1. Strong Passwords
   1. Should not appear in dictionary
   2. Should not be derivative of a dictionary word
   3. Should be long
2. Social Engineering
   1. Scamming/Tricking people to get information out of them, which regularly people should not be giving up.
   2. Can be info based (via phishing attempts) as well as physical (attackers might want to get inside the org).
3. Cyber Security
   1. Protecting the systems and data they contain
   2. Defense in depth: There is no such thing as a perfect security mechanism. To help individual security measures, use complimentary security mechanisms to achieve the overall desired result.
   3. Common security areas:
      1. Physical Security
      2. Network Security
      3. Email Security
      4. OS Security
      5. Network Endpoint Security
      6. WiFi Security
      7. Others
4. Phishing/Spear Phishing/Whaling
   1. Phishing is an attempt to steal info from computer via deceitful practices.
   2. Spear phishing attacks are targeted attacks
   3. Whaling means going after the top executives.
5. How Physical Security and Info Security complement each other
   1. Physical Security is to safeguard the devices, data servers, etc. via 3G – Gates, Guns and Guards.
   2. Info Security protecting data via passwords, authentication methods, anti-virus, anti-malware, etc.
6. Safer Digital Communications at Work
   1. Not to open executable files like .exe, .bat etc.
   2. .doc / .xls / .ppt may also contain virus
   3. Open files via sandbox if possible
7. Malware at Work
   1. Spread through email, IM and browsers, USB, etc.
   2. Common Malware types:
      1. Viruses
      2. Spyware
      3. Adware
      4. Ransomware
8. Mobile Device Security
   1. Lock device using password/PIN
   2. Use self-destruct mechanism
   3. Set up remote wipe and device tracking capabilities
   4. Cautious of shoulder surfing
9. Security for Cloud Service
   1. Circumventing IT is shadow IT
   2. Shadow IT is not advisable as it has serious potential consequences.
   3. Potential Consequences
      1. Regulatory penalties
      2. No IT support
      3. Data leakage
      4. Business impact
      5. Lawsuits
10. Identifying PII:
    1. Anything that gives info about the person
    2. Use DLP (data loss prevention) softwares/tools
11. Better Security on Road
    1. Use cellular connection if possible
    2. Use VPN
    3. Be cautious of shoulder surfers
    4. Cautious of device theft