RV College of Engineering®

Go, change the world

22EM106-Introduction to Cyber Security

UNIT- V

Chapter-2: Digital Devices security, Tools, and Technologies for Cyber Security

Course Incharge: Dr.Mohana
Department of Computer Science & Engineering (Cyber Security)
RV College of Engineering, Bangalore-560059

Unit - V Syllabus

Unit-V	8 Hrs
Digital Devices security, Tools, and Technologies for Cyber Security End Point device and Mobile phone security, Password policy, Security patch management, Data backup, Downloading and management of third-party software, Device security policy, Cyber Security best practices, Significance of host firewall and Ant-virus, Management of host firewall and Anti-virus, Wi-Fi security, Configuration of basic security policy and permissions.	

Digital security: Introduction

- This increased reliance on the internet and digital networks brings risks along with the convenience it provides.
- banking, bill paying, social planning etc. even parts of our job.
- Online criminals, hackers, even just bored mischief-makers lurk in the shadows, waiting to rob you, commit fraud, steal your identity, or simply embarrass.
- digital information security is of paramount concern

What is Digital Security?

- collective term that describes the resources employed to protect your online identity, data, and other assets.
- These tools include web services, antivirus software, smartphone SIM cards, biometrics, and secured personal devices.
- digital security is the process used to protect your online identity.

Difference Between Digital Information Security and Cyber Security

- Illegally accessing someone's data, identity, or financial resources is called a "cybercrime,"
- Digital security involves protecting your online presence (data, identity, assets).
- cyber security covers more ground, protecting entire networks, computer systems, and other digital components, and the data stored within from unauthorized access.
- Digital security a sub-type of cyber security.
- Digital security protects information, and cyber security protects the infrastructure, all systems, networks, and information.

What Kind of Information is Considered a Digital Security Risk?

- Personal Identification Data
- Personal Payment Data
- Personal Health Data

Different Types of Digital Security

- Antivirus Software
- Current, Updated Firewalls
- Proxies
- Remote Monitoring Software
- Vulnerability Scanner

Specific Examples of Digital Security Tools

Instant Message Encryption Tools

- ChatSecure is a messaging app that offers secure encryption for Android and iOS phones, and
- Cryph secures your Mac or Windows-based web browsers.

Navigation Privacy Tools

- Anonymox protects your identity by creating a proxy, letting you change your IP and surf anonymously. It's available as an add-on for Google Chrome and Firefox.
- Tor isolates every website you explore, so advertisements and third-party trackers can't lock into you. It also your browsing history, removes cookies, and provides multi-layer encryption.

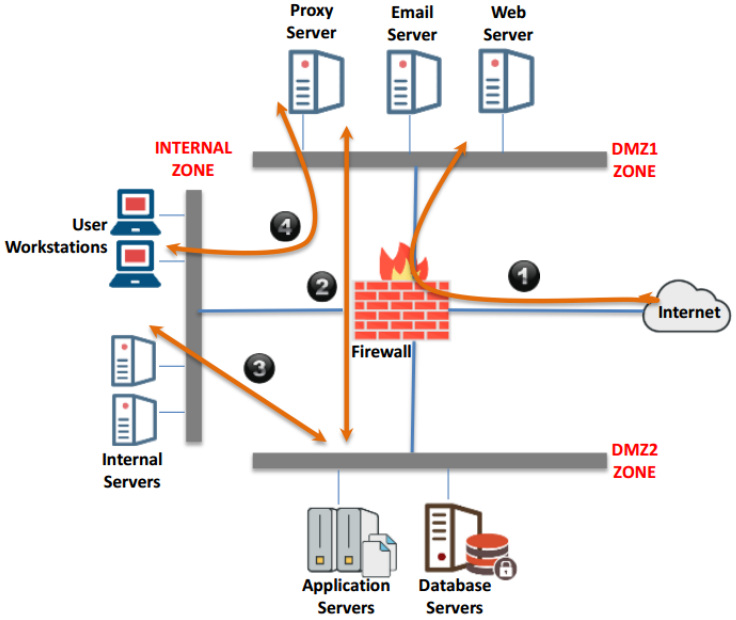
Telephone Encryption Tools

- SilentPhone offers smartphone users end-to-end encryption for voice conversations, messaging, file transfer, video, and more.
- It’s compatible with Android and iOS devices and is free.
- Signal is an independent nonprofit resource that lets users share text, GIFs, voice messages, photos, videos, and data files.

