* **Common Attacks and their effectiveness:**
  + **Phishing: the use of digital communications to trick people into revealing sensitive data or deploying malicious software.**
    - Business Email Compromise (BEM): A threat actor sends an email message that seems to be from a known source to make a seemingly legitimate request for information, in order to obtain a financial advantage.
    - Spear phishing: A malicious email attack that targets a specific user or group of users. The email seems to originate from a trusted source.
    - Whaling: A form of spear phishing. Threat actors target company executives to gain access to sensitive data.
    - Vishing: The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source.
    - Smishing: The use of text messages to trick users, in order to obtain sensitive information or to impersonate a known source.
  + **Malware: software designed to harm devices or networks.**
    - Viruses: Malicious code written to interfere with computer operations and cause damage to data, software, and hardware.
    - Worms: Malware that can duplicate and spread itself across systems on its own
    - Ransomware: A malicious attack where threat actors encrypt an organization’s data and demand payment to restore access
    - Spyware: Malware that’s used to gather and sell information without consent. Can be used to access devices and allows threat actors to collect personal data.
  + **Social Engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.**
    - Social Media Phishing: A threat actor collects detailed information about their target from social media sites. Then, they initiate an attack.
    - Watering hole Attack: A threat actor attacks a website frequently visited by a specific group of users.
    - USB baiting: A threat actor strategically leaves a malware USB stick for an employee to find and install, to unknowingly infect a network.
    - Physical social Engineering: A threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location
* **Social Engineering Principles:** 
  + Authority: Threat actors impersonate individuals with power
  + Intimidation: Threat actors use bullying tactics
  + Consensus/Social proof: threat actors use others’ trust to pretend they are legitimate
  + Scarcity: A tactic used to imply that goods or services are in limited supply.
  + Familiarity: Threat actors establish a fake emotional connection with users that can be exploited
  + Trust: Threat actors establish an emotional relationship with users that can be exploited over time
  + Urgency: A threat actor persuades others to respond quickly and without questioning
* **Certified Information Systems Security Professional (CISSP) Security Domains:**
  + Security & Risk Management focuses on defining security goals and objectives, risk mitigation, compliance, business community, and law.
  + Asset Security focuses on securing digital and physical assets. It also related to the storage, maintenance, retention, and destruction of data.
  + Security Architecture & Engineering focuses on optimizing data security by ensuring effective tools, systems, and processes are in place.
  + Communication & Network Security focuses on managing and securing physical networks and wireless communications.
  + Identity & Access Management focuses on keeping data secure, by ensuring users follow established policies to control and manage physical assets
  + Security Assessment and Testing focuses on conducting security control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities.
  + Security Operations focuses on conducting investigations and implementing preventative measures
  + Software Development Security This domain focuses on using secure coding practices, which are a set of recommended guidelines that are used to create secure applications and services.
* **Attack Types:**
  + **Password attack:** 
    - An attempt to access password-secured devices, systems, networks, or data. Some forms of the attack:
    - Fall under the communication and network security domain.
  + **Social engineering attack:** 
    - Manipulation technique that exploits human error to gain private information, access, or valuables.
    - Related to the security and risk management domain.
  + **Physical attack:** 
    - A security incident that affects not only digital but also physical environments where the incident is deployed.
    - Fall under the asset security domain
  + **Adversarial artificial intelligence:** 
    - A technique that manipulates [artificial intelligence and machine learning](https://www.nccoe.nist.gov/ai/adversarial-machine-learning) technology to conduct attacks more efficiently
    - Falls under both the communication and network security and the identity and access management domains.
  + **Supply-chain Attack:**
    - Targets systems, applications, hardware, and/or software to locate a vulnerability where malware can be deployed.
    - Fall under several domains, including but not limited to the security and risk management, security architecture and engineering, and security operations domains.
  + **Cryptographic attack**
    - Affects secure forms of communication between a sender and intended recipient
    - Fall under the communication and network security domain