A+ Certification 902 Study Guide

Section 1: Windows Operating Systems

Overview of windows Vista

Released 1-30-2007, 5 years after XP
Features-upgraded GUI, has Aero and integrated search functions
-Emphasis on security, UAC added
Home Use - Home basic: No AD or aero
Home Premium: DVD burning, more games
Ultimate: bitlocker included, language packs, video background (dreamscene)
Work Use - Vista Business: AD, encrypting files, RDP, supports 2 CPUs
Enterprise - bitlocker, multilingual

Overview of Windows 7

Released 10-22-2009
Same HW and SW as vista, increased performance
New Features: libraries, homegroup, pinned taskbar

Starter- made for netbooks, no dvd drive, no aero, no WMC, only 32 bit, 2gb RAM max
Home Premium - aero, dvd, 64 bit, 16gb ram max
Ultimate - domain support, RDP, encryption, bitlocker, 64 bit 192gb ram max, same features as enterprise
Professional - same features as home premium
Domain support, RDP, EFS, no bitlocker 64bit 192gb ram
Enterprise- sold only in volume license

Overview of Windows 8

New UI, new start menu. 8.1 was an update, but same OS

Core- very basic, 32&64 bit, account integration, windows defender

Pro- similar to 7 pro/ultimate, bitlocker, EFS(full disk and file)

Domain support and group policy

Enterprise - large volume license, applocker, windows to go, direct access

Physical Access Extension (PAE)

PAE- allows 32 bit OS to use more than 4gb of ram

Nx processor bit - protects against malicious software

Streaming SIMB Extension 2 (SSE2) - instructions used by 3rd party SW And drivers

Windows Features

-64 bit can run 64 and 32 bit programs

-Drivers must match OS bit

-64 bit installs 32 bit apps in one folder (program files/x86) and 64 bit in another(program files)

Windows Aero- Only in Vista and 7, enhanced UI, allows switching between apps

UAC- user account control, limits software access, asks for admin password

Bitlocker- protects entire drive, including the OS, stays on HDD in case it's stolen

Volume shadow copy - backup entire volumes while OS is running, even open file

System Restore- go back in time on OS to fix issues, not good for virus/malware

accessories/system tools/system restore

Sidebar/gadgets- vista had sidebar, 7 has gadgets that can go anywhere

Gadgets were discontinued for vulnerabilities

Windows 8 started using Apps instead of gadgets

Ready Boost- cache to RAM instead of HDD

Can be stored on flash memory

Plug in compatibility

Compatibility Mode - Run app as an old OS, OS pretends it's an older version

Windows XP mode (XPM) - VM on windows 7, not supported on any OSs anymore

Windows Easy Transfer - migrates files and settings, xp/vista/7/8

8.1- only files, no settings

Admin tools- in the CP- computer management, services, memory tools

Windows Defender- anti malware in vista/7, antivirus also in 8/8.1
Windows Firewall - allows or disallow certain traffic, prevents malware
Security Center - vista (called action center in 7/8/8.1) - security overview of AV, Updates, etc.
Event Viewer - shows everything going on, info, warnings, critical events
Control Panel - category view and classing view (everything in alphabetical order)

Windows 8/8.1 Features:

- **Pinning : Put apps on task bar: right click then pin to taskbar**
- **Onedrive: cloud service in OS, stores files and settings**
- **Windows Store: central point for modern UI apps**
- **Multimonitor taskbar: multiple monitors with different taskbars**
- **Charms: shortcuts available at anytime**
- **Powershell: command line for sysadmins**
- **Centralized account login: syncs account with email**

Windows File Structures and Paths

Storage Device Naming- letter followed by a colon (C:)

Files & Folders - just like physical folders
Folders can contain other folders
Folder names separated by backslash
C:\users\admin\documents\file.text

Windows Folders - \users: user doucments, important,make sure to backup
\program files: all applications
\windows : OS files

Windows Upgrade Paths

Upgrade- keeps files in place, much quicker, no install needed
Options: in place upgrading and clean install
Cannot upgrade 32>64 or 64>32, must do clean install
XP cannot install to 7, clean install

Install - start over completely fresh

Windows anytime upgrade- upgrade within the current OS
Very easy, not available in Vista

Preparing For Windows Install

Make sure updates are current, make room on HDD, backup important data

Installation sources- cd/dvd/usb/ pxe network boot/ netboot (MAC)
Type of installs- In place upgrade- saves apps and settings
-clean install
-image- deploy a clone on every computer
-unattended- answers questions asked during install
-repair install- fixes OS problems, no file changes

Dual Boot - 2 OS's on one computer
Recovery Partition- hidden partition with install files
Refresh/Restore - Windows 8 feature, built into OS, no install media needed
Disk Partitions - separates physical drive into logical pieces
Volumes- formatted partitions with file systems (NTFS, fat 32)
MBR partition - Masterboot Record
-Primary - contains OS bootable file
-marked as active when booted from
-max of 4 primaries per disk
-Extended - extends max number of partitions
-one extended per disk
-partitions inside extended not bootable
GPT partition- GUID partition table- latest, requires UEFI
-up to 128 primary partitions
First step when preparing disk- partition needs to be compatible with
Windows (MBR or GUID)
File Systems- FAT: File allocation table, one of the first PC file systems
FAT32: Larger (2 TB) volume sizes, max file size of 4gb
exFAT: microsoft flash drive system, files can be >4gb
NTFS: NT file system, started in windows NT, improvements
Included quotas, file compression, encryption, large
File support, recoverability
CDFS- CD file system, all OS's can read the CD
Ext3 - 3rd extended file system, use in linux
Ext4 - update from Ext3, used in Linux and Android
NFS- network file system, access drives as if they were local
Storage Types - layered on top of partition and file system

Basic Disk Storage- in DOS and windows, partitions cannot
Span across separate physical disks
Dynamic Disk Storage - span across multiple disks to make
One volume (RAID)

Quick Format - new file table, overwrites existing file table

Full Format - overwrites and writes zeros to all data
Checks disks for bad sectors

The Windows Command Line

OS command line tools - Not all users can run all commands, need permissions
Type “help” + command or [command]/? to get info
Close cmd with “exit”

Diskpart- change existing volumes

Format - erases everything in a partition
Example - “format C:”

CHKDSK - CHKDSK /f - fix errors found on disk
CHKDSK /r - finds bad sectors and recovers readable info
If volume is locked, run during startup

DIR - lists files and directories

DEL - removes file   example - del [filename]