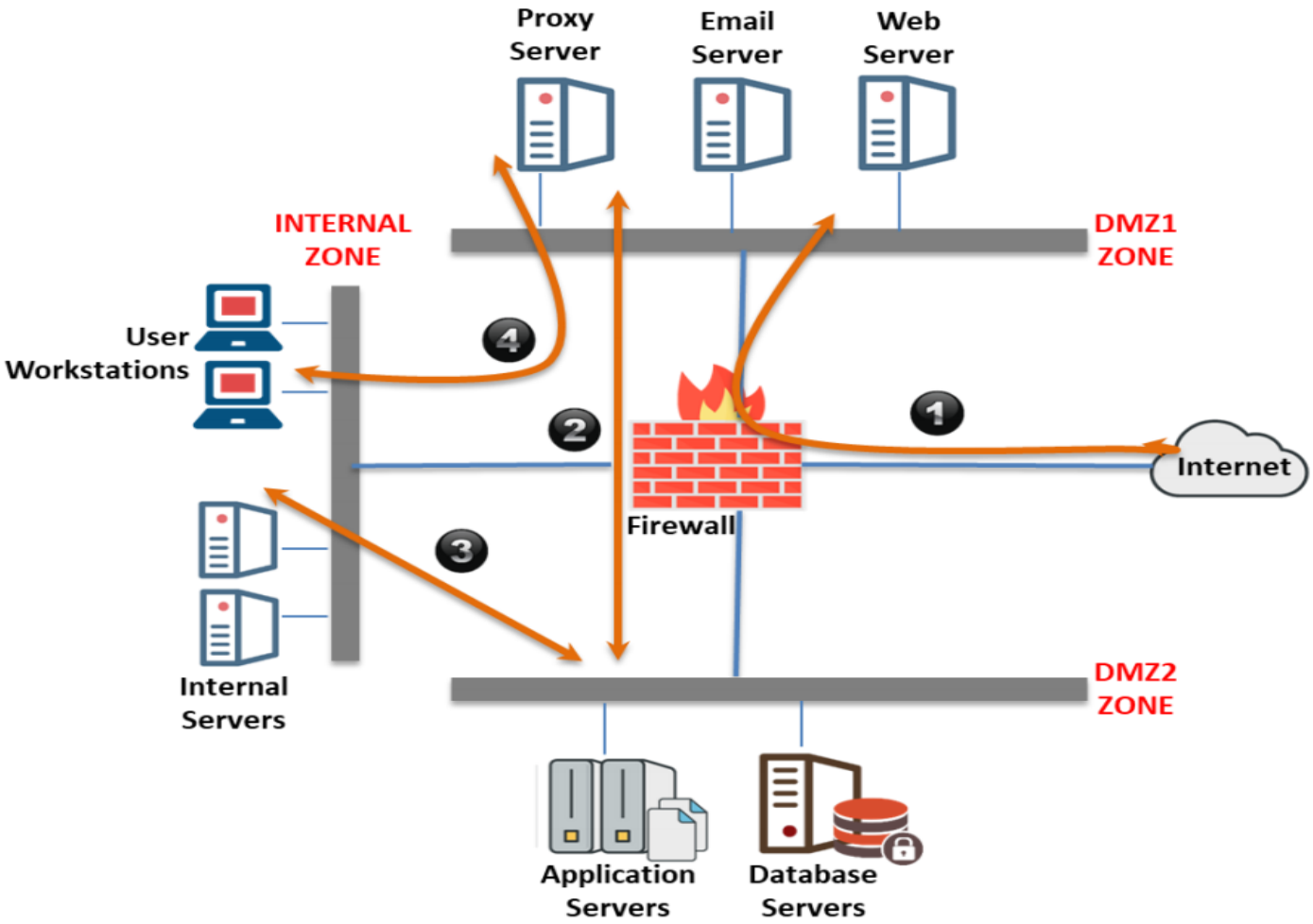
Network Segmentation

What is Network Segmentation?

