CHAPTER 6: SECURITY, PRIVACY AND DATA INTEGRITY

6.1 DATA SECURITY

6.1.1 Definitions

Data Security:

- Ensuring data is protected against loss and unauthorized access
- Protection of data on computer system

Data Integrity:

- Ensuring data is valid and does not corrupt after transmission
- Data is accurate and reliable

Data Privacy:

- Ability to determine what data is shared with third party

6.1.2 Threats to Computer and Data Security

Malware:

- Software designed to damage computer or network
- **Virus:** Replicates by inserting copy into other software; can crash computer, delete/corrupt data
- **Spyware:** Gathers information about users' activity; monitors online/offline behaviour

Hacking:

- Illegal access to computer system
- Obtain confidential data
- Can cause identity theft

- Can delete/corrupt data

Phishing:

- Emails attempting to obtain confidential data
- Impersonates legitimate organizations
- Causes identity theft

Pharming:

- Redirects users to fake websites
- Appears legitimate
- Gains confidential data

6.1.3 Security Measures

User Accounts and Passwords:

- Deny unauthorized access
- User-assigned privilege levels
- File access permissions

Firewalls:

- Filters information between computer and internet
- Detects illegal connection attempts
- Blocks unauthorized access

Authentication:

- Determines if someone is who they claim
- Methods: passwords, digital signatures, biometric scans

Anti-virus Software:

- Detects and removes viruses
- Checks files for malicious patterns
- Runs in background

Anti-spyware Software:

- Detects and removes spyware

Encryption:

- Converts data to code
- Doesn't stop access but makes data meaningless
- Requires decryption to read

Data Backup:

- Exact copy of original data
- Stored at different location
- Disk-mirroring: writes to multiple disks simultaneously

6.1.4 Data Security vs System Security

Data Security	System Security
Protection of data on system	Protection of computer system
Prevents corruption, unauthorized use	Prevents viruses, hacking
Example: encryption	Example: firewall, passwords

6.2 DATA INTEGRITY

6.2.1 Data Validation

Definition: Checks if data entered is valid (sensible).

Methods:

Method	Description
Range Check	Data must be between set values
Format Check	Data must follow correct pattern
Length Check	Data must have exact number of characters

Method	Description
Presence Check	Checks if data has been entered
Existence Check	Data entered must exist in database
Limit Check	Value within acceptable min/max
Check Digit	Arithmetic result of other digits; verifies accuracy

6.2.2 Data Verification

Definition: Checks data entered is accurate (correct).

Data Entry Verification:

Method	Description
Visual Check	Person manually compares original with entered data
Double Entry	Enter data twice; compares results

Data Transfer Verification:

Parity Check:

- Number of 1s in byte must be odd or even
- If parity doesn't match, error detected
- Limitation: Cannot detect 2-bit transposition

Checksum Check:

- Data sent as block of bytes
- All bytes added together
- Checksum calculated before and after transmission
- If different, error occurred; block must be resent

Revision #1
Created 2026-03-16 12:02:09 UTC by Samuel Lee
Updated 2026-03-16 12:02:22 UTC by Samuel Lee