. Some viruses may attack the operating system of a device rendering it useless. Other viruses may delete data from within the hard drive. There are a multitude of known computer viruses, each with varying degrees of severity.

Spyware is another common type of malicious software. Some spyware tracks and monitors Internet usage for marketing purposes. The most dangerous spyware may include key loggers. These record and transmit everything that a user types. Hackers can then use this information to access a user's accounts and perpetrate identity theft and fraud.

How Users can Protect Themselves

Users can protect themselves by using the following Internet security protocols:

· **Use a firewall** - A firewall can help keep a network secure by controlling incoming and outgoing traffic by analyzing data-packets and using a predetermined set of rules. It can be hardware or software-based. Often, one can be found built directly into the user's operating system. Additionally, many broadband routers have rudimentary firewall capabilities built in.

· **Use anti-virus and anti-spyware software** - This software will analyze programs and files as they are downloaded on to the user's system. Users should also be sure to run frequent scans of their entire computer system to check for malware that may have slipped through, or that was not yet identified by the software. It is crucial that users keep their software up-to-date as new

viruses are frequently developed and identified.

· **Disable the ability to run scripts without permission** - some Web browsers will allow users to block scripting. Because scripting is needed for infected or malicious websites to install code onto a user's computer, disabling this ability will serve to protect users.

· **Monitor mobile devices for the presence of unauthorized software additions** - Users may occasionally be prompted to update an application on their mobile device that they do not remember installing. This may be a sign that their device has been infected. Users are advised to periodically look through the applications on their devices and delete any that are unimportant or that they do no use.

· **Block third-party cookies** - Most Web browsers make it possible for users to block cookies. While most cookies present no threat to the user, a few can. Blocking the cookies can provide a bit of security to a user.

· **Do not open suspicious emails** - Viruses and spyware can be embedded within an email. Sometimes, hackers will send an email that appears to be from a known source. Within the email will be a link. Clicking on the link can infect a user's computer and present a security risk. The link may also be a phishing scheme that will trick users into entering usernames and passwords into a bogus site.

· **Use strong passwords** - Users are advised to use strong passwords that include capital and lower case letters as well as numbers and special symbols. People should not use passwords that are easy to guess, such and names of family members or pets.

Most of the time when we start to communicate using computer with another computer, we are taking a risk. This risk perhaps may worsen when there is no protection. Thus, with the use of internet security, the computer's internet account and files from the computer are protected from any intrusion of any unknown users. Basically, it works well by protecting the computer through passwords, changing file permissions and backing up computer's data.

When it comes to the use of IT systems, internet security is very important to the business users because it makes them feel secured and confident from any cyber criminal attacks knowing that when they attack the IT system, it can be very profitable. This implies that business users need to be very vigilant from any attacks that may come to their way. In making decision on how to enhance and improve the system, security needs to be held from its requirements.

Before an internet security fully works, it should be fluent in the four major aspects which are: penetration testing, intrusion detection and incidence response. Also, it must be legally complied with the law.

A number of the useful programs contain features with hidden malicious intent. The following are some of the programs:

• Malware is the general term used for any malicious software designed. It is commonly used to damage or infiltrate a computer program or any other programmable device and system such as the home or office computer system, networks, mobile phone, PDA, automated device, robots, or any other devices that are sufficiently complex.

• Viruses are programs that enable to replicate their own structure or effect by incorporating itself to the existing files or structures on a penetrated computer. Moreover, it usually contains a malicious or humorous payload designed to threaten or alter the actions or data of the host system or device without consent. The common example of it is by deleting or corrupting the information from its owner.

• Trojan Horse or Trojan are programs that are stealing information, altering it or causing difficult problems on the computer or other programmable system or device by just pretending to do nothing.

• Spyware are programs that secretly keep an eye on the keystrokes or any other activity on the computer system and report the information to others without consent.

• Worms are programs that replicate itself on an extensive computer network. Thus, it also

performs some malicious acts that can eventually affect the whole system of the economy.

• Bots are programs that use the resource of a computer system by taking over it in a network without consent, and transmit that information to others who controls the Bots.

The different concepts above can overlap and be combined together. Thus, the terminologies, as well as the dangers involved, are continually developing.

In protecting the computer or any other programmable device/system, Antivirus programs and Internet security programs are commonly used to guard from any malware.

Such programs are commonly used to identify and extinguish viruses. When purchasing Anti-virus software by downloading through Internet, a caution should be done since not all programs are effective as compared to others in finding and eliminating viruses or malware. Additionally, when downloading anti-virus software over the Internet, buyers should be careful because some websites may say that they are providing the best protection from malware, but in reality, they are trying to install malware on your computer by pretending to be something else.