***What is Data Security?***

In simple terms, data security is the practice of keeping data protected from corruption and unauthorized access. The focus behind data security is to ensure privacy while protecting personal or corporate data.

Data is the raw form of information stored as columns and rows in our databases, network servers and personal computers. This may be a wide range of information from personal files and intellectual property to market analytics and details intended to top secret. Data could be anything of interest that can be read or otherwise interpreted in human form.

However, some of this information isn't intended to leave the system. The unauthorized access of this data could lead to numerous problems for the larger corporation or even the personal home user. Having your bank account details stolen is just as damaging as the system administrator who was just robbed for the client information in their database.

There has been a huge emphasis on data security as of late, largely because of the internet. There are a number of options for locking down your data from software solutions to hardware mechanisms. Computer users are certainly more conscious these days, but is your data really secure? If you're not following the essential guidelines, your sensitive information just may be at risk.

***Encryption***

Encryption has become a critical security feature for thriving networks and active home users alike. This security mechanism uses mathematical schemes and algorithms to scramble data into unreadable text. It can only by decoded or decrypted by the party that possesses the associated key.

(FDE) Full-disk encryption offers some of the best protection available. This technology enables you to encrypt every piece of data on a disk or hard disk drive. Full disk encryption is even more powerful when hardware solutions are used in conjunction with software components. This combination is often referred to as end-based or end-point full disk encryption.

***Strong User Authentication***

Authentication is another part of data security that we encounter with everyday computer usage. Just think about when you log into your email or blog account. That single sign-on process is a form authentication that allows you to log into applications, files, folders and even an entire computer system. Once logged in, you have various given privileges until logging out. Some systems will cancel a session if your machine has been idle for a certain amount of time, requiring that you prove authentication once again to re-enter.

The single sign-on scheme is also implemented into strong user authentication systems. However, it requires individuals to login using multiple factors of authentication. This may include a password, a one-time password, a smart card or even a fingerprint.

***Backup Solutions***

Data security wouldn't be complete without a solution to backup your critical information. Though it may appear secure while confined away in a machine, there is always a chance that your data can be compromised. You could suddenly be hit with a malware infection where a virus destroys all of your files. Someone could enter your computer and thieve data by sliding through a security hole in the operating system. Perhaps it was an inside job that caused your business to lose those sensitive reports. If all else fails, a reliable backup solution will allow you to restore your data instead of starting completely from scratch.