MD - make directory

CD- change directory

RD- remove directory

COPY /V - verifies files are written correctly

COPY /y - suppresses overwrite prompt, example - copy [filename][drive]/v

XCOPY - copies files and entire directory trees
Example - xcopy /s Documents E: (E being destination)

ROBOCOPY - a better Xcopy, can resume copy if errors occur

TASKLIST - manage tasks from cmd, show current processes

TASKKILL - terminate process

SFC- scan integrity of all protected file systems
/scannow - repairs files

SHUTDOWN - shut down pc
/s or /r = shutdown or restart

EXPAND - expands folders

Managing Group Policy- manage PCs in an AD domain, GP updated at login

GPUPDATE - force a GP update

GPRESULT - view policy settings for a computer or user

Windows Recovery Environment Command Prompt

Preboot Command Prompt-

Can be very dangerous, make it a last resort

Can fix issues before the OS starts

Able to modify system files, enable/disable services

Able to create/modify partitions

Start by booting from install media (choose troubleshoot on windows 8)

Master Boot Record (MBR) - not located in a partition

-knows all other partitions, master list

-knows location of active bootable partition

Problems with MBR - error loading OS, missing OS, invalid partition table

Fixing MBR - cmd bootrec /fixmbr,fixes MBR on physical drive

Partition Boot Record - also called volume boot record

Problems- “invalid partition table”

Fix - bootrec/fixboot

Rebuilding Boot Config Data - Bootrec/rebuildbcd

Creates a new boot configuration data store

Windows Operating System Features

Windows Administrative Tools

Computer Management: pre built microsoft management console

Shows events, users, accounts, storage management

Device Drivers - OS does not know how to talk to hardware

Drivers are found in device manager

Local users and groups - admin is the super user, has all permissions

Regular users and guest accounts

Users can be put into groupd

Local Security Policy- large companies manage this through AD

Standalone computers need local policies
(password length, complexity, expire time length)

Performance Monitor- gathers long term statistics, creates reports
-OS metrics such as disk usage, memory, cpu usage

Services - running in background, no user interaction (AV,file indexing,etc)
Useful when troubleshooting startup
Many services start up automatically
Cmd control - net start, net stop
Task Scheduler- schedule and app or batch file
Includes pre defined schedules
Print Management - manage and configure printers and drivers
Memory Diagnostics - check memory modules for read/write errors

Windows Firewall & Advanced Security

Stateful firewalls - remembers the state of traffic going through it

Windows Firewalls - integrated into the OS
Has fundamental firewall rules
Based on apps, no detailed control
No scope or IP range, all traffic applies
No connection security or rules
Advanced Security - inbound/ outbound rules
Connection security rules
Set rules by program/ port, predefined, custom

Using Windows System Configuration

Msconfig - manage boot process, startup apps, services
General tab- normal startup - loads all normal programs
Diagnostic startup - loads basic services,
Step up from safe mode
Selective startup - you choose what starts

Boot Tab - set different configurations

Advanced options - set number of CPUs, max memory
Boot options - safe boot, remove GUI, create boot log

Services Tab- enable/ disable services, easier to manage, check/uncheck
Startup tab - manage which programs start automatically at log in
Moved to task manager in 8/8.1
Tools Tab- easy to access popular admin tools

Using Task Manager

Task manager contains real time statistics (CPU usage, memory, disk)

Windows 7 - Applications tab - apps running on desktop
Processes-interactive & system tray apps,other user processes
Performance- shows historical usage
Networking - see performance of each network adapter
Users- see what they are doing, send messages, log off

Windows 8/8.1 - apps, processes, and services are all on one tab
Users- shows separate processes, performance stats

Using Windows Disk Management

Used to manage disk operations
Disk status - Healthy, healthy & at risk, initializing, failed
Failed Redundancy - failed RAID 1 or 5
ReSyncing- RAID 1 is syncing data between drives
Regenerating- RAID 5 is recreating itself based on parity bit
Mounting Drives- extend the available storage space, can be a folder
Makes it so you do not need another drive letter
Can set up a RAID 1 mirrored volume
Storage Spaces - storage for data centers or clouds
Multiple tiers, administrator controlled

Windows Migration Tools

Migrate- moving all files and settings

Upgrade advisor (windows 7) - checks s/w and h/w is compatibility with OS
Upgrade Assistant (windows 8)- check s/w and h/w compatibility with OS

Migration Methods - side by side- 2 pcs, transfer from one to the other

- **Wipe & load - export data, wipe pc, install OS, move data To new OS**
- **Windows 8/8.1 - use one cloud to save files and settings**
- **Windows easy transfer - transfers all user info,docs,app**
  - **Settings, videos pics, not the actual apps**
  - **Supports side by side & wipe and load**

User State Migration Tool- can be used on any upgrade

- **Included with automatic install kit (AIK)**
- **Used at command line, in large enterprises**
- **Can migrate a large quantity of machines**
- **2 step process:**
  - **1: scan state- compiles and stores data**
  - **2: load state - loads on destination PC**

Windows System Utilities

Run Line- start an app as a command

CMD- very powerful, can do anything with right permissions

Regedit- windows registry editor, huge master database

- **Drives, services, security account manager, backup**

Services.msc - shows background apps running

- **Useful for troubleshooting startup**
- **Services can reveal dependencies on others**

MMC- microsoft management console

- **Build your own management framework**
- **Decide what utilities or “snap ins” you want**

MSTSC- Microsoft Terminal Services Client

- **Remote Desktop connection utility**
- **Common for “headless” machines**

Notepad - view & edit text files

Explorer- file management, copy, view, or launch files

MSinfo32- windows system info

DXDIAG- direct x diagnostic tool, manage direct x installation

DEFRAG - disk defragmentation

- **Moves file fragments so they are contiguous**

- Not needed with SSD’s
- System Restore - go back in time to an earlier working configuration
  - Does not resolve virus or malware issues
- Windows update - keeps OS up to date, can be automatic
  - Can download and not install

Windows Control Panel

- Internet Options- make changes to IE
  - General - homepage, history settings
  - Security-
  - Privacy- cookies, popup blocker, anonymous browsing
  - Connections- VPN or proxy settings
  - Programs- default browser, plug ins
  - Advanced- detailed settings and reset
- Display- resolution, color, depth, refresh rate
- User Accounts- all local user accounts, change account settings
- Folder Options- manage windows explorer
  - General- expand folders
  - View- hide files, hide extensions
  - Search- search options, searching non-indexed
- System- PC info, OS version and edition
  - performance - virtual memory
  - Remote settings- remote assistance and RDP
  - System Protection- system restore
- Windows Firewall- integrated into the OS, protects from attacks
- Power Options- customize power usage
  - Sleep- saves power, quick startup
    - Switches to hibernate if power is low
    - Stores open apps in memory
  - Hibernate- open apps and docs are saved to disk
    - Common on laptops
    - No power is used during hibernation
- Programs and features- install/uninstall apps
  - Can also enable/disable on windows
- Homegroup(7&8) - easily share files and devices
  - Network settings must be set to home network
  - Single password for everyone

