Security Concepts

Physical Security Concepts

- Authentication Factors
  - Something you know
    - PIN
      Password
  - Something you have
    - Smart Card
  - Something you are
    - Biometrics
  - Somewhere you are
    - Uses GPS to identify location
  - Something you do
    - The way you type.
- Multifactor Authentication
  - Uses more than one of the above

Layered Approach to Physical security

- Outer Level Access control
- Fences
  - Allows internal separation too (e.g. HVAC equipment servicing)
- Physical Barriers
  - Locked doors
- Multiple Barrier system
  - More than one physical barriers
  - Ideally a minimum of 3
    - Perimeter fence (Alarmed, CCTV, etc.)
    - Security guard on entry (ID badges)
    - The actual building (keyfob entry etc)
      - Combination Door lock (also called cipher lock)
  - Slows down an intruder
- Magnetometers
  - Posh name for a metal detector!
  - Protects from malicious intent

Physical Security

- Biometrics
  - Something you are
    - Fingerprint
    - Iris scanner
    - Gait Analysis
      - https://www.newscientist.com/article/mg21528835-600-cameras-know-you-by-your-walk/
    - DNA Scanner in the future?
- Other Physical Security
  - ID badges
  - Key fobs
  - Hardware token
    - Generate OTP (one Time Passwords)
    - Code changes every 60 seconds
  - Smart Cards and RFID badges

Information Security

- Privacy Filters
  - Prevent screens being read from the side
- Cable locks
  - Uses a Universal Security Slot (USS)
  - Kensington Security Lock

- Secure physical documents
- Shred Confidential documents one not needed

Logical Security

- Antivirus and Anti Malware Software
  - Viruses have common characteristics
  - Can test using EICAR
    - https://www.eicar.org/?page_id=3950
      - Open Notepad.
      - Copy the following string and paste it into Notepad:
      - X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
      - Save the file and cross your fingers that your scanner doesn't detect it on close.
- Firewalls
  - First line of defence
  - Often built into the router
  - Separate box in a server rack in larger companies

Logical Security

- Firewalls
  - https://www.youtube.com/watch?v=kDEX1HXybrU

  - First line of defence
  - Often built into the router
  - Separate box in a server rack in larger companies
  - ACL – Access Control List
  - Packet Filter

  - Proxy Server
    - A form of firewall
    - https://www.youtube.com/watch?v=5cPIukqXe5w

Logical Security

- MAC Address Filtering
  - Normally for switches
  - Only allows connections based on the devices MAC address
- Port Security
  - Services run on PCs using specified port
    - E.g. RDP 3389
  - Close unused ports
- Email filter
  - Remove Spam
  - Remove payloads before forwarding

Logical Security

- Data Loss Prevention (DLP)
  - Ensures that end users don’t send sensitive or critical information
  - Outbound mail filter
  - MS Exchange allows admins to create DLP policies
- Virtual Private Networks
  - Secure way to connect two sites
  - Tunnels data
- Passwords
  - https://howsecureismypassword.net

Network Policies

- Acceptable Use Policy (AUP)
  - Includes smart phone usage
  - USB devices
- Trusted / Untrusted Software Sources
  - Licensing is important
- Mobile Device Management (MDM)
- Bring Your Own Device (BYOD)
- Principle of Least Privilege (PLP)
  - Only assign the permissions that the individual needs
  - Admin users should have two accounts