- Network segmentation is the practice of **splitting** a network into smaller network segments and separating groups of systems or applications from each other
- In a segmented network, groups of systems or applications that have no interaction with each other will be placed in different network segment
- Security benefits of Network Segmentation
  - ✓ Improved Security
  - ✓ Better Access Control
  - ✓ Improved Monitoring
  - ✓ Improved Performance
  - ✓ Better Containment

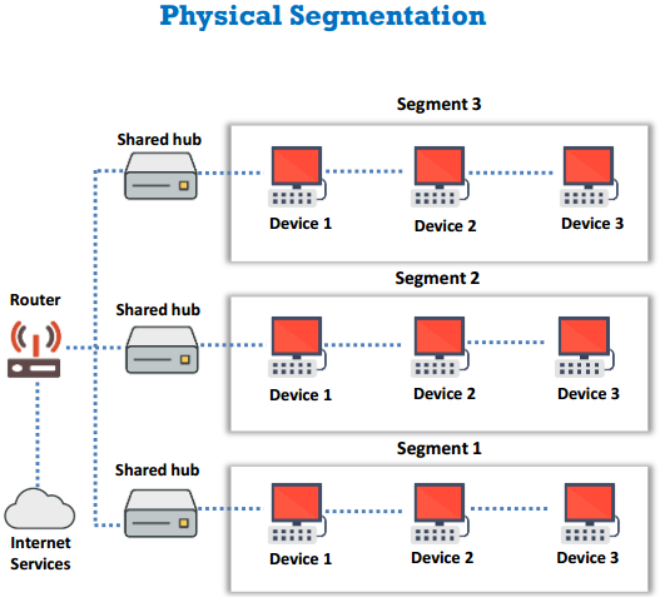


Working Principle of Network Segmentation



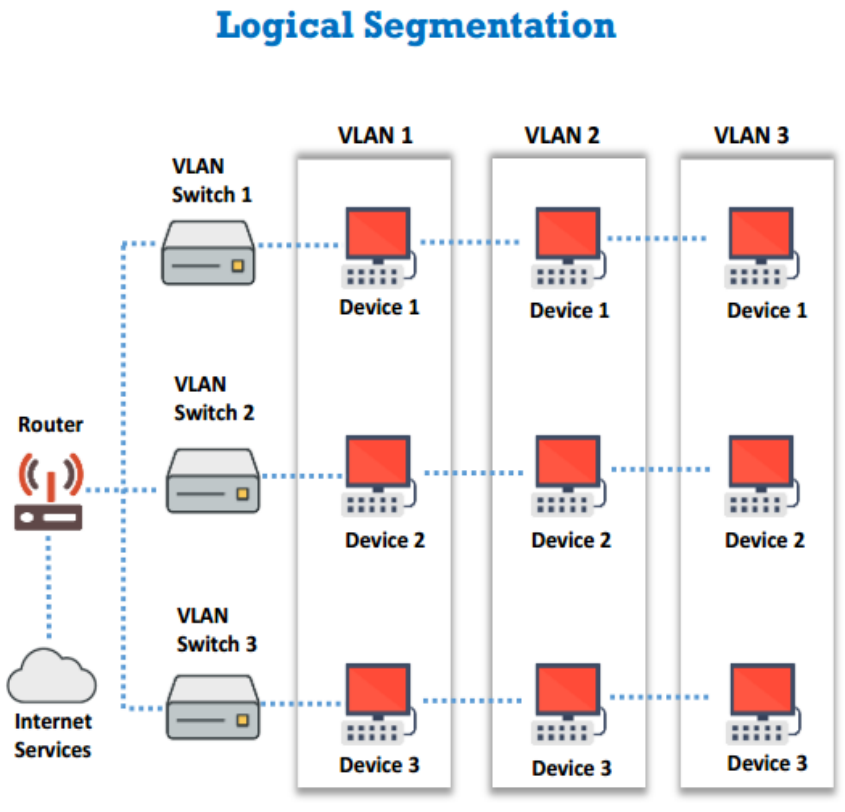
Types of Network Segmentation

- Physical segmentation is a process of splitting a larger network into **smaller physical components**
