Preventing Misuse of Data

Unit R012 - Understanding tools, techniques, methods and processes for technological solutions

Introduction

- When data and information is stored it needs to be protected to keep it safe.
- There are different ways in which systems can be protected to prevent the misuse of data.
- These can be categorised as:
  - Physical Methods
  - Logical Methods
  - Secure Destruction Of Data

Physical Methods

- There are many physical protection measures that can be taken.
- The choice of measure will depend on the device being protected.
- One of the main physical methods is Biometric Access Devices.

Biometric Protection Measures

- A biometric protection measure uses a physical characteristic of the user such as:
  - A Fingerprint
  - Voice Recognition
  - Palm Veins
  - Palm Print
  - Geometry Of The Hand
  - Iris Recognition
  - Retina Recognition
  - DNA
  - Signatures
  - Handwriting

Biometric Protection Measures

- It is common for personal devices to need a biometric measure to be positive before the device can be accessed.
- The owner of the device will have stored their characteristic as part of the security settings on the device.
- Only people whose characteristic is stored and recognised can access the device.
- Large businesses can use biometric protection measures to protect entry to rooms.

Biometric Protection Measures

Advantages of biometric systems:	Disadvantages of biometric systems:
Improved security	Environment and usage can affect measurements
Improved customer experience	Systems are not 100% accurate.
Cannot be forgotten or lost	Require integration and/or additional hardware
Reduced operational costs	Cannot be reset once compromised

TECH 15/12/2017 03:55 GMT | Updated 15/12/2017 15:49 GMT

167

Woman In China Says Colleague's Face Was Able To Unlock Her iPhone X

It could also be cheeky passcode training, an Apple spokesman says.

By Mary Papenfuss, HuffPost US

Other Physical Methods

- The following are other physical methods that prevent the misuse of data:
  - **Locking doors** when rooms containing equipment are not in use
  - Using **swipe** or RFID **cards** or **keypads** to activate locks
  - **Bolting** computer equipment to desks
  - Using **special pens** to mark the **postcode** on computer equipment
  - Using **CCTV** cameras
  - **Closing windows** and blinds when rooms are not in use

Logical Methods

- There are many logical protection measures that can be taken to prevent the misuse of data.
- The choice of measure will depend on the data and information being protected.
- Some logical methods are:
  - **Access Rights And Permissions**
  - **Authentication**
  - **Usernames and Passwords**
  - **Anti-virus Software**
  - **Encryption**
  - **Secure Backups Of Data**
  - **Secure Destruction of Data**

Access Rights And Permissions

- **Files** and **folders** containing data can have **access rights** and **permissions**
- These can be **adjusted** to control who can **read**, **edit** or **alter** and **save** the file.
- The **usernames** can be used to **set access rights** and permissions for each person.

Authentication

- Some access systems use **two-step authentication** as another layer of protection.
- The most common authentication protection is by using a **token code**.
- When a user tries to access a secure area, the username and password is entered.
- When these are submitted and checked, the system creates a **token code**, which is sent to the **email address** linked to the **username** and **password**.
- To access the secure area, the user must **input** the **token code**.

Usernames and Passwords

- The username acts as authorisation while the password acts as authentication. Without both parts being correct, access will be denied.
  - **Username = Unique identifier for a user**
  - **Password = Method of restricting access. Without the correct password, access is denied.**

- **Individual documents** can also have **passwords** set on them so **only authorised** people can **see** the document.

- **Restrictions** can be placed on part of a document too
  - **Locking** the **cells** on a **spreadsheet** so it can not be changed.

Anti-Virus Software

- **Anti-virus software** is used to **detect** any **viruses** and to **remove** them to limit their damage to the computer system.
- The software tries to **detect** the **virus before** it **enters** the **computer** system.
- If a virus is **detected** then the **software** will either **automatically quarantine** it or will **send** an **alert** to the user asking what action should be taken.
- It is important **anti-virus software** is **kept up to date** as **new viruses** are being created and distributed all the time.

Anti-Virus Software

- **Anti-virus** scans can also be **carried** out by the **software**.
- These can be **automatically ran** at a selected time and day.
- These scans will **search** for any **viruses** that may be on the computer system and that have not been detected by the anti-virus software.

Secure Backup

- A secure **backup** of data is a **copy** of **data** or files that are **currently** in **use**.
- **Backups** are made **regularly** and **stored away** from the computer system.
- **Depending** on what the **files** contain **depends how often** businesses **backup** data.
- **Banks** for example will back up **every few minutes** because their **data** is so **important**, retailers may backup once a day.

Secure Backup

- Businesses such as **supermarkets** have **huge amounts** of **data**, meaning that DVDs or USBs aren't big enough so they will **use tape drives** or **extra hard disks** to store data.

- **Backups** are **kept** in a **secure** place so they **can't** be **stolen** and are also **encrypted** so that if they were **stolen** they would be **inaccessible without** the encryption **key**.