Devices & Printers- see everything on network
Quicker and easier than device manager
Sounds - configure output levels
Troubleshooting - automates most common issues
May require elevated access
Network & Sharing Center - all network adapters (wired & wireless)
Device Manager- list devices and drivers, add/remove hardware

Windows Networking

Workgroups - logical group of network devices, non centralized
Every device is standalone and everyone is a peer
All on a single subnet
Homegroups- share files with everyone else on the homegroup
Works only on a private network
Network settings must be set to home or private
Domain- business networks, centralized authentication
Manage all devices from one central point
Supports thousands of devices on multiple networks

No homegroups on Vista, 7 has home network, 8 has private network

Windows Network Technologies

Network locations in Windows 7
Home - everything is trusted
Work - Can see other computer but cannot join homegroup
Public- You are invisible
Network Locations in Windows 8
Private - similar to home, everything is trusted
Public- No sharing or connectivity

Remote Access - Remote Assistance - one time remote access
Single use password
Can be used through a firewall
Remote Desktop Connection - on going access, may have to open ports

Proxy Settings - can change the traffic flow, is an internet go between
Defines an address and exceptions
Network Shares - A folder accessible by anyone on the network
Assign a drive letter to the network share
Shares ending in “$” are hidden
Printer Shares - similar to sharing folder, add a printer in windows explorer

Establishing Windows Network Connections

Network and sharing center found in the Control Panel

VPN Concentrator- decrypts the encrypted data to the destination
Windows has a built in VPN
Multifactor Authentication - something you know, have, or are
Dial Up Connections- uses a modem connection, standard phone line
Wifi - 802.11 is the wifi standard
SSID = Service Set Identification which is the network name
WWAN - Wireless Wide Area Network - connects to cellular data

Configuring Windows Firewall

Windows firewall should always be on, only turn off for troubleshooting

Settings - public and private
Block all incoming connections- ignores exception list
Modify Notification - notifies if app is blocked
Traffic can be allowed/blocked by program name or port number
Windows firewall has pre defined exception

Windows IP Address Configuration

Windows gets IP address automatically through DHCP

DHCP- Dynamic Host configuration Protocol
Used to automatically assign private IP addresses
APIPA - Automatic Private IP addressing (169.254.1.0 - 169.254.254.255)
Only used if DHCP is unavailable

Does not have any internet connectivity, non routing

Static Address- addressed you assign manually

IP Address- Unique identifier

Subnet Mask - Identifies what the subnet is

Gateway- The route from the subnet to the rest of the internet

DNS - Translates names to IP addresses

Loopback Address - 127.0.0.1

Configuring Network Adapter Properties

Properties- Link speed and Duplex need to match (autonegotiation)

Wake on LAN- computer will sleep until needed

Good for late night software updates

QOS - Quality of service, used to prioritise network traffic

Apps, VOIP, video, all devices must support QOS

DSCP Classification - Differentiated Service Code Points Classification

Allows windows to change packets

Managed through policy or group policy

Network adapters can be enabled/disabled in BIOS

Windows Preventative Maintenance Best Practice

Scheduled Backups - can be hourly, daily, weekly

Must specify what you want backed up

onsite and offsite

SMART- used to avoid hardware failures and look for warning signs

Logical and physical disk checks - in windows used CHKDSK

Scheduled Defrag - setup a weekly schedule, not needed for SSDs

Windows Updates - security patches, drivers, features

Patch Management - allows you to manage updates, many patches

Drivers/ Firmware - some updated more than others, some automatic

AV- keep it up to date

Windows Backup - backup/restore individual files

Can also do images and recovery discs

Cloud took over in windows 8

Section 2: Other OS's & Technologies

Best Practices for MAC OS

Scheduled Backups - "Time Machine" Included in MAC
- Hourly backups, daily, or weekly
- Starts deleting oldest data when disk is full

Scheduled Disk Maintenance- Disk Utility- rarely needed
- Other utilities can run during
- Used to verify disk, run as needed

System Updates- updates can be found in the app store
- Can be automatic or manual
- Both OS and app updates

Driver/Firmware Updates- done in background, almost invisible
- System information is detailed hardware list

Antivirus/Antimalware- not included in MAC os, 3rd party app
- MAC is not as vulnerable as windows

Best Practices For Linux

Scheduled Backups - can use a CLI or GUI
- TAR- tape archive, easy to script schedule
- RSYNC- sync files between storage devices,
  - Instant or scheduled

Disk Maintenance- file systems require little maintenance
- Check file system
- Clean up disk space from log files

System Updates - CLI tools, "apt-get" and "yum"
- GUI updates also
- Used of patch management, can be scheduled

Driver/Software updates- many drivers are in the kernel
- Updated whenever the kernel updates
- Additional software updates can be done yourself

Antivirus/Antimalware - not as vulnerable as windows
- Clam AV - open source, same update practices

MAC OS TOOLS

Time Machine - used for backups, auto and easy to use

- **MAC takes local snapshots if time machine is unavailable**

Image Recovery - build a disk image in disk utility

- **Creates an apple disk image file (.dmg)**
- **Mount on any MAC os system**
- **Appears as a normal system file**
- **Restore in disk utility**

Disk Utility - manage disks and images

- **Verify and fix file systems**
- **Erase disks, modify partitions**
- **Manage RAID, restore image to volumes**
- **Create, convert, and manage images**

Terminal - CLI, used to run scripts

Screen Sharing - intgerated into the OS

- **Can be used with virtual networking computing**
- **Available devices in Finder or access them by IP**

Force Quit - stop an app from executing

- **Command + option + escape or hold option key + right click**

Linux Tools

Backups - May be built into OS

- **GUI- backup/restore, scheduling**
- **CLI - TAR & RSYNC**

Image Recovery - not as many options as windows

- **“DD”- Date Description- built into Linux and very powerful**
  - **Creates an image of the entire drive**
  - **3rd party- GNU parted, clonezilla**

Disk Maintenance - Linux file systems do not require much maintenance

- **Clean up logs, logs are stored in /var/log**
- **File System check- sudo touch /forcefsck**

Terminal - CLI for OS

Screen Sharing - Can have screen access from remote device

Closing Programs - use terminal, “sudo” gives admin privileges

- **“Killall” can be used to stop program**

    Example: sudo killall firefox

    xKill- graphical

    kill<processID> - kill individual program

MAC OS Features

Mission Control - Quickly view everything that is running

Spaces- multiple desktops running

Keychain- password management: passwords, notes, certs, etc.