- These segments can communicate via **intermediary devices** such as switches, hubs, or routers
- Physical network segmentation can be an easy approach to divide a network, but it is **expensive** as it occupies more space



Types of Network Segmentation (Cont'd)

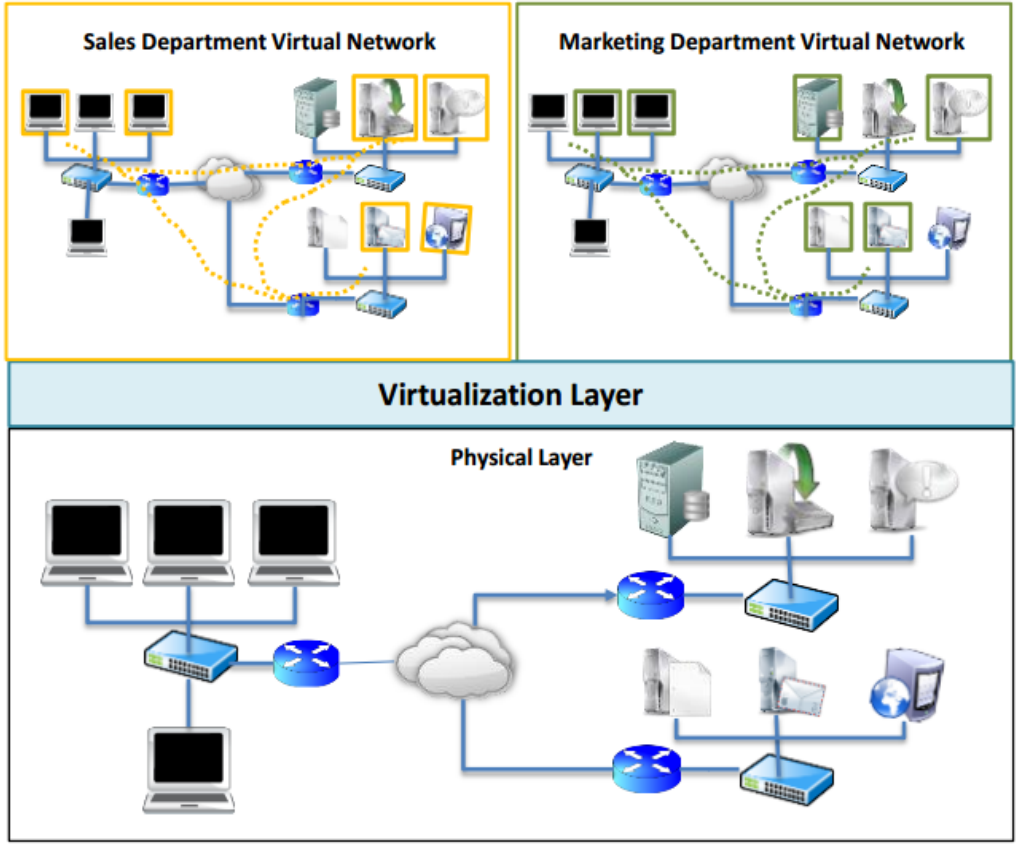
- Logical segmentation utilizes **VLANs**, which are **isolated logically** without considering the physical locations of devices
- Each VLAN is considered an **independent logical unit**, and the devices within a VLAN communicate as though they are in their own isolated network
- In this approach, **firewalls** are shared, and **switches** handle the VLAN infrastructure
- It is easier to implement and flexible to operate



