Cyber security intro

Nist- is the ability to protect from cyber attacks

CNSS

preventing damage to all devices

Preventing the loss of information

INTEGRETY AVAILABILTY AUTHENTICTION CONFIDENTIALTY AND NON REPUDIATION.

MC Cumber cube

A framework for evaluating information security.

Desired goals

Data states

Safeguards

Confidentiality, integrity, availability

Transmission , storage, processing

Human factors, policy and practices, Technology.

p

Confidentiality- unauthorized access is prevented

Integrity- Data should not be modified

Availability- Access should not always be available.

Essential terms-

Asset- the item that you are trying to protect

Vulnerability – this could be some sort of weakness in your network or system

Exploit – the way hackers use leverage vulnerabilities.

Threat- this is the action that we are trying to protect ourselves against

Risk- is the risk of assets threats and vulnerabilities.

Cyber threats

Malware -This is normally a software that does malicious actions and tasks to your device.

Spyware- This is a form of malware that hides and will provide you with information so you wont know it is there.

DDos- when the attacker floods the network with requests so it will disrupt the network.

Ransomware- will take the data ransom until the money is paid.

Trojan- this is a backdoor into your system.

Wipers- this is when the intention is to wipe the hard drive.

Theft of money – this is when a cyber criminal gains access to card information.

Unpatched software normally has issues that is why updates are carried out.