6.1 Data Security Notes

Objective:

- Explain difference between terms **security**, **privacy** and **integrity** of data.
- Show appreciation of need for both security of data and security of computer system.
- Describe security measures designed to protect computer systems, ranging from stand-alone PC to network. Including user accounts, passwords, authentication techniques such as digital signatures, firewall, antivirus software, anti-spyware, and encryption.
- Show understanding of threats to computer and data security posed by networks and internet. Including **malware** (virus, spyware), hackers, phishing, and pharming.
- Describe methods that can be used to restrict risks posed by threats.
- Describe security methods to protect security of data. Including encryption, access rights.

Definitions of Data Integrity, Privacy and Security

- **Data Integrity** means data is **Accurate** and **Up to date**.
  - ✓ Data integrity refers to accuracy, consistency, and reliability of data.
  - ✓ It ensures that data remains unchanged and retains its intended meaning, preventing errors, corruption, or unauthorized alterations.
- **Data Privacy** means data is available only to **authorized** users.
  - ✓ **Data protection laws** are used to penalize offenders who breach privacy.
  - ✓ Major aspects of data protection laws relate to personal data that individual supplies to organization. Data protection laws oblige organizations to ensure **privacy** and **integrity** of this data.
- **Data Security** means data is **recoverable** if lost or corrupted.
  - ✓ Data can be said to be **'secure'** if it is available for use when needed and data made available is data that was stored originally.
  - ✓ Security of data has been breached if data has been **lost** or **corrupted**.
  - ✓ Data security is a **prerequisite** for ensuring data **integrity** and **data privacy**.

Threats to Security of System

- ✓ Internal mismanagement
- ✓ Natural disasters
- ✓ Unauthorized intrusion into system by an individual.
- ✓ Malicious software entering system.

Security Measures designed to protect Computer System

Data Security refers to methods used to prevent **Unauthorized Access** to data, as well as to **Data recovery** methods if it is lost.

Use of User Accounts

- ✓ User accounts are used to **authenticate** user.

- ✓ User accounts are used on both **standalone** and **networked** computers in case computer can be accessed by a number of people. This is often done by a **screen prompt** asking for a username and password. User accounts control **access rights.**

Use of Passwords Passwords are used to **restrict access** to data or systems. Password should be difficult to **crack** and **changed** frequently to retain **security**. Passwords can also take form of **biometrics**.

Passwords are used when;

- Accessing email accounts
- Carrying out online banking or shopping
- Accessing social networking sites.

Way to Protect Password:

- Run **Anti Spyware** software to make sure your passwords are not being sent to whoever put **spyware** on your computer.
- Regularly change passwords in case they have been seen by someone else, illegally or accidentally.
- Make sure passwords are difficult to **crack** or **guess.**

Digital Signatures

Digital signatures protect data by providing a way of **identifying** the **sender**. If an incoming transmission is an **email**, you might want to check **identity** of **sender**. Solution is to insist that sender attaches **digital signature** to email.

Use of Firewalls

Firewall can be software or hardware. It **sits** between **user's computer** and **external network** and **filters** information in and out of computer. Firewall allows user to decide to allow communication with an **external source** and warns user that an external source is trying to access their computer. Firewalls are primary defence to any computer system to protect from hacking, malware (viruses, spyware), phishing and pharming.

Tasks Carried out by Firewall:

- Examining **traffic** between user's computer and public network.
- Checking whether incoming or outgoing data meets a given **set of criteria**.
- **Logging all** incoming and outgoing traffic to allow later interrogation by network manager.
- Preventing Access to certain **undesirable sites** – the firewall can keep a list of all undesirable **IP addresses**.
- Helping to **prevent viruses** or hackers entering user's computer (or internal network).
- Warning user if some software on their system is trying to access an **external data**

source (such as an automatic software upgrade). User is given option of allowing it to go ahead or request that such access is denied.

Uses of Antivirus

Running **antivirus** software in background on computer will constantly check for virus attacks. Different types of antivirus software work in different ways, they all

- Check **software** or **files** before they are run or loaded on a computer.
- Compare **possible viruses** against a database of known viruses.
- **Quarantine** files or programs which are possibly infected.

Antivirus software needs to be kept **up to date** since new viruses are constantly being discovered. **Full system** checks need to be carried out regularly, since some viruses lie dormant and would only be picked up by this full system scan.

Use of Anti-Spyware

Anti-spyware software **detects** and **removes** spyware programs installed **illegally** on user's computer system. Software is either based on **rules** (it looks for typical features associated with spyware) or based on **known file** structures which can identify common spyware programs.