Types of Network Segmentation (Cont'd)

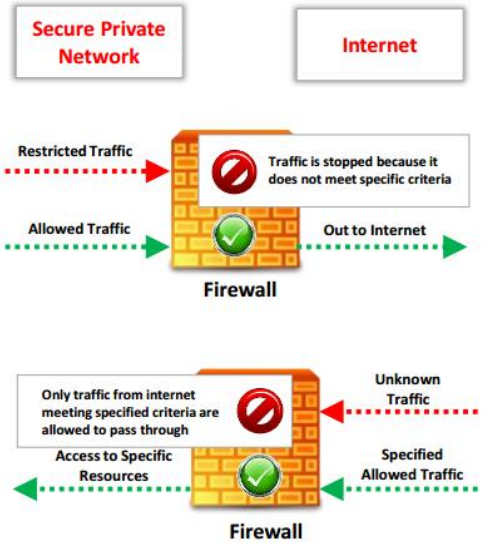
Network Virtualization

- Network virtualization is a process of combining all the available network resources and enabling security professionals to share these resources amongst the network users using a **single administrative unit**
- Network virtualization enables each user to access available network resources such as files, folders, computers, printers, hard drives, etc. from their system

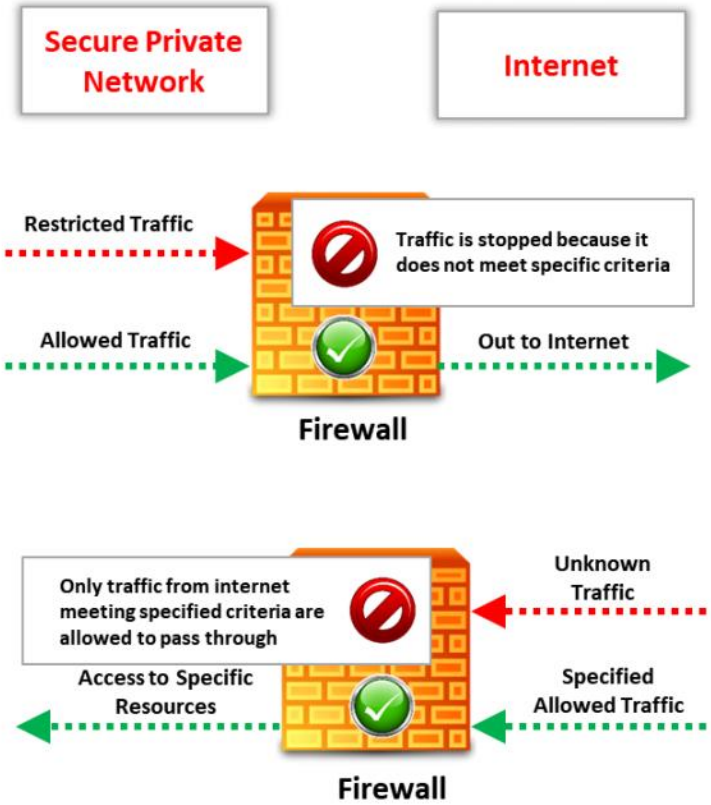


What is a Firewall?

- Firewall is a software or hardware, or a combination of both, **which is generally used to separate a protected network from an unprotected public network**
- It monitors and filters the incoming and outgoing **traffic** of the network and prevents unauthorized access to private networks



Working of a firewall:

