Week 1:

Common attacks

Phishing: using communication to obtain financial or other types of information

* Spear phishing, whaling, vishing, smishing

Malware: software used to harm devices and networks, programs, etc.

* Virus: malicious software used to interrupt processes of the computer: hardware, applications, software, etc. Spreads to other computers through networks
* Worms: malware that spreads on its own
* Ransomware: attackers encrypt user’s data and ask for a price to decrypt it
* Spyware: malware that steals/takes information by gaining access to devices

Social engineering: exploiting human error to gain personal/financial information, valuables, or access

* Gain information through social media, then launch an attack
* Watering hole: attacking a website used by a group of users
* USB baiting: leaving a usb for employee to use
* Physical: impersonation to gain access
* Very effective, people trust authority
  + Authority, intimidation, consensus/sheep persuasion, scarcity, familiarity, trust (long term tactic), urgency

Week 2:

8 Domains of Security: classifications

* Security and risk management: checks for compliance, defines security goals and objectives, risk mitigation
* Asset security: secures digital and physical assets. Responsible for storing, destroying data
* Security architecture/engineering: optimizes data security by updating tools and processes and systems
* Communication and network security: secures physical networks and wireless communications
* Identity and Access management: Makes sure users are following policies to protect physical assets (office spaces), and logical assets (networks/apps)
* Security assessment and testing: Designing, managing, testing security
* Security operations: Following procedures in order to solve/fix a breach or issue
* Software development security: Understanding, applying, and enforcing software security