**Digital Security**

Security, in IT is the defense of digital inform and IT assets against internal and external, malicious and accidental treats. This defense includes defection, prevention and response to threats trough the use of security, policies, software tools and IT services.

Physical security is the protection of personnel, hardware, software, networks and data from physical actions, intrusions and other events that could damage an organization. This includes natural disasters, fire theft and terrorism a many other threats to physical security may require less technical savvy on the part of the attacker, but physical security is just as important as information security.

Information security, also called infuse, encompasses a broad set of strategies for managing. The process, tools and policies that aim to prevent, detect and response to threats to both digital and no digital information assets. Infosec includes several specialized categoris including application security the protection of application from threats That seek to manipulate application and access, steal, modifity on delete data.

Basic digital security depends on two technique encryption and authentication. These techniqus are often combined to protect data from unauthorized access and to make data unintelligible if it’s somehow hacked.

Passwords protect digital devises from unauthorized access, and the protect user accounts at online banks. Web sites, and app stores. A strong password is difficult to hack. The Internet provides a wide variety of opportunities for communication and development, but unfortunately if also has it dark side. Hacker are computer criminals who use technology to perform a variety of crimes: virus propagation, fraud, intellectual property theft, etc. Hackers differentiate themselves into three groups:

A white hat hacker, upon finding some flaw in a system, will report the flaw to the vendor up that system.

A black hat hacker is the person normally depicted in the media.

A gray hat hacker is normally a law-abiding citizen, but in some cases will venture into illegal activities. Internet-based crimes include scam, email fraud to obtain money or valuables and phishing, bank fraud.

Malware is software created create to damage or alter the computer data or it’s operations. These are main types:

* Viruses are programs that spread by attaching themselves to executable files or documents.
* Worms are self-copying programs that have the capacity to move frame are computer to another without human help by exploiting security flaws in computer networks.
* Trojan horses are malicious programs disguised as innocent-looking files or embedded within legitimate software.
* Spyware, software designed to collect inform. From computer for commercial or criminal purposes, is another example of malicious software fraud – is an intention act of deception trough the presentation of false or minsteading information, iconic is done to gain an unfair advanteges or profit.

Unfair profit can be in The form of :

* Money
* Good services
* Sensitive inform.
* personal