Data breach: incident where information is taken without permission

Have i been pwned - checks if data has been stolen

Identity theft - when a person uses someone else’s personal information without their permission

Secure passwords are the easiest way to protect yourself:

* Lowercase letters
* Uppercase letters
* Numbers
* Special characters
* Different for each account

Password managers recommended

Python is used as it is open source and easy to learn, containing many resources specific to cyber security

The field of Cybersecurity started in the 1970s when more and more information started being stored on computer systems and networks

The CIA Triad is the model used to discuss cybersecurity

CIA = confidentiality, integrity, availability

Confidentiality ensures only authorized users have access to data

Integrity ensures data can be trusted and has not been tampered with

Availability ensures networks, systems, and applications are up and running to authorized users whenever they hope to use them

Cia triad helps give direction and focus to how to protect and access data and services

Problems should be looked at through cia triad

Cybersecurity: the practices that people use to protect computer systems and networks from digital threats

People include: governments, nations, companies, communities, organizations and individuals

A cybersecurity incident occurs when one or more of the CIA triad pillars are at risk

Data breaches are incredibly common

They are caused by malicious actors taking advantage of a vulnerability or weakness in a security system

The weaknesses can be technical, physical or social

Technical = weakness in computer network or system that someone can take advantage of

Physical = weakness in the physical world including theft and access to a computer or network

Social engineering = a person who manipulates another person to give up information

Phishing email = an email crafted to look real and convince people to share personal information

NIST framework: identify, protect, detect, respond, recover

Identify = penetration testers: identify any weaknesses in a cybersecurity system and give recommendation to improve it, cryptographers: protect information by encrypting/hiding data in secret codes to keep it private

Recover and Respond = Cyber forensics experts: respond to cyber security incidents and recover data systems and networks and investigate the cause of an incident and work with law enforcement to provide evidence

All = Security engineers and architects: strategize a big picture approach to designing building and implementing a sound cyber security structure and create a plan to identify, protect, detect, respond and recover

Chief information security officer: develop and implement an organization’s information security program to ensure their data remains secure and anticipates, assesses, and actively manages new and emerging threats and responds to data breaches and other security incidents and develops policies and procedures to protect enterprise communications, systems and assets from internal and external threats and works with other departments to align security initiatives with business goals and identifies security objectives and metrics and establishes secure business and communication practices and communicates complex security concepts to both a technical and non-technical audience and has a strong understanding of information technology and security and researches potential cyber threats and future cybersecurity technology