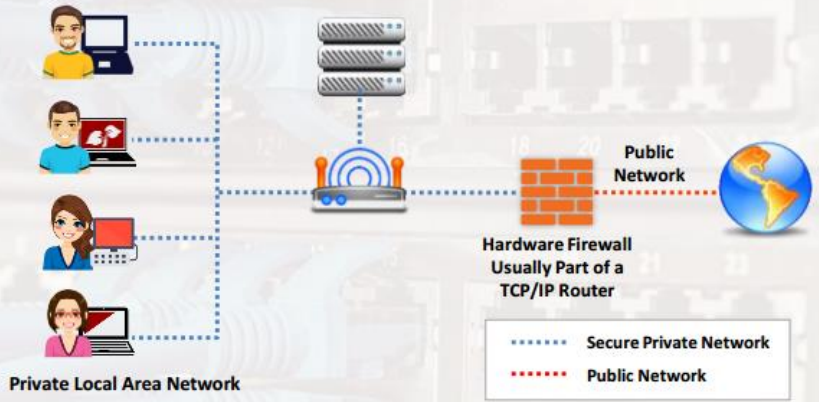


Types of Firewalls: Hardware Firewalls

01 A hardware firewall is either a dedicated **stand-alone hardware device** or it comes as part of a router

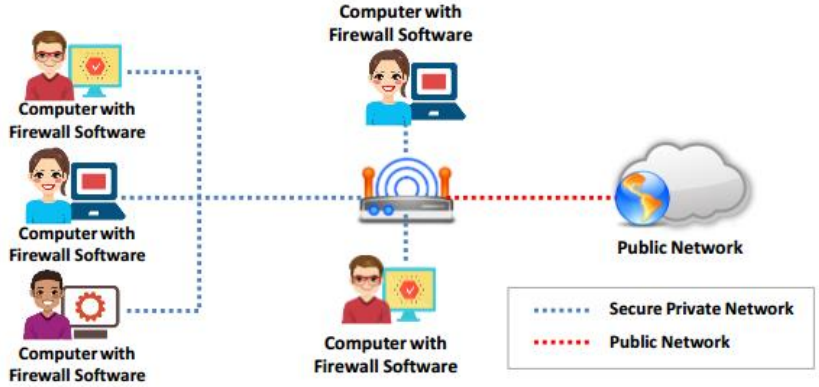
02 The network traffic is filtered using the **packet filtering** technique

03 It is used to **filter out** the network traffic for large business networks



Types of Firewalls: Software Firewalls

- A software firewall is a **software program** installed on a computer, just like normal software
- It is generally used to **filter traffic** for individual home users
- It only filters traffic for the computer on which it is **installed**, not for the entire network



Note: It is recommended that you configure both a software and a hardware firewall for best protection

Types of Firewalls: Host-based and Network-based Firewalls

Host-based Firewalls

- The host-based firewall is used to filter inbound/outbound traffic of an **individual computer** on which it is installed
- It is a **software-based** firewall
- This firewall software comes as part of OS
- **Example**: Windows Firewall, Iptables, UFW etc.

Network-based Firewalls

- The network-based firewall is used to filter inbound/outbound traffic from **Internal LAN**
- It is a **hardware-based** firewall
- **Example**: pfSense, Smoothwall, Cisco SonicWall, Netgear, ProSafe, D-Link, etc.

Note: It is recommended to configure both a host and network-based firewall for best protection

Configuring Firewall

Mobile phone security

- Smartphones
- They face most of the security challenges we associate with computers, plus a number of additional threats related to portability, ubiquity, insecure network architecture, location tracking, media capture and other such considerations.

OPERATING SYSTEMS

- Google's Android or Apple's iOS
- iOS works only on Apple devices and makes it much more difficult to run applications that have not been approved by Apple.
- updates is one of the most important considerations
- Some cheaper models do not provide access to updates that are needed to fix important security flaws.
- This could leave you vulnerable to malware or other attacks.

BRANDED AND LOCKED SMARTPHONES:

- Smartphones are often sold locked to a specific carrier or mobile network operator.
- This means that the specific smart phone will only work with that company's SIM card.
- Mobile network operators often customise the operating system and install additional software on locked smartphones.
- They may also disable some functionality. This could leave you with apps on your smartphone that you cannot uninstall or prevent from accessing your information, including your contacts and storage.
- it is usually safer to buy an unlocked smartphone that is not locked to a particular mobile provider.
- Unfortunately, these are often more expensive.

