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

Cyberkill chain: reconnaissance = harvesting email addresses, conference information, etc. - weaponization = coupling exploit with backdoor into deliverable payload - delivery = delivering weaponized bundle to the victim via email, web, usb, etc. - exploitation = exploiting a vulnerability to execute code on victim’s system - installation = installing malware on the asset - command and control = command channel for remote manipulation of victim - actions on objectives = with ‘hands on keyboard’ access intruders accomplish their original goals

166 days is the average time it takes an unauthorized person to compromise a system as it is a long process with a lot of steps

**National Health Services data breach in 2017**

* Involves NHS, patients and the public, 16 hospitals, 45000 computers across 74 countries
* No indications that patient data was compromised, however operations at hospitals were severely impacted
* Attack made use of EternalBlue, developed by NSA to break through Windows security and made public as part of a Shadow Brokers dump in April, with its code widely available to anyone who downloaded the dump. Microsoft issued an update to protect against the vulnerability more than a month before the Shadow Brokers made it public, however not all systems were updated, such as those in the 16 hospitals, the attack froze systems and encrypted files.
* Wanna Decryptor ransomware demanded for $300 in bitcoin to access the files, however the attack has already cost over the $300 demanded.
* It has been informally recommended that ransomware targets pay to decrypt their files.
* Analysis: The breach complied with the confidentiality pillar of the CIA triad, as the data remained encrypted and confidential, however it was encrypted by the hackers, and so the data was hidden to the victims, not to the hackers. This meant that the availability pillar was not followed as the data was not available for the victim to use. The integrity of the data was also compromised as the victim can not be certain the data was not tampered with as they do not have access to it.
* I would recommend that a victim do some research online to see if there was a cure to the virus available online, however if it was not available, and if it was the only way for life to continue and less money to be wasted, I would recommend paying for the payload so that life can continue as quickly as possible.