1. What is Cyber Problem
   1. Information Security people worry about:
      1. Confidentiality
      2. Availability
      3. Integrity
   2. Motivation to attack:
      1. Money
      2. Steal data which they could use
      3. Use inside info
   3. Attacker profile:
      1. Industrial/Corporate espionage
      2. Other country spy agency (industrial/personal data)
      3. Misc./Activist to cause disruption
   4. Cyber Security Professionals protect:
      1. Money
      2. PII (banking info, photos, phone number, user ID and passwords)
      3. IP
      4. Business Model – [{customer, IP, processes}, {short & long term plans}]
   5. Consequences on a successful cyber-attack:
      1. Profits
      2. Investor Confidence
      3. Customer Confidence
      4. Operations
      5. Legal Liabilities
   6. Finding important info in company:
      1. Acceptable usage policy: what you can do and cannot do with company resources
      2. Information Classification & Handling:
         * Public – info sharable externally
         * Private – info sharable internally
         * Secret – restricted distribution
      3. Report info sec events to proper authorities
      4. 2 most common email accidents: CC/BCC and Email autocomplete
2. Stealing Digital Identity
   1. Phishing for Username and Password:
      1. Attackers want to be you
      2. Attackers want you to download/install malicious software on your device
      3. Attacking methods: phishing

Use CUTE [Cute, Unexpected, Time, Emotional response] method to detect phishing.

What to do 🡪 report it and delete it.

* 1. 3 things Info Sec professionals do to minimize phishing:
     1. Additional authentication method: 2FA / MFA
     2. Limited/Minimum privilege or access to company data is given to associates. Managers give the access to their subordinates.
     3. User access recertification: access to associates is re-confirmed on periodic basis.
  2. Password Hygiene:
     1. Use unique password for every website
     2. Use 2FA/MFA
     3. Combine 3 words for strong password.

1. Getting Inside Your Computer (installing/downloading malicious software):
   1. Via sending email with/without software as attachment
   2. Asking user to visit a page with software
   3. Can cause:
      1. Unauthorized access and info loss
      2. Ransomware via data encryption
   4. If you get tricked, report the same ASAP.
2. Remote Working and Security in Office
   1. Attackers in Physical Space:
      1. Targeted: you/company are targeted, highly sophisticated
      2. Opportunist: those taking advantage of a situation
   2. At home:
      1. Don’t let anyone use your company laptop
      2. Don’t write work passwords near computer
      3. Keep security tokens separate from the computer
   3. At office:
      1. Red tag teams do penetration testing
      2. TO DO: Lock Computer, Clear Desk, Confidential Material, Security Passes.
   4. Travelling:
      1. People peeping at your screen while in public
      2. Stealing actual hardware
      3. To avoid: shut down PC, keep it safe, don’t write password on PC, report issue immediately to info sec team.
3. Vulnerabilities and 5 imp things to remember:
   1. Vulnerability: a software bug which allows attackers to take control of PC. To avoid attackers exploit vulnerabilities, keep all softwares updated with patches.
   2. 5 things to remember:
      1. CUTE checklist.
      2. Report phishing or anything suspicious to Info Sec team.
      3. Don’t install unauthorized software.
      4. Take care of devices physically as well.
      5. Strong password (2FA/MFA/long passwords)