Integrated into the OS

Encrypts password with “3DES”

Spotlight - finds files, images, apps, or searches the web

Similar to windows search

iCloud- integrates all MAC OS’s and files

Shares across system (calender, photos, contacts)

Backs up your iOS device, integrated into OS

Gestures - customize what happens on trackpad

Swipe, pinch, click one finger, two fingers, three

Finder - OS file manager, similar to windows explorer

Remote Disk - use an optical drive from another computer

Designed for copying files

Made for data cds, not music or video

Setup in system preferences

Can set up to share with windows

Dock- fast and easy access to apps

Dot underneath icon indicates the app is running

Folders can be added to Dock

Boot Camp - dual boot into windows or MAC

Not the same as virtualization

Managed in boot camp, install partitions, drivers, etc.

Basic Linux Commands

Man- manual, help

“Man grep”

SU/SUDO - gives elevated rights, stands for superuser do

SU- become super user instead of typing SUDO everytime

“Exit” to go back to regular user

SUDO - used to run a single command as a super user

LS- list directory contents, similar to “dir” in windows

Lists files and directories, may suppost color coding

blue= directory red = archived file

Ls-l= long output

Grep- find text in a file, search through many files at once

Grep Text File

“Grep banana document.log

Cd- change directory, use forward slashes instead of backslashes in windows

cd/var/log

Shutdown - similar to windows shutdown command

Run as SU, time is in minutes

“Sudo shutdown 2”

Restart - “sudo shutdown -r 2”

Ctrl-c to cancel

PWD- print working directory, displays current working directory path

Passwd- change a user account password

“Passwd username”

Can change other use password if SU

MV - move a file or rename a file

Move - Mv source destination

Rename - “Mv first.txt second.txt”

CP - copy a file

Cp source destination

Rm- removes a file or directory

“Rm file.txt”

Mkdir- make a directory or create a folder for file storage

“Mkdir notes”

Chmod - changes mode of a file system object

Chown- change a file owner or group, modify file settings

Sudo chown owner:group file

“Sudo chown user banana.txt

Iwconfig- view or change wireless network configuration

Change the essid, frequencies, channel, mode, rate

Ifconfig- view or configure networking info

Ip,subnet, similar to ipconfig on windows

PS- view all current processes and process IDS (PID)

Apt-get - advanced packaging tool, install update or remove

“Sudo apt-get install wireshark”

Vi- visual mode editor, full screen editing with copy,paste, and more

Vi filename

“Vi text.txt”

Dd- convert and copy files, backup and restore an entire partition

Virtualization

Ability to run multiple OS’s on a single desktop

Host based Virtualization- virtual box, running on one main OS

Enterprise Level- standalone machine that hosts the VMs

Hypervisor - software that is able to create the VMs

Manages the physical hardware

Emmulation - trying to run the app as if it is the required OS

Virtualization is the actual OS

Resource Requirements - CPU must support virtualization

Intel :Virtualization Technology (VT)

AMD: AMD-V

Memory must go above host requirements

Network Requirements - VMs share IP with physical host

Uses NAT to convert to the host IP

Uses a private IP inside the VM

Bridged Network - VM is its own device on network

Private address- Can only communicate with other VMs

Cloud Computing

4 Characteristics-

Rapid Elasticity - scale up and down as needed

Seamless to everyone

On Demand Self Service- adding resources in easy, virtualized
Resource Pooling - all computer power located in one place
One large instead of several small resources
Measured Service- cost and use are closely tracked

Software as a service (SaaS) - on demand software, no local installation
Program is managed by someone else (email,payroll)
Your data is stored elsewhere (gmail)
Infrastructure as a service (Iaas) -using someone elses hardware
You are responsible for management and security
Your data is elsewhere but you control it
Example - web hosting providers
Platform as a service (PaaS) - no server, no software, so HVAC
Someone else handles the platform, you handle the product
You do not have direct control of data, people, infrastructure
Example- salesforce.com

Cloud Deployment Models: Private- your own virtualized local data center
Public- available to everyone on the internet
Hybrid- mix of public and private
Community- several organizations sharing resources

Network Services

Web server- responds to browser requests, uses standard protocols
HTML, HTML5
Web pages are stored on a server
Web pages are downloaded to the browser
Pages can be static or built dynamically
File Server- stores all types of files
Standard system of file management
Windows uses SMB apple used AFP
Print Server - connect a printer to a network
Uses standard printing protocols (SMB, LDP)
DHCP server - assigns IPs automatically
Enterprise DHCP servers are redundant

- DNS Server - converts names in IP addresses
    - Distributed- load balanced on many servers
    - Managed by ISP or enterprise IP department
- Proxy Server - intermediate server, client makes requests to proxy
    - Proxy performs the actual request from there
    - Proxy provides result back to the client
    - Features- caching, access control, content/url filtering
- Mail Server- incoming/outgoing mail, managed by ISP or IT dept.
- Authentication Server - login authentication to resources
    - Centralized management
    - Always on enterprise networks, not usually home
    - Usually set of redundant servers so it’s always available
- IDS/IPS- Intrusion detection system\ Intrusion Prevention System
    - Intrusions - exploits in OS, apps, etc
        - Buffer overflows, cross-site scripting, and others
    - Detection - alarm or an alert for intrusion, does not stop
    - Prevention- stops it before it gets into the network
- All-in-one security appliance - can be called next generation firewall
    - Unified Threat Management (UTM)
    - Web security gateway
    - Examples - Firewall IDP/IPS, router, switch, spam filter
- Legacy Systems - really old systems
    - Be aware if important service is running on legacy comp
- Embedded Systems - Purpose built device, usually no access to OS
    - Example- alarm system

Mobile Operating Systems

- iOS- based off of Unix, closed source
    - Apps developed with software developer kits (SDK)
    - Apps must be approved by apple
- Google Android- open source, based off of Linux
    - Apps are on google play or 3rd party sites
- Windows Mobile -Microsoft OS,closed source,based on Windows NT kernel

- Device Displays & Technologies-
    - Calibration- older resistive touchscreens require calibration
        - Periodically, modern touchscreens do not

