# Unit 1.4: Security

## 1.4.1 THREATS TO ONLINE DATA

Phishing: one that tricks you into handing over sensitive or personal information (login details, bank details, etc.)

- -You receive what looks like a legitimate email and it then urges you to visit a website and enter your personal details
- -What to look out for:
  - -greeting
  - -the sender's address – often a variation on a genuine address
  - -forged link – links look genuine but may not link to the website given
  - -request for personal information
  - -sense of urgency
  - -poor spelling and grammar
- -Protecting yourself: use a SPAM filter & don't click any links or download attachments

Pharming: malicious code is installed on a personal computer or server, misdirecting users to fraudulent websites without their knowledge or consent

- -internet service providers to filter & check for https & spelling of URL

Trojan Horse email: offers you an attachment or link and installs a virus once clicked

Virus-generated email: appears to be sent from a friend and encourages you to click a link to a sales website or transfer cash

DoS attack: attempts to make a website or network unavailable to legitimate users

- -Motive is often revenge, blackmail or terrorism

## 1.4.2 KEEPING DATA SAFE

Threats to data:

- -Accidental damage
- -Natural disaster
- -Malicious actions

Backups: made regularly so that data lost or corrupted can be restored

- -Should be stored in a secure location offsite
- -Holding the company's data in the Cloud

Archived data: data that is no longer needed for immediate processing but needs to be kept

Accidental damage:

- -Data entry errors can result in erroneous data being held, or data being accidentally deleted
- -Program errors may mean that a program crashes in the middle of an operation and data is lost
- -Errors in procedure

Accidental loss:
- -Loss of a portable device
- -Accidental deletion

Hardware failure:
- -Hard disk crash
- -Damage to a storage device

Physical security: data needs to be kept physically secure from intruders
- –Locks on doors
- –Security guards
- –Biometric security
  - –fingerprint recognition
  - –voice recognition
  - –iris recognition

Acceptable use policy: policy that needs to be signed before given a network ID

Passwords:
- -Changed regularly
- -Use a variety of symbols and characters
- -Mixture of upper case and lower case
- -Length of 18-20 characters

---

## 1.4.3 ONLINE SYSTEM SECURITY

Intercepting data: data that is transmitted over a network can be intercepted

Encryption: the encoding of data so that it can no longer be easily understood
- –the original message to be encrypted
- –the encrypted message
- –the process of converting plaintext into ciphertext
- –a sequence of numbers used to encrypt or decrypt, often data using a mathematical formula
- –the formula for encrypting the plaintext
  - –two inputs: plaintext and a secret key

Symmetric encryption: same key used to encrypt and decrypt a message

Asymmetric encryption: two keys – a public key known to everyone for encrypting and a private key for decrypting
- omore secure as you never have to send or reveal your decryption key

Cryptanalysis: objective is to decode the ciphertext
- -Brute-force attack
  - -every possible key is tried
- -Non-brute-force attack (cryptanalytic attack)

Key strength: the more bits in the key size, the more the strength of the encryption increases

Modern ciphers: created using two very large prime numbers multiplied together

- Larger the prime number, the more difficult it is to find the two numbers needed to break the code

Algorithmic security: ciphers are based on computational security

How to protect data:

- Passwords
- Firewall: software that checks data coming from the internet or a network
  - blocks/allows data to pass through
  - acts as a filter or barrier between your own trusted network and another
  - only data packets that meet set filtering rules are allowed to pass through
- Security protocols:
  - SSL: protocol for transmitting private documents via the internet
  - TLS: upgrade to SSL and uses more bits
  - Uses asymmetric encryption to encrypt data before transmission

Proxy server: a computer that acts as an intermediary between a web browser and the internet

- Helps to improve web performance by storing a copy of frequently used web pages
- May act as a firewall
  - filters out some web content and malware
  - blocks/allows data packets through
- a gateway from one network to another