Encryption

If data on a computer has been **accessed illegally** (by a hacker) it is possible to encrypt data, making it **virtually** impossible to understand without **encryption keys** to decode it. This cannot stop a hacker from deleting files, but it will stop them using data for themselves.

Biometrics

In an attempt to stay one step ahead of hackers and malware, modern computer devices use biometrics as part of password system. Biometrics rely on **unique** characteristics of human beings. **Examples** include **fingerprint scans**, **retina scans** (pattern of blood capillary structure), face recognition and voice recognition.

Threats to Computer and Data

Hacking

It is **illegal access** to computer system without owner's permission.

Types of Hacking

- **Malicious Hacking** is **illegal** access to computer system without user's permission or knowledge. It is usually employed with intention of deleting, altering or corrupting files, or to gain **personal details** such as bank account details. **Strong passwords**, **firewalls** and software which can detect **illegal activity** all guard against hacking.

- **Ethical Hacking** is **authorised** by companies to check their **security measures** and how **robust** their computer systems are to **resist** hacking attacks. It is **legal** and is done with a company's permission with a fee paid to ethical hacker.

Malware

Malware refers to any computer program that is designed to do things that are **harmful** to or unwanted by a computer's legitimate user — meaning you. Malware is one of biggest risks to **integrity** and **security** of data on a computer system. Term malware is short for "**Malicious Software**."

Viruses A virus is a program that **replicates** itself and is designed to **cause harm** to a computer system. Viruses need an **active host** program on target computer or an operating system that has already been infected before they can run.

Worms

A type of stand-alone **virus** that can replicate themselves with intention of spreading to other computers; they often use networks to search out computers with weak security.

Logic Bombs Code embedded in a program on a computer. When certain conditions are met (such as a specific date) they are activated to carry out tasks such as deleting files or sending data to a hacker.

Trojan Horses Malicious programs often disguised as legitimate software. They replace all or part of legitimate software with the intent of carrying out some harm to the user's computer system.

Spyware Software that gathers information by monitoring, for example, key presses on the user's keyboard. The information is then sent back to the person who sent the software – sometimes referred to as key logging software.

Phishing Phishing is act of attempting to acquire **Sensitive Information** like usernames, password and credit card details by representing as a **trustworthy** source. Phishing is carried out through **emails**, as soon as user click on that scam email attachment or link, user is directed to **bogus** website. When user enter his personal information on that website, all information is sent back to creator of that bogus website leading to fraud or identity theft.

Ways to prevent Phishing Attacks:

- Users need to be aware of new **Phishing Scams** by attending security awareness training.
- Do not click on links unless certain that it is safe to do so.
- It is important to run **anti-phishing toolbars** on web browsers since these will alert user to malicious websites contained in an email.

- Look out for **https** or **green padlock** symbol in the address bar.
- Ensure an **Up-to-Date** browser, with all of latest security upgrades, is running, and run a good firewall in the background at all times.

Pharming

Hacker creates **fake** website which appears similar to original website and installed **malicious code** on your hard drive. When user types URL of **original website** in browser. **DNS** server directs user to **fake website** designed by hacker. User not knowing that it is fake website, shares his confidential information such as login, password... etc. Hacker gets user confidential information from his fake website and uses it to access original website. Hacker exploits user's confidential information leading to fraud or identity theft.

Protection against Pharming:

It is possible to mitigate risk of pharming by;

- Using **Antivirus** Software, which can detect unauthorized alterations to a website address and warn the user.
- Using **modern web browsers** that alert users to pharming and phishing attacks.
- Checking the **spelling** of websites
- Checking for https and/or the green padlock symbol in the address bar.

Security Measures for Data Protection

accidental loss of data (for example, accidental deletion of a file)	■ use back-ups in case the data is lost or corrupted through an accidental operation ■ save data on a regular basis ■ use passwords and user IDs to restrict access to authorised users only
hardware fault (such as head crash on the HDD)	■ use back-ups in case data is lost or corrupted through the hardware fault ■ use uninterruptable power supply (USP) in case power loss causes hardware malfunction ■ save data on a regular basis ■ use parallel systems as back-up hardware
software fault (for example, incompatible software installed on the system)	■ use back-ups in case the data is lost or corrupted through the software fault ■ save data on a regular basis in case the software suddenly 'freezes' or 'crashes' while the user is working on it
incorrect computer operation (for example, incorrect shutdown or procedure for removing memory stick)	■ use back-ups in case data is lost or corrupted through wrong operation ■ correct training procedures so users are aware of the correct operation of hardware

****