Accelerometer - motion sensor and detects orientation
Gyroscope - detects pitch, roll, and yaw
GPS - created by DOD, over 30 satellites in orbit
Precise navigation requires at least 4 satellites
Determines location based on timing differences
Location services use GPS, WIFI, and cell towers
WIFI Calling - uses VOIP technologies,
Virtual Assistant- talk to phone to get assistance (siri)
Production and Development Models- IOS developed on MAC OSx, Linux
Android- apps developed on windows, MAC osx, Linux
Apps distributed in Android app package (APK) format
Windows- apps developed in windows 8.1 visual studio
Wireless Emergency Alert- similar to SMS, no cost
Works on all mobile OS's
Mobile Device Payments - can be used with SMS
Charge to mobile account (apps)
Mobile web payments from browser
NFC

Mobile Device Connectivity

Baseband Radio Processor- communicates to the mobile provider
Has it's own firmware and memory
Firmware updated over the air
PRL updates (preferred roaming list)
Used on CDMA networks (verizon & sprint)
Allows phone to be connected to correct tower
PRI updates (product release instructions)
Radio settings (ID numbers) network & country codes
IMEI - International Mobile Station Equipment Identity
Identifies the physical mobile device
Every phone has a different IMEI
Can be used to allow/disallow access
IMSI - International Mobile Subscriber Identity
Identifies the user of a mobile network
In the SIM card
Wireless networks - Enable/disable data,wifi,bluetooth independently

iOS- settings/cellular

Android - settings / wireless & network settings

Windows - settings / wifi

Bluetooth - is a Personal Area Network (PAN)

Range of 10 meters

Tethering - phone is a wifi hotspot, uses carriers internet

Airplane Mode - turns off all radios

VPN - turn phone into a VPN endpoint, integrated into OS

May support mulitfactor authentication

Configuring Email on Mobile Devices

Retrieving Email- POP3 & IMAP

Sending Email - SMTP

POP3- downloads email to local client

May delete email from mail server (TCP/110)

IMAP- Access mail on a central mail server

Mail is stored on the server (TCP/143)

Network ports - defined by the mail provider

May not be 110 or 143

SSL settings - POP3S - TCP/995 IMAPS- TCP/993

SMTP - sends email from device to server

Must send mail from a local or trusted server

Microsoft exchange - enterprise email, contacts, calendar, and reminders

Able to sync with a mobile device

S/MIME - secure/multipurpose Internet mail extensions

Encrypts and digitally signs emails

GMAIL- IMAP and POP3

Yahoo - IMAP and POP3

Outlook - IMAP and POP3

iCloudmail- IMAP only

Mobile Device Synchronization

Syncing is used for many types of data (contacts, programs, emails, pics)

Syncing to desktop - needs minimal memory but lots of storage space
iOS- Itunes syncs everything from phone so it can transfer to another
Android - syncs online with google or can use 3rd party to sync locally
Windows phone - windows app with sync media but not email or contacts

Cloud syncing - all wirelessly, may be integrated with email
iOS- syncs all data to cloud, good for backup and recovery
Android- syncs to google
Windows- syncs to your microsoft account
Synchronization Connections- iOS- usb to 30 pic (older) or 8 pin lightning cable
802.11 wireless, or mobile network
Android - usb micro or wireless

Section 3: Security

Threats- Malware- Malicious software, can gather info, such as keystrokes
Can be a bot and run in a group, called a Botnet
Used for extortion-money
Viruses and worms can be malware
Spyware- Malware that watches you, tricks you into installing
Captures web browsing habits, can be a keylogger
Viruses- malware that can reproduce itself through network file systems
May or may not cause issues, can be invisible or annoying
AV must be updated regularly, there are new viruses everyday
Worms- malware that self replicates, can take over many PC's quickly
Worms can also be good, can fix issues by spreading
Trojan Horse- software that pretends to be good, but is actually a virus
Better trojans can avoid and disable your AV
Rootkits- can be invisible to the OS, won't see in task manager or services
Modifies your core system files, part of the kernel
Can be named something similar to a common windows file
Ransomware- data is held hostage, OS will work but data is encrypted
Must pay the bad guys for encryption key, untraceable
Phishing - social engineering, fake web pages to get your login, password
Always check the URL when logging in
Spear Phishing- Targeted and sophisticated phishing
Spoofing- pretending to be someone you are not

Mac spoofing- changing mac to look like one on network

IP spoofing- changing IP to look like one on network

Spoofing is used in many DDOS attacks

Social Engineering- suspicious phone calls, unattended persons

Tricking you into giving info

Shoulder Surfing - watching what someone is doing, easy to do in public

Can be done from afar with binoculars

Zero Day Attacks- many vulnerabilities in apps not found yet

Bad guys try to find before good guys patch them

DDOS- launch an army of computers to bring down a service

Uses all the bandwidth or resources, traffic spike

Bad guys use botnets-thousands or millions of pcs at your command

Attackers are zombies, most have no idea their computer is a bot

Brute Force - keep trying to log in until password is guessed

Online- very slow, most accounts will lock out after so many

Offline- obtain the list of users and hashes, calculate

Dictionary Attack - only using well known words to brute force

Non-Compliant Systems - constant challenge, always changes and updates

Standard Operating Environment (SOE) - set of tested and approved hardware/software systems

OS & App updates- must have patches to be in compliance, OS & AV

Tailgating- use someone else to gain access to a building, follow them in

Man-in-the-middle attack- traffic goes to man in middle, he forwards to Destination

You never know the traffic was redirected

Example - ARP poisoning

Avoid by encrypting your data

Security Prevention Methods

Door Access Control- conventional key and lock

Deadbolt- physical bolt

Electronic- keyless, RFID badge

Token based- magnetic swipe card, key fob

Biometric- hand, finger, retina

Mantraps- one door on each side of the room

All doors unlocked, but opening one locks the other

Securing Physical Items- safes- heavy, difficult to steal, environmental
Cable Locks- temporary security, connects hardware to something solid
Privacy Filters- screen looks black when walking by
Badges & Entry Roster - security guard- physical protection
Validates identity
ID Badge- picture, name, other details
Many include RFID chip

Digital Security Prevention Methods

Antivirus/Antimalware - software the runs on the PC, must keep updated
Host Based Firewall- also called a personal firewall
Included in many OS's, can be 3rd party
Windows Firewall filters by port,app, etc.
Stops people from accessing pc from outside
Only allows communication if you have started it
Network Based Firewall- filters traffic by port number tcp/udp layer 4
Can encrypt traffic in/out of network
Can proxy traffic as well
Most firewalls can be a layer 3 device (router)
User Authentication - user name and password to gain access
Identifier- every windows account has security identifier
Credentials- password, pin, smartcard
Profile- info stored about the user (name,contact,group)
Strong Passwords - weak passwords can be easy to brute force
Hashed passwords can be brute forced online
Complexity and constant refresh
Multi Factor Authentication - more than one factor
Something you are,have,know, or do
Can be expensive, separate hardware tokens
Can be cheap - free smartphone apps
Directory permissions - NTFS permissions- much for granular that FAT
Lock down access, prevent accidental mods or deletes
VPN Concentrator- VPN- encrypts private data traversing on public network
Concentrator- encrypt/decrypt access drive
Can be hardware or software
Data Loss Prevention (DLP) - stops unencrypted data from leaking
Can be built into the firewall
Access Control Lists (ACL)-permissions associated with an object

Used in file systems, network devices, OS etc

List Permissions- “Bob can read files”

“Fred can access network”

“Jim can access network 192.168.1.0/24 using 80,443,8088”

Disabling Unused Ports - stop anyone from plugging into your network

Does not just rely on 802.1x

Required periodic audits

Smart Cards- contains a digital certificate

Multiple factors- card + pin or fingerprint

Email Filtering - unsolicited email/spam- stopped at gateway before it Gets to users

Scan & Block malware - executables

Trusted/Untrusted Software Sources- consider the source

Must not have access to the code

Trusted Source - Internal apps, well known publishers

Digitally signed

Untrusted Source - apps from 3rd party, links from emails

Drive by downloads

Security Awareness

All policies on intranet so everyone can see

In person training sessions

Company policy for visitors

How to deal with viruses procedure

Network Policies- govern network use, AUP, all rules signed

Principle Of Least Privileged- only have rights required for job

Applies to physical & digital

Windows Security Settings

Accounts - Admin- super user

Guests- Limited Access

Standard User- Regular access

Power user- not much more control than standard

Groups - assign group of users with certain permission

NTFS Permissions- apply to local and network connections

Share Permissions- apply only over the network

Most restrictive settings win deny > allow

Explicit Permissions - set default permissions for a share or object

Inherited Permissions - set a permission & applies to everything under

Explicit permissions take priority over inherited

Administrative Shares - Hidden Shares created during installation

Local Shares are created by user

View Shares - computer management/shares

-net shares

Authentication - user name & password + others

Single Sign On (SSO) - windows domain, provide credentials once

Managed through kerberos

Run as Administrator- additional rights and permissions

Can edit system files & install services

Right click + run as administrator

Bitlocker - encrypts entire volume of data including the OS

Bitlocker to go - encrypts USB flash drives

Encrypting Files Systems (EFS) on NTFS- password and username to

Encrypt key

Workstation Security

Password Complexity- no single works or obvious passwords

Strong password, atleast 8 characters

Set password expiration and require change

Password Expiration - all passwords should expire

Critical systems could expire more often

Recovery should have a formal process

Desktop Security- require a screensaver password

Disable auto run, disabled in the registry

No autorun in 7/8/8.1

Consider changing autoplay (Flash drive)

Have all security patches

Passwords- change all default usernames/passwords

BIOS- supervisor/admin password- prevent changes

User password - prevents booting

User Permissions - Not everyone should be an admin

Groups - assign rights to group, add users to group

Login Time restrictions - only able to log in during work hours

Disabling Unnecessary accounts- disable guest account if not needed

Only some accounts run services, disable interactive logins

Change default names and passwords to prevent brute forcing

Account Lockout- too many wrong passwords, can prevent brute forcing

Data Encryption - full disk or file system, removable media

Backup keys, may be integrated into AD

Patch & Update Management - built into the OS, update utility

Many apps include updater

Securing Mobile Devices

Screen Lock- fingerprint,face recognition,swipe pattern,passcode/pin

Too many fails- iOS- erase all data after 10 attempts

Android- locks device and requires a google login

Windows - delays next attempt or factory reset

Locators - built in GPS, able to find phone on a map

Control from afar, or wipe everything

Remote Backup- backup to cloud, restore with one click

Antivirus/Antimalware- iOS- equipment less vulnerable

Malware must find a vulnerability

Android- more open, apps can be installed from anywhere

Easier for malware to find a way in

WIndows phone - closed environment

Apps run in "sandbox"

Patching/OS Update- security updates, don't want to get behind

Biometric Authentication - multifactor authentication

Something you are, know, have….etc.

Authenticator Apps - random token generator

Full Device Encryption - phone keeps the key

iOS8 & later- data encrypted with passcode

Android- encryption can be turned on

Windws phone 8/8.1 - available with exchange active sync

-also available with mobile device manager

Trusted vs Untrusted Source - Do not install APK from untrusted source

iOS- all apps are checked by the app store

Andorid - google play is good, 3rd party bad

Windows- apps are created by microsoft

Firewalls- mobile phones do not include a firewall

Most activity is outbound, not inbound

Mobile firewall apps are available

Policies & Procedures - BYOD- bring your own device

MDM- mobile device manager

Centralized management of mobile devices

Set policies, data stored, camera, control device

Manage Access Control- require pins or passcodes

Data Destruction and Disposal

Physical Destruction - never to be used again

Shredder, tools, electromagnet, fire

Certificate of Destruction - done by 3rd party

Gives confirmation it was destroyed

Paper trail of when it was destroyed

Disk Formatting - Low Level Format- provided by factory

Not possible by user

Standard/Quick Format- sets up a file system

Clears master file table

Creates a boot sector

Can still be recovered

Standard Formatting - overwrites every sector with 0's

Available in windows vista and later

Cannot recover data

Hardware Security - always audit 3rd party destruction

File Level overwrite-Sdelete- windows sysinternals

Whole drive wipe - DBAN, Dariks Boot & Nuke

Secure data removal

Securing a SOHO Network

SSID Management - Service Set Identifier

Change default name to something unique

Disable your SSID broadcast

Wireless Encryption - only people with password can transmit and listen

WEP- outdated and insecure

Use WPA or WPA2

Antenna Placement - AP's close to each other should not be on same channel

Same channel will cause frequency overlap

Power Level Controls- set as low as possible so people in house can access
Make it so no one outside can access
MAC Address Filtering - Limit access through phyical address
Not foolproof, MAC cloning
Set up in WAP
WPS- wifi protected setup
Easier to connect to wifi, uses a pin configured on the AP
Push button on the AP , NFC is used
Very easily hacked, not used on modern APs
Default username and password- must change to something unique
IP Addressing - DHCP or static
IPs are easy to see on unencrypted network
Firewall Settings - Inbound- allow only required traffic
Port forwarding to map ports to device
Consider a DMZ
Outbound- blacklist- allow all, block some
Whitelist- block all, allow some
Disabling Physical Ports- disable unused ports to prevent access
Network access control- 802.1x controls
Cannot communicate unless authorized
Content Filtering- control traffic based on data within content
Can filter data for sensitive data
Can control inappropriate content
Scan against malware and viruses
Physical Access- doorlocks, biometrics

Section4: Software Troubleshooting

BSOD- startup and shutdown BSOD- bad hardware, drivers, app
Apple- pinwheel/beachball- hang or constant retries by app
Fix- use last known good configuration or safemode
Restore or remove hardware
Boot errors- cant find OS, OS could be missing
Boot loader chaged or replaced, multiple OS's installed
FIX- check boot drive, remove any media
Start up repair, command "bootrec/rebuildbcd
Improper Shutdown- should recover normally
If not, "launch startup repair" should fix most issues
Missing GUI- no login or desktop, start in VGA mode and run SFC

Update the drivers in safe mode
8/8.1- repair/refresh

Startup Repair

Missing NTLDR- main windows bootloader issue
Run startup repair, check boot device
Missing OS- boot configuration may be wrong
Run startup repair or manually configure BCD
Auto safe mode boot- run startup repair
Linux- Missing GRUB- Grand Unified Bootloader, most common
LILO- Linux Loader, least common
Missing bootloader- could be overwitten by other OS

Starting the System

Device not starting- check device manager and event viewer
remove/replace driver
“One or more services failed to start”- bad driver/hardware
Try manual start, check permission
Check file systems, reinstall app
DLL- Dynamic Link Library- code installed that many apps use
A shared library
DLL versions are very specific
Apps are written to a library version
Windows File Protection/Windows Resource Protection
Protects DLL versions to avoid conflicts
Files & Compatibility Errors- files associated with apps
Configure file types to specific apps
Control panel / default programs applet
Compatibility Tab- run app as an older windows app

Slow System Performance

Task Manager- check for CPU usage and input/output
Windows Update- Keep patches and drivers updated
Disk Space- check for available disk space or run defrag

Laptops- confirm the laptop is not in power saving mode
AV/AM- scan for any infection
Kernel Panic- unix, linux, MAC OSx, similar to windows BSOD
Stops all activity
Multiple Monitor Misalignment- monitors not "aligned"
Mouse will not move easily between screens
Just drag the monitors into alignment
Can be fixed in control panel/display/screen resolution

OS Troubleshooting Tools

BIOS/UEFI Tools- Built in diagnostics, check for temps and current stats
SFC- system file checker, integrity scan os OS files, find & corrects errors
Logs- found in windows event viewer & Boot logs
C:\windows\nbtlog.txt
Linux- individual app logs
/var/log
MAC- utilities/console
CMD- can accessed pre boot, gives you complete control
System Repair Disc- boots & provides you with recovery options
Pre-Installation Environment (PE)- minimal windows operating environment
Used for troubleshooting and recovery
Can built your own PE
MSconfig- enable/disable startup apps and services
Defragmentation- modifies file fragments so they are contiguous
Cmd-defrag
Regedit- registry editor, used to modify settings
add/modify/delete keys
Regsvr32- register/unregister DLLs
Event Viewer- see what is going on with apps, setup, security, settings
Options at Boot time- F8 to get to advanced boot options
Most recovery options are found here
Safe Mode- in advanced boot options
VGA mode- low resolution, used for video driver issues
Uninstall/reinstall/repair- 8 & 8.1 includes a refresh option
Refresh option cleans out windows without losing files

Troubleshooting Security Issues

Popups- Could be legitimate or malicious

Have an updated browser and a pop up blocker

If pop ups are not related to your browsing, scan for malware

Browser Redirection- instead of a google result, you end up elsewhere

Caused by malware, run a malware scan

Browser Security Alert- security alerts and invalid certificates

Means something is not right

Check out details by clicking the lock icon

Could be an expired or wrong domain

Malware Network Symptoms-slow performance, lockups, connectivity Issues, OS update failures

Malware OS Symptoms- Renamed system files, files disappear or become Encrypted, can change file permissions

System Lockup - completely stops, toggle caps lock to see if OS responds

May be able to terminate bad apps with task manager

Check logs after restarting to see the cause

App Crashes- apps stop working or just disappear

Check out the event log and the reliability monitor

Reliability monitor has history of app issues

Virus Alerts & Hoaxes- Rogue Antivirus- fake, may include real logs

Wants to bill you

Ransomware- asks for money or subscription for Access to your PC

Email Security- Spam- unsolicited email, phishing, ads, spreads viruses

Hijacked email- infected PCs can become email spammers

Tools for Security Troubleshooting

AV&AM- stops malware from running, must keep signatures updated daily

Sometimes they are bundled together

Recovery Console/CMD - very powerful, filesystem access

Terminal- cmd for MAC/Linux, able to modify every aspect of the OS

System Restore- create restore points, go back in time to correct problems

Does not guarantee recovery from virus/malware

LVM Snapshots- local volume manager- just like windows restore

Works very quickly

Pre Installation Environment- minimal windows OS environment

Used for troubleshooting and recovery

Event Viewer- get info about security events and whats going on in your PC

Refresh & Restore- windows 8/8.1

Refresh- reinstalls windows but keeps files and settings in place

Restore- returns to a previous restore point

MSconfig- safeboot minimal- loads GUI but no networking

Safeboot alternate shell- cmd with minimal services, no network

Safeboot active directory repair- safe mode with file explorer & AD

Safeboot:Network- uses networking

Best Practices for Malware Removal

Malware Symptoms - odd error message, unusual icons or apps, very slow

Quarantine Infected systems-disconnect from network to stop spreading

Isolate removable media

Disable System Restore- malware can also infect restore points

Delete all the restore points you have

Disable system protection

Update AV- keep signature and AV version up to date

Automate updates instead of doing it manually

Malware can prevent updates

Scan & Remove- get a well known program, use standalone removal apps

Safe mode- just enough services to get the OS running, bare minimum

May prevent the malware from running

Schedule- AV&AM automatically update signatures

Make sure OS updates are scheduled

Enable System Restore- only do once the system is clean

Educate End User- one on one training, visable posters

Troubleshooting Mobile Device Apps

Dim Display- check brightness settings

Could be a backlight issue

Wireless Connectivity- intermittent, try moving closer to the AP

None- check/enable wifi, confirm correct key

Do a hard reset

Non responsive touchscreen- Apple- iOS restart, hard or regular

Android- remove battery and put back in

Hold the power and volume button

App issues- apps run slow or not loading

Restart the phone or close out of the app

Update the app

Unable to decrypt email- built into corporate email systems

Each user has their own private key

Install individual private keys on each device

Done with the mobile device manager

Short battery life- bad reception, always signal searching

Turn off unnecessary features

Battery could be aging

Overheating- phone will automatically shut down if too hot

Check apps for CPU usage

Avoid direct sunlight

Frozen System- hard or soft reset

If problem is ongoing, do a factory reset

No sound- check volume settings for the app and phone

Bad software, delete and reload

Try headphones or external speakers

Sound starts then stops- could be dueling apps

No sound- factory reset, load the latest software

Inaccurate Touch Screen response- close some apps, low memory

Restart the device

May require new digitizer or reseat cables

System Lockout- too many incorrect password attempts

Mobile Device Security Troubleshooting

Signal drop/weak signal- only use a trusted network

Never use public wifi without a VPN

Speed test- cell tower analyzer and test

Power Drain- heavy app usage, increased network activity

Check app before install, use app scanner

Run anti malware, factory reset and clean app install

Slow Data Speeds- use a trusted wifi network

Run a wifi analyzer

Run a speed test

Examine apps for unusual activity

Unintended Bluetooth Pairing- never pair a device that isn't yours

Remove device and repair

Can just disable bluetooth completely also

Leaked Information- determine cause of data breach with AV or AM

Do a factory reset

Unauthorized Camera/Mic usage- AM scan, factory reset, app scanner

Section 5 Operational Procedures

Managing Electrostatic Discharge

Static Electricity- electricity that does not move, can be very damaging when discharged

Around 3500 volts.100v is only needed to cause damage silicon

Controlling ESD- humidity over 60% helps but does not entirely prevent

Use hand to self ground, metal case of PS works

Unplug PC from a power source

Do not touch components directly, card edges only

Use antistatic pad & wrist strap

Antistatic bags for components

Computer Safety Procedures

Remove all power sources before working on a device

Replace entire power supply versus trying to repair it

Equipment Grounding- diverts electrical faults away from people

Large equipment racks have a large groundwire

Do not use electrical grounding for static grounding

Personal Safety- Remove jewelry, neck/badge straps

Lift with legs keeping back straight, use a cart

Electrical Fire Safety- no water or foam

Carbon dioxide, FM-200, dry chemicals, remove power supply

Cable Management- tie together, avoid trip hazards

Safety glasses & air filter mask

Toxic Waste- dispose of batteries at hazardous waste facilities

CRT glass contains lead

Recycle & reuse toner, ship toner back to company

Local Government & Regulations- health and safety laws

Building & electrical codes

Environmental- proper disposal of electronic components

Managing Your Computing Environment

Disposal Procedures- check your MSDS/SDS (Material Safety Data Sheet) and Safety Data Sheet are interchangeable terms for the same thing

MSDS- product and company info

Includes ingredients, hazard info, etc.

Environmental Controls- Temperature- devices need constant cooling

Humidity- 50% is good

Proper ventilation- helps circulate the heat

UPS- uninterruptible power supply- backup battery

Types- Standby- always a primary power, has backup batteries

Line-interactive UPS- handles brownouts

On-line- always running off of the batteries

Surge Suppressor - spikes are sent to ground

Noise filter removes line noise

Surge Suppressor Specs - higher joules is better, more protection

High amp rating is good

Let through rating- less is better

Protection From Airborne particles- protects from dust,oil,smoke, etc.

Dust & Debris- cleaning with neutral detergents, non ammonia based

Use a computer vacuum, reduces static

Avoid isopropyl alcohol unless specified

Compressed air pump instead of canned air

Prohibited Activity & End User Policies

First Response- identify issue- logs, in person, monitoring data

Report to proper channels

Collect and protect info on event

Documentation - outline in security policy

Documentation must be available to employees

Detail as much as possible

Chain Of Custody - control evidence, maintain integrity

Avoid tampering, use hashes

Label and catalog, seal, store, digitally sign

Licensing/EULA - closed source- source code is private

End user only gets the .exe file

FOSS- Free and Open Source Software

End user makes their own .exe

EULA - determines how software is allowed to be used

Digital Rights Management - DRM- electronic limits on use of software

Licenses- Personal- associated with the device owned by one person

Designed for home use, one time purchase

Enterprise - site licenses, can install everywhere, annual renewals

PII- part of privacy policy, determines how to handle PII

Contents Policies - security policies

Block Policies - block by URL, app, username/group

Communication

Communication skills are needed for troubleshooting

Avoid Jargon - no acronyms or slang when helping customer

Translate technical terms for simpler terms

Avoid Interrupting- Listen to customers issue even if you know answer

Clarify Customer Statements - ask questions to clarify customers issue

Repeat your understanding to customer

Setting Expectations - offer options (repair/replace)

State the cost & time frame

Document everything

Follow up for customer satisfaction

Professionalism

Maintain a positive Attitude- keep a positive tone of voice

Problems cannot always be fixed but do your best

Have a good attitude with the customer

Avoid Being Judgemental- No insults, you are the teacher

You also make mistakes

Goal is to make people smarter

Be on time & Avoid Distractions- no phone, no talking to others

customer and their issue is your number one concern

Create an environment for conversation

Difficult Situations- Do not argue or be defensive

Make easier by listening and asking questions

Communicate even if there is no update on progress

Never vent on social media

Don’t minimize problems - technical issues can be traumatic

Must be a tech and a counselor

Maintain Confidentiality- keep private info private

IT people have access to a lot of data

Be respectful with other’s personal info

Troubleshooting Theory

Identify the problem- gather information

Get as much info & duplicate issue if possible

Identify symptoms, may be more than one

Question the end user

Determine any recent changes to environment

Establish a Theory - start with the obvious, but consider everything

Make a list of all possible causes

Test The Theory - confirm the theory, determine the next steps

Re-establish theory if it did not work

Call an expert for other ideas

Create A plan of action - once theory is working, correct the issue

Some issues cannot be fixed curing regular hours

All plans can go bad, have a plan A,B, & C

Implement the Solution - fix the issue

Escalate if necessary, may need 3rd party

Verify Full System Functionality- confirm the solution solved the issue

Have the customer test and confirm also

Implement preventative measures

Document Finding- Don’t lose the knowledge

Consider a formal database