BASIC SECURITY SETUP:

- help to manage the security of the device
- **use Google's Play store for Android or Apple's App Store for iOS devices.**
- Android apps in various places online, Some of these apps contain malware.
- Only install software that comes from a source you trust.
- Applications in the Play Store and in the App Store benefit from a limited review by Google and Apple, respectively
- Even "official" apps sometimes behave poorly.
- it asks for permission to send your contacts over a mobile data connection to a third party, you should be suspicious.

- keep all of your apps up-to-date.
- uninstall apps that you no longer use.
- A new owner could alter an app that you have already installed and push a malicious update.

MOBILITY AND THE VULNERABILITY OF INFORMATION:

- The mobile phones we carry around with us often contain sensitive information.
- Call logs, browser histories, text and voice messages, address books, calendars, photos and other useful functions can become liabilities if the device on which they are stored is lost or stolen.

- sensitive information on your mobile phone as well as the online data to which it grants automatic access.
- These data have the potential to endanger not only the device's owner, but everyone who appears in their address book, inbox or photo album.

DEVICE AND DATA ENCRYPTION

- Recent iOS devices have strong encryption turned on by default, as long as you set a strong passcode.
- Android supports device encryption as well, and you should enable it if you can. Remember to back up the contents of your smartphone before turning on full disc encryption in case there is a problem while the phone is encrypting itself.

ACCESS TO YOUR PHONE

- Enable Lock SIM card, found under Settings -> Personal -> Security -> Set up SIM card lock.
- Set up a Screen Lock, found under Settings -> Personal -> Security -> Screen Lock, which will ensure that a code, pattern or password needs to be entered in order to unlock the screen once it has been locked.
- Set the security lock timer, which will automatically lock your phone after a specified time.

DEVICE ENCRYPTION

- Settings -> Personal -> Security -> Encryption

NETWORK SETTINGS

- Turn off Wi-Fi and Bluetooth by default. Ensure that Tethering and Portable Hotspots, under Wireless and Network Settings, are switched off when not in use.
- Settings -> Wireless & Networks -> More -> Tethering & Mobile hotspot.

LOCATION SETTINGS

- Switch off Wireless and GPS location (under Location Services) and mobile data (this can be found under Settings -> Personal -> Location).

CALLER IDENTITY

- If you want to hide your caller-ID, go to Phone Dialler -> settings -> Additional Settings -> Caller ID -> hide number.

SOFTWARE UPDATES

- The phone operating system: go to: settings -> About phone -> updates -> check for updates.
- Apps you have installed: Open the Play store app, from the side menu select My Apps.

Password policy

Password- Basics

- Choosing the right password

- Use at least eight characters, the more characters the better really, but most people will find anything more than about 15 characters difficult to remember.
- Use a random mixture of characters, upper and lower case, numbers, punctuation, spaces and symbols.
- Don't use a word found in a dictionary, English or foreign.
- Never use the same password twice.

Things to avoid

- Don't just add a single digit or symbol before or after a word. e.g. "apple1"
- Don't double up a single word. e.g. "appleapple"
- Don't simply reverse a word. e.g. "elppa"
- Don't just remove the vowels. e.g. "ppl"
- Key sequences that can easily be repeated. e.g. "qwerty","asdf" etc.
- Don't just garble letters, e.g. converting e to 3, L or i to 1, o to 0. as in "z3r0-10v3"

- Choose a password that you can remember so that you don't need to keep looking it up, this reduces the chance of somebody discovering where you have written it down.
- Choose a password that you can type quickly, this reduces the chance of somebody discovering your password by looking over your shoulder

Bad Passwords

- Don't use passwords based on personal information such as: **name, nickname, birthdate, wife's name, pet's name, friends name, home town, phone number, social security number, car registration number, address** etc. This includes using just part of your name, or part of your birthdate.
- Don't use passwords based on things located near you. Passwords such as **"computer", "monitor", "keyboard", "telephone", "printer**", etc. are useless.
- Don't ever be tempted to use one of those oh so common passwords that are easy to remember but offer no security at all. e.g. "password", "letmein".
- Never use a password based on your username, account name, computer name or email address.

