* Cybersecurity is the practice of ensuring confidentiality, integrity and availability of information by protecting networks, devices, people and data from unauthorized access or criminal exploitation.
* **Key Cybersecurity terms and concepts:**
  + Compliance is the process of adhering to internal standards and external regulations and enables organizations to avoid fines and security breaches.
  + Security Frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy.
  + Security Controls are safeguards designed to reduce specific security risks. They used with security frameworks to establish a strong security posture.
  + Security Posture is an organization’s ability to manage its defense of criminal assets and data and react to change.
  + Threat Actor (Malicious Attacker) is any person or group who presents a security risk. This risk can relate to computers, applications, networks, and data.
  + An internal threat can be a current or former employee, an external vendor, or a trusted partner who poses a security risk. At times, an internal threat is accidental
  + Network security is the practice of keeping an organization's network infrastructure secure from unauthorized access.
  + Cloud security is the process of ensuring that assets stored in the cloud are properly configured, or set up correctly, and access to those assets is limited to authorized users.
* Transferable skills are skills from other areas of study or practice that can apply to different careers, such as:
  + Communication
  + Problem-solving
  + Time management
  + Growth mindset
  + Diverse perspectives
* Technical skills typically require knowledge of specific tools, procedures, and policies, such as:
  + Programming languages
  + Security information and event management (SIEM) tools
  + Intrusion detection systems (IDSs)
  + Threat landscape knowledge
  + Incident response