Internet Security

Internet security encompasses the internet, browser security, web site security and network security as it applies to other applications or operating systems as a whole. Its objective is to establish rules and measures to use against attacks over the internet. The internet is an inherently insecure channel for information exchange, with high risk of intrusion or fraud, such as phishing, online viruses, trojans, ransomware and worms. Many methods are used to combat these threats, including encryption and ground-up engineering.

Network Security

Network security consists of the policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs: conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises and other types of institutions. It does as its title explains: it secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Data Security

Data security means protecting digital data, such as those in a database, from destructive forces and from the unwanted actions of unauthorized users, such as a cyber attack or a data breach.