① Various Types Of Cyber Crime are :

i) Cyber Stalking :- It is an act of stelking, harassing or threatning someone using Internet/Computer as a medium. This is often done to defame a person and use email, social network, instant messanger, web posting etc. as a using Internet as a medium as it offers anonymity. The behaviour includes false accusations, threats, sexual exploitations to minoss, monitoring etc.

ii) Forgery and Counterfeiting : It is a use of computer to foregery and Counterfeiting is a document. With the advancement in the hardware and the software it is possible to produce couterfeit which matches the original document to such an extent that it is not possible to judge the authenticity of the document without expert judgement.

iii) Software Piracy and Crime related to IPRs : Software Piracy is an illegal reproduction and distribution for personal use or business. It comes under crime related to IPR infringement. Some of the other crimes under IPR infringement are: download of songs, movies etc.

iv) Cyber Terrorism : It is defined as the use of computer resources to intimidate or ~~an individual~~ coerce government, the civilian population or any segment thereof in furtherance of political or social objective

v) Phishing :- It is a process of acquiring Personal and sensitive information of an individual via email by disguising as a trustworthy entity in an electronic communication. The purpose of Phising is identity theft and the personal information like username, password and credit card number etc. may be used to steal money from user account. If a telephone is used as a medium for identity theft, it is known as voice Phising.

vi) Computer Vandalism :- It is an act of Physical destroying computing resources using physical force or malicious code.

vii) Computer Hacking :- It is a practice of modifying computer hardware and software to accomplish a goal outside the creator's original purpose. The purpose of hacking a computer system may vary from simply demonstration of the technical ability, to sealing, modifying or destroying information for social, economic or political reasons. Now the corporate are hiring hackers, a person who is engaged in hacking computers, to intentionally hack the computer of an organization to find and fix security vulnerabilities.

(2) A) Role Of Antivirus :- Antivirus software is designed to prevent computer infections by detecting malicious software, commonly ~~called~~ by malware, on your computer

and, when appropriate, remoing the malware and disinfecting the computer. The purpose of antivirus software is to detect, neutralize or eradicate malware. Antivirus software not only will identify and destroy the computer virus, but it also designed to fight off other kinds of threats such as phishing attacks etc.

B) **Secure Passwords :**

Things To Do : • Use at least eight character.
• Use a random mixture of characters, upper and lower case, number, puctuations, spaces and symbols.
• Dont use a word found in a dictionary, English or foreign.
• Never use the same password twice.

Things Not To Do : • Not just add a single digit or symbol before or after a word. E.g 'ABC1'.
• Dont double up a single Word E.g 'ABCABC'.
• Dont simply reverse a word E.g 'egnaro'.
• Dont just remove the vowels E.g 'rng'.
• Dont use key sequences that can easily be repeated. E.g 'qwerty', 'asdf', 'zxcv' etc.
• Dont just garble letters E.g Converting E to 3, L or l to 1, o to 0.

C) **Two-Step Authentication :** Two step authentication is an additional layer of security that you can add onto your gmail. 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 basically increase the security of your account and make sure that hackers cant get into your account even if the guess or steal your password.

D) Password Manager:- We use password to ensure security and the confidentiality of our data. One of the biggest modern day crimes is identity theft which is easily accomplished when password are compromised. The need of the hour is good password management. Have you ever thought of an alternative to remembering your passwords and not repeatedly entering your login credentials. Password managers are one of the best way 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.

E) Wifi Security:- Anyone with Wifi connectivity in his computer can connect to unsecured access points. Anyone in the range can connect to an access point if it is unsecured. Once the connection is established the attacker can send mails and perform other attacks also. All these criminal acts will naturally be associated with the legal user of access point. It is upto the legal user of the access point to defend himself to prove that he has not been involved in these acts. It now becomes the responsibility of the user to secure his own access point.

③ Best Practice for Windows &

Security refers to provide a protection system to computer system resources such as CPU, memory, disk, software programs and most importantly data/information stored in the computer system. If a computer program is run by an unauthorized user, then he may cause several damages to computer or data stored in it. So a computer system must be protected against unauthorized access, malicious access to system memory, viruses, worm etc. We can secure windows by using -

- Authentication
- One time passwords
- Program Threats
- System Threats
- Computer security Classifications

Date
Page

⇒ Best Practice For Android :-

i) Installing Safe Applications :- The easiest and safest way to install new application on android is to use Google's Play Store.

ii) Store encrypted Data :- Whenever you have to store the important or Personal data on your Android Phone then try to store that data in encrypted form or try that data should be password protected.

iii) Recording Password Safely :- You can store most of your Passwords in a single, encrypted file on device by installing some apps. These apps allow you to remember a single, strong master password and use it to lookup your passwords. This is the safest method.

iv) Physical Device Security :- Always set a strong screen lock code and avoid sharing it with others. Regularly backup important data from phone to computer.

v) Spam applications :- If someone sends you a application by a spam email or mesege then dont try to install that application, that may be virus.

⇒ **Best Practice For IOS &**

i) **Encryption** & You can easily protect the content on your device using encryption. If someone gets physical access to your device, they will also need password for decryption.

ii) **Safe Applications** :- The safest and easiest way to install or download new applications on iOS is to use Apple's Store.

iii) **Malicious Applications** & If some random person sends you any link of website or application then dont try to open that link. It might be some malware or virus which will delete your whole data or do something illegal,

iv) **Secure Password** & In iOS, there is an application named MiniKeyPass which can help you to remember a single, strong master password and use it to lookup your passwords.

v) **Scree Lock** & Always set a strong screen lock code and avoid sharing with others. Also try to change passwords after some time.