SECURITY FUNDAMENTALS
• IT Security
• Physical Security
  • Locks
  • Tailgating
  • Documents
  • Biometrics
  • Badges
  • Key FOB/RFID Badge
  • RSA Token
  • Privacy Filter
• Digital Security
• User Education
• Principal of Least Privilege
• Security Threats
  • Social Engineering
  • Malware
  • Best Security Practices
  • Data Destruction/Disposal
  • Physical Destruction
• Secure a SOHO Wifi Network
• The practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc...).
• Bolt lock & key
• Combination/cypher, keypad, dial system
• ID access card with electronic chip or sensor
• Biometric – fingerprint, retinal
• Hardware locks – laptops, hard drive, portable devices
• Allowing an individual(s) access to a secure area by entering just behind a person who gained authorized access
• Risk reduced by strong policies (termination) for individuals who violate policy
Physical Security - Documents

• Store confidential and secure documents in a secured area
• Destroy by
  • Shredding
  • Burning
• Prevent dumpster divers
• Use an individual's unique characteristics for identification purposes
• Fingerprint scanner
• Retinal scanner
Physical Security - Badges

- Includes picture and name
- Can include
  - Other demographics (DOB, height, weight, department, etc.)
  - Expiration date
  - Bar codes
  - Seals, icons, layered images
  - Embedded micro chips
• Electronic device that permits access to a locked area when in proximity to a detector.
• RFID – Radio Frequency ID
  • Electronic device that responds via radio waves, when queried by a RFID reader/antenna
• Electronic device that enables two factor authentication
• Two factor authentication - two or more of:
  • Something only the user knows (i.e. password)
  • Something only the user has (i.e. RSA Token code)
  • Something only the user is (biometrics)
• Display filter which only allows viewing of display information when immediately in front of the display
- Anti-virus software
- Anti-spyware software
- Firewall
- User authentication
- Directory/folder permissions
• Informing end users of security principles and practices
  • Sharing of password and log-in sessions
  • Password complexity
  • Defending against social engineering attempts
  • Restricting user permissions
  • Changing default user names
  • Downloading malware
• Give the minimal access necessary to complete a specific task
• Similar in concept to a “need to know”
Security Threats—Social Engineering

- Uses deception or trickery to convince unsuspecting users to provide confidential information or access
- Spoofing
- Impersonation
- Hoax
- Phishing/Vishing
- Whaling
- Spam/spim
• Unwanted software with the potential to do damage to a system, enabling further attacks, transmit data, corrupt or erase files
  • Virus – spread by opening executable file
  • Worm – spreads on own through network
  • Trojan Horse – appears as legitimate software
  • Logic Bomb – event triggered
  • Adware – automatically displays ads
  • Rootkit – gains admin/root access
  • Spam – email based fraudulent ads
- Requiring passwords
- Setting strong passwords (random > 8 characters)
- Restrict user permissions (avoid admin accounts)
- Change default user name (avoid “administrator” user name)
- Disable guest account
- Enable screensaver password
- Disable autorun
• Low level format – writing sector markings to disk like it is done during manufacturing process
• Standard format – OS level function that builds file allocation table structure and checks and marks error prone sectors of the disk
• Drive wipe – process of removing traces of data from a storage device
• Overwrite – write random data over old data multiple times
Physical Destruction

- Shredder – paper and optical media
- Drill – physical destruction of hard disks
- Electromagnetic – magnets create field to scramble magnetic information on magnetic media
- Degaussing Tool – removes the magnetic properties of magnetic media
Secure a SOHO Wifi Network

- Change default SSID login and passwords
- Change default SSID
- Setting WPA2 AES/CCMP encryption
- Disable SSID broadcast
- Enable MAC filtering
- Access point placement
- Use directional antennas
- Adjust radio power levels
- Turn off DHCP/assign static IP
- Physical security
• Change default usernames and passwords
• Enable MAC filtering
• Turn off DHCP/assign static IP
• Disable external ports
• Physical security
THANK YOU