Internet based banking is one of recent revolutions in the world of banking that has revolutionized the method of banking transactions. Various banking institutions have gone electronic and are reaping the benefits of complete digitalization. Banking institutions have implemented proper security measures in order to make sure that the internet banking activities are carried on safely. However, it also becomes the responsibility of the customers to adopt certain security measures to safeguard their e-transactions. Certain internet security pointers should always be kept in mind while carrying on e-banking activities in order to thwart them from being a victim of cyber crime.

According to a recent survey, more than 60% of the active online banking customers have become a victim of unauthorized account access and other similar crimes in a last couple of years. Therefore, it has become quite essential to follow some simple internet security tips and safeguard the online financial activities. Further in this article, I have discussed some simple pointers that you should bear in mind while availing such e-services.

• First and foremost, you should try and keep you account password as well as pin number secret. Any information related to these two aspects should not be disclosed to any known or unknown individual. You should adopt the policy of changing the password after regular intervals of time and try to keep the same unique.

• Secondly, you should try to keep your system safe from web based threats. Internet security measures like installing up to date anti-virus software, in combination to software capable of removing the spyware, should be followed. Spyware remits your private information to the internet and the hackers can use this information to fulfill their evil desires.

• Installing updated versions operating systems as well as highly protective firewalls should also be one of your internet security strategies. These help in safeguarding your system from unwanted elements by acting as a barrier between the internet and your PC.

• You should also keep a regular check on your bank pass book and transaction statements in order to spot any transactions that may have carried on without your prior knowledge.

• You should always be alert and vigilant while accessing your online account from a public computer, office computer or internet cafe.

• Lastly, as an active internet security measure, you should always log off your e-account after completing the session. If the account is completely logged off, the crackers can acquire all the necessary details of your account and can even carry out unauthorized transactions.

So, these are some vital internet security tips that you must surely follow while surfing your internet banking account in order to stay safe from the reach of evil e-elements.

Features and tools are what make an internet security software program. The stronger they are, the more effective the internet security will be.

And in many cases, the less features and tools it has, then the less effective it is at malware (malicious software) prevention.

When you're looking for an internet security program, always look to see how the current version's features fare against last year's features and tools. The reason for this is that new and more harmful threats are released each year. And if your security product hasn't improved, then the latest virus and Trojan threats will circumvent its protection nets.

And another reason is that most major security programs update their features and tools so you don't want to waste money on a program that's not updating and therefore providing less protection.

Another thing to look for in your search for internet security software is how many new features and tools it releases each year.

Trend Micro, for example, released its cloud security a year later than other leading security programs so users of their software had to wait a whole year to use this crucial feature that provides added protection.

Then there're security programs like Panda that are missing some features like a gaming mode, home network manager, virtual keyboard and a secure virtual browser.

You can get by without some of these features and tools but your scope of protection will be limited.

Which brings us back to our question - Which internet security protection has the best features and tools?

Kaspersky has been identified as the software with the best internet security protection and here are some of the features in the software:

Antispyware

Kaspersky's antispyware feature protects from spyware, adware, Trojans, keyloggers, browser hijackers and other programs that are built to spy on your PC.

It's more effective than many standalone spyware removal programs and there're many reasons for this.

One of these is that its Intrusion detection tools block attacks by DLL (dynamic-link library) code injection. DLL is a malicious method that occupies the address space of a legitimate process and alters its behaviour from benign to harmful. An example would be a hacker assigning injected code the task of reading the contents of textboxes that hold passwords.

Antivirus

Kaspersky has been tested and approved by many leading test labs including AV-Test, a Germany-based testing organisation.

The test results show that it's one of the most effective at detection and removal of virus threats and at blocking them too.

Firewall

Kaspersky has a two-way firewall that allows you to connect to the web at home, at work, or on the road with confidence.

It automatically adjusts its settings to suit your present location and provide the level of protection you need.