Choosing a password

- Use good password generator software.
- Use the first letter of each word from a line of a song or poem.
- Alternate between one consonant and one or two vowels to produce nonsense words. eg. "taupouti".
- Choose two short words and concatenate them together with a punctuation or symbol character between the words. eg. "seat%tree".

Changing your password

- You should change your password regularly, I suggest once a month is reasonable for most purposes.
- You should also change your password whenever you suspect that somebody knows it, or even that they may guess it, perhaps they stood behind you while you typed it in.
- Remember, don't re-use a password

Protecting your password

- Never store your password on your computer except in an encrypted form. Note that the password cache that comes with windows (.pwl files) is NOT secure, so whenever windows prompts you to "Save password" don't.
- Don't tell anyone your password, not even your system administrator
- Never send your password via email or other unsecured channel.
- Yes, write your password down but don't leave the paper lying around, lock the paper away somewhere, preferably off-site and definitely under lock and key.
- Be very careful when entering your password with somebody else in the same room.

Remembering your password

- Remembering passwords is always difficult and because of this many people are tempted to write them down on bits of paper. this is a very bad idea.
- Use a secure password manager, see the downloads page for a list of a few that won't cost you anything.
- Use a text file encrypted with a strong encryption utility.
- Choose passwords that you find easier to remember.

Bad Examples

- "fred8" - Based on the users name, also too short.
- "christine" - The name of the users girlfriend, easy to guess
- "kciredref" - The users name backwords
- "indescribable" - Listed in a dictionary
- "iNdesCribaBle" - Just adding random capitalisation doesn't make it safe.
- "gandalf" - Listed in word lists
- "zeolite" - Listed in a geological dictionary
- "qwertyuiop" - Listed in word lists
- "merde!" - Listed in a foreign language dictionary

Good Examples

- None of these good examples are actually good passwords, always choose your own password don't just use somebody elses.

- "mItWdOtW4Me" - Monday is the worst day of the week for me.

four main techniques hackers can use to get hold of your password:

Steal it:

- That means looking over your should when you type it, or finding the paper where you wrote it down.
- it's very important that if you do write your password down you keep the paper extremely safe.
- Also remember not to type in your password when somebody could be watching.

Guess it:

- people use a password based on information that can easily be guessed.
- Psychologists say that most men use 4 letter obscenities as passwords and most women use the names of their boyfriends, husbands or children.

A brute force attack:

- This is where every possible combination of letters, numbers and symbols in an attempt to guess the password.
- While this is an extremely labour intensive task, with modern fast processors and software tools this method is not to be underestimated.
- A Pentium 100 PC might typically be able to try 200,000 combinations every second this would mean that a 6 character password containing just upper and lower case characters could be guessed in only 27½ hours.

A dictionary attack:

- A more intelligent method than the brute force attack
- This is where the combinations tried are first chosen from words available in a dictionary.
- Software tools are readily available that can try every word in a dictionary or word list or both until your password is found.
- Dictionaries with hundreds of thousands of words, as well as specialist, technical and foreign language dictionaries are available, as are lists of thousands of words that are often used as passwords such as "qwerty", "abcdef" etc.

Two step authentication process

- Two-Step Verification is an additional layer of security that you can add onto your Gmail account.
- When enabled, you will have to enter your password, and enter a special code that is sent to your device, or verify the sign in attempt on your phone.
- This dramatically increases the security of your account and makes sure that hackers can't get into your account even if the guess or steal your password.

Method 1 Text Message or Voice Call

- Decide if you want to use the text message or voice call option.
- With this enabled, a code will be sent to your phone via text, or Google will call your phone and tell you the code.
- You then enter this code into the sign in prompt in order to sign in.

USING PASSWORD MANAGER

- Password managers are one of the best ways to store, back up and manage your passwords.
- A good password is hard to remember and that's where a password manager comes in handy.
- It encrypts all the different passwords that are saved with a master password, the only one you have to remember.
- USING PASSWORD MANAGER List

WI-FI SECURITY