Class – 8
Subject- ICT
Chapter-3
Video no- 2

Malware: - The common names of all harmful software that enter the computer and damage it is malware.
Name of some malware software: - Computer virus. Worm, Trojan horse, Rootkits, Kilgar, Dialer, Spyware, Adware, etc.

Computer virus:- Computer virus is a kind of malicious software or malware that can be multiple and transmitted from one computer to another. It is a common misconception that virus includes all kind of malware. When virus is spread out on the internet, it is transmitted other computer. It cannot be spread out without the interference of the user. For example, if a pen drive contains any virus infected file, it cannot be active and spread out as long as it is not connected to other computer.

Computer worm:- being active, automatically spreads out from network to network and attacks the computers.

Trojan horse:-Malware hides its identity under the guise of useful software. When the disguised software becomes active, the Trojan corrupts the file, and import new Trojans. This is the way of working by the Trojan horse.

Adware:- By definition, adware displays advertisements on a computer. Most often, however, people use the word adware to refer to malicious software that shows deceptive ads, flashing pop-up windows, large banners, and full-screen auto-play commercials within their web browser. It is not harmful software.

Rootkit: A Rootkit virus is a stealth type of malware that is designed to hide the existence of certain processes or programs on your computer from regular detection methods.
Spy ware: Spyware notices our movements, which websites we visit, how long we stay, and how we use our devices to it can reveal or use information against us.

Difference between Virus and Worm: -

Virus	Worm
The virus needs human help to execute and spread.	Worms automatically execute and spread.
Virus attaches itself with the host and spread where the host reaches.	Worms don't need a host and exploit the vulnerability of a network to spread.
Viruses destroy, damage, or alter the files in the infected computer.	Worms don't affect the file but increase the resource usage to crash the system or network.
Virus spreading speed is low compared to worms.	Worms spreading speed is fast, and it quickly infects multiple computers or networks.
To clean the infection of virus or stop its infection, the user needs an antivirus.	To remove the worm's infection or prevent the infection, the user needs antivirus and a firewall.

Computer virus and its types: -

A computer virus is one type of malware that inserts its virus code to multiply itself by altering the programs and applications.

The computer gets infected through the replication of malicious code. Computer viruses come in different forms to infect the system in different ways. The example of virus is CIH. CIH virus active on 26 April every year and it formats your hard disk. Now it remains Inactive.

How computer virus damage our system: -Computer virus damage our system in various way. Such as

- Slow computer performance or reducing of speed
- Erratic computer behavior
- Unexplained data loss
- Frequent computer crashes
- Problem of hanging on and
- Rebooting are visible

Types of virus:-

Virus can be divided on its nature of working after being active into two types

1. ***Resident***: - Some viruses after being active take a permanent shelter in the memory. When the users run any program, it infects that one. This virus is called resident virus.
2. ***Non- resident***:Some viruses after being active look for the programs that are vulnerable and after infecting them leave the control on the main program and become inactive. These are called non-resident virus.

How to get rid of Malware: -

- download Anti-virus or Anti Malware
- Antivirus software scans a file, program, or an application and compares a specific set of code with information stored in its database. If it finds code that is identical or similar to a piece of known malware in the database, that code is considered malware and is quarantined or removed.
- Update anti-virus regularly

- Antivirus name: - Norton, Avast, Panda, Kasperski, Microsoft Security Essential etc.

Antivirus: - anti-virus software, also known as anti-malware, is a computer program used to prevent, detect, and remove malware. Antivirus software was originally developed to detect and remove computer viruses

Anti-virus works:-

Antivirus software scans a file, program, or an application and compares a specific set of code with information stored in its database. If it finds code that is identical or similar to a piece of known malware in the database, that code is considered malware and is quarantined or removed.

Antivirus name:- Norton, Avast, Panda, Kasperski, Microsoft Security Essential etc.

Online identity and Its safety: -

Online identity is a social identity that an Internet user establishes in online communities and websites. It can also be considered as an actively constructed presentation of oneself. This identity expresses individual on the social network.

Identity Theft: - If anybody is recognized by his online identity, he becomes trustworthy, if the identity of the user is not recognized, he is regarded suspicious person.

The online identity of a man can be any one of the following or a combined form:

i. ***E-mail address***: An email address is a unique identifier for an email account. It is used to both send and receive email messages over the Internet. Email message requires an address for both the sender and recipient in order to be sent successfully. For example xyz@gmail.com
ii. ***His profile name on social network***: - Social profiles are a description of individuals' social characteristics that identify them

on social media sites such as LinkedIn and Facebook. When create an account, set up a name. This name can be your original name or pseudonyms.

Some techniques are given below to protect the secrecy of password: -the user should be careful about using the social media to protect his identity on the internet. He must be vigilant so that nobody can use his email or Facebook account. The secrecy of password to enter the account should strictly be preserved and it is mandatory.

Some techniques are givenbelow to protect the secrecy of password:-

1. Use long password instead of short one.Favourite sentence can be used if necessary.
2. Both the capital and small letters can be used instead of using either capital or small letters.
3. Use strong password. Create password with word, sentence, number and symbol; For example- Z26a1sal81l@gmail.com
4. There is a scope to verify the strength of password online. Verify the strength of password by using the scope, and if it becomes weak, strengthen it.
5. If you use any system run by many people (as cyber café, Union Information and Service Centre), log out before leaving the place.
6. Use password manager, such as lastpass, keepass, etc.as many users use.
7. Develop the practice of changing password.

Hacking:- Hacking means getting into any computer system or network without the permission of the concerning authority or the users. Those who do this work are called hackers.

The hacker community has divided themselves into different groups:-

i. ***White hat hackers***: - White hat hackers choose to use their powers for good. Also known as “ethical hackers,” white hat hackers can

sometimes be paid employees or contractors working for companies as security specialists that attempt to find security holes via hacking.

ii. ***Black hat hackers***: - Black hat refers to a hacker who breaks into a computer system or network with malicious intent. A black hat hacker may exploit security vulnerabilities for monetary gain; to steal or destroy private data; or to alter, disrupt or shut down websites and networks.

iii. ***Gray hat hackers***: - Gray hat describes a cracker who exploits a security weakness in a computer system or product in order to bring the weakness to the attention of the owners. Unlike a black hat, a gray hat acts without malicious intent. The goal of a gray hat is to improve system and network security.

The reason of hacking: - A hacker hacks other's computers for numerous reasons. Such as-

i. Earn Illegally
ii. Harming a person, organization humiliation
iii. Disturbing security
iv. Steal information or leak information
v. Vulnerability Testing