Ch 25 - Care and Feeding of Mobile Devices

Maintaining Mobile Devices

- CDMA phones do not use SIM cards; GSM phones use SIM cards
- IMSI defines critical SIM information, IMEI defines the phone itself
- All mobile 0893 have built-in VPN and backup software
- Anti-malware is common for Android, less so for iOS

Only 2 Kinds of Cell Phones -

GSM (Global System for Mobile Communications) - Come with a SIM Card

CDMA (Code Division Multiple Access) - Don't use a SIM Card

Lots of things that need to be Upgraded

Firmware - There's no Storage where we store things,
so we store things on ROM, which needs to be Updated

Baseband Updates - Cellular Related
Broadband Updates -
Radio Firmware Updates -

PRL (Preferred Roaming List) - If Texting is running Slow,
or Phone Calls are taking long to connect,
consider updating your PRL.
Something like *228 (Star228)

PRI (Product Release Information) - Big chunk of updates that hit
all at once, which includes updating PRL.

These updates are for the most part pretty good, so don't hesitate to update!!

IMSI (International Mobile Subscriber Identity) - This # gives Personal Information
through your SIM Card (so this won't be for CDMA),
like what Payment Plan you have.

IMEI (International Mobile Equipment Identity) - This # defines the Phone
*#06# (type this for your number).
To Activate your Phone, you need to connect IMEI & IMSI.

VPN (Virtual Private Network) - You can setup a VPN on your Phone,
just like you can on your Desktop!

3rd Party VPN's are better than the one built into your phone
Give the VPN a Name
Set up VPN
Need your Server's IP Address

Remote Backups - Android → Google Drive iOS → iCloud
Make sure you have Remote Backup Turned On!!!

Antivirus & Anti-Malware - you can install this on your Phone,
but for the iPhone it's nearly not necessary
because of the tight quality control in the Stores.

The iPhone & Android Stores are regulated high quality Trusted Apps,
which aren't of concern to download & install.

Android - for the freedom, you can download Apps from Websites,
which can lead to Untrusted Apps

Firewalls - If you're going to be using Untrusted Apps,
you're going to be dealing with Firewalls.

Host based Firewalls are just as important on a Smart Device as they are on a Desktop. Because of these regulated Stores, it's less of an issue on an Apple Device than an Android Device.

If you just stick to the Store on either of these types of devices,
chances are very slim you'll need Antivirus, Anti-Malware, or Firewall.

Mobile Devices and Email

- E-mail setup on smartphone always means adding an e-mail account
- Traditional e-mails require SMTP and an IMAP/POP server address and account passwords
- Most traditional e-mail servers use encrypted port numbers

Configuring Email on a Mobile Device -

Recall what we already know about email….

2 Different Protocols for Incoming Email: POP3 or IMAP
and for Outgoing Email: SMTP

Corporate Email Configuration -

Accounts → Add an Account → Personal (IMAP)

Need to know…

For SMTP Server…...

1) FQDN (Fully Qualified Domain Name)
2) Username & Password
3) Port Number (usually Port 25)

For IMAP Server…...

4) FQDN
5) Username & Password
6) Port Number (usually Port 143)

Encrypted Ports…..

POP3 - Port 995 IMAP - Port 993 SMTP - Port 465 or 587

What you get out of using these is P2PE (Point-to-Point Encryption)

S/MIME (Secure/Multipurpose Internet Mail Extensions) - If you've ever attached anything to an email to be sent out, you've used MIME, which takes a binary file, and takes every 8 bits and turns it into an ASCII Code ("Ass-Key") (text) and gets interpreted by the receiving thing and it's able to reconstruct your file.

Encrypting emails is relatively new, so what we used to do is
Encrypt the Attachments going through the process of S/MIME.
S/MIME is an obsolete term, because today all emails are encrypted end-to-end

ProtonMail - Fully Encrypted from End-to-End

Today, we tend to move towards Point-to-Point Encrypted Emails,
and S/MIME is forgotten.

Mobile Synchronization

- Synchronization - update 2 or more data stores so their information is identical
- We synchronize our devices to a desktop, to an automobile, or to the cloud
- Android syncs with Google Drive; iOS devices sync with iCloud
- Most browsers provide synchronization as well
- We can also sync location, ebooks, social media, and applications

Synchronization - update 2 or more data stores so their information is identical
Contacts

Backup - Copy of something rather than having the need for it to be Synchronized

Synchronizing to the Desktop -
iTunes - Synchronizes all of your Music from your Phone onto your Desktop

Synchronize to an Automobile -
Bluetooth - make Phone Calls with your Voice, GPS Functions

Synchronize to the Cloud -
Google Drive, iCloud - All of your Devices are doing Cloud Synchronization

Types of Data to Synchronize - Calendar, Contacts, Docs, Gmail, Music, etc

Bookmarks - Create an Account with your Web Browser, Sign In,
and Customize your Synchronization Settings

Location Data - GPS Apps Need this info
E-Books - Sync your Purchased Books to your E-Reader Device (Kindle)

Social Media - Your Sync is handled within the App & the Service

Mobile Device Security

- Screen locks prevent others from accessing your phone and use fingerprints, pin codes, passwords, or facial recognition
- Multifactor authentication means to use more than one way to authenticate
- Authenticator apps add an extra layer of security
- Location apps like Find My Phone help locate lost devices

Screen Lock - Swipe (really no security here), Pattern, PIN, Password
Face Recognition - Need a 3rd Party App for Android

Multifactor Authentication - requires more than one of these
Usually done for Apps

Number of Failed Log In Restrictions -

Authenticator Apps - Be Careful with these. Can be an issue if you lose your Phone and are Restoring your Backup Info

Locator Apps - “Find My iPhone” & “Android Device Locator”
Google “Find My Device”
Locates your Device on a Map
Play Sound
Secure Device (Device Lockout)
Erase Device

MDM (Mobile Device Management) - Enables Organizations to account for devices to Process, Store, Transmit, and Receive Organizational Data

BYOD (Bring Your Own Device) -

COPE (Corporate-Owned Personally Enabled) -

Mobile Security Troubleshooting

- Take time to memorize the security troubleshooting scenarios
- Many security troubleshooting scenarios are simple misconfiguration
- Practice these scenarios on both Android and iOS if possible

Signal Drop/Weak Signal - Somebody might be Turning Down your Connectivity
This is what people want to do when attacking your Device.

They don't want you to be Connecting, or Updating,
or anything being Checked.

This type of thing is very obvious, as far as location goes.
If you're in a big city where you should be having 5 bars,
and everything drops off completely.
This is different than being out in the country and having no service.

If you suspect this is intentional, Turn Off your Device & check it out later.

Power Drain/Slow Data Speeds/High Resource Utilization -
This points to somebody who put something on your Device.
Typically an Android issue, rather than an Apple Device.
Run some sort of Anti-Malware.
Anti-Malware for Android is good, but isn't perfect.

Check your Accounts & Change your Passwords!!
Factory Reset & Reinstall from Scratch

Unintended Wi-Fi/Bluetooth Connection -
Don't use Broad AT&T/Verizon/etc Connections
People wait for you to connect to these & have their way with your device

Check your Accounts & Change your Passwords!!
Factory Reset & Reinstall from Scratch

Results of a Hack - Leaked Personal Files/Data, Unauthorized Account Access (Facebook is having things you never put in there), Unauthorized Location Tracking, Unauthorized Camera/Microphone Activation

Mobile Device Troubleshooting

- Take time to memorize the many troubleshooting scenarios
- Keep in mind that many troubleshooting scenarios are simple misconfiguration
- Practice these scenarios on both Android and iOS if possible

Inaccurate/Non-Responsive Touchscreen -

If you're system is overloaded, your touchscreen moving really slowly/jaggedly is a sign your system is too full of stuff.

Restart your System. Try Uninstalling some of your Apps.

Dim Display - Turn Up your Brightness. Is your Auto-Brightness on?

The backlights on any display will go bad over time/usage, so this just happens.

Cannot Display to External Monitor -

Are you on the same Wireless Network as this External Monitor?
Make sure that you're trying to connect to the right External Monitor!
Can't assume that all External Monitors will Instantly work with your Device. Check with the Manufacturer

No Sound from Speakers -

Trying to play sound from speakers, but device is connected to Headphones & playing from there instead. Un-Pair any Bluetooth Devices

Volume - check ALL of the different sources where you can adjust volume!!! Speaker Knobs, Windows Volume Adjust, Application/Website Volume, Volume Knob on your SmartBoard

Intermittent/No Wireless Connectivity - New wall built/Physical Interference, Baby Monitor near Router, Relocation of your Router, Antennas Adjusted, SSID Password Changes

No Bluetooth Connectivity - Make sure Device is in Discoverable Mode
Is anyone else connected to the Device?, Make sure Bluetooth is Turned On!!

Apps Not Loading/ App Log Errors -
Many Apps use Caching. Clear the Cache & Try again.
Forced Stop to Shut the App Down.
Restart your Phone!
Reinstall the App
Double Check on Google. You're probably not the only one having this issue.

Slow Performance - You're Running too many Apps!!!
You can't upgrade your RAM/ROM, so close some Apps!

Extremely Short Battery Life - Things that burn your battery life…..
GPS Anything that's Running Real Time in the Background
Constantly Syncing

Overheating - All Smart Devices have Thermal Trip Switches built into them
that should prevent a Device from getting too Hot.
They will fail if you don't provide any form of Ventilation.

Frozen System - Problem with an App
Streaming Apps steal a lot of CPU Cycles
because they're waiting for something to come in from the Network.
You may run into the "Black Screen of Death" on an Android

Delete the App and wait for a Patch for that App

System Lockout - Typing in a Password too many times
Factory Reset & Reinstall
Usually from someone else trying to do something evil.
Someone trying to sell you a $1000 phone for $200 and it has a System Lockout
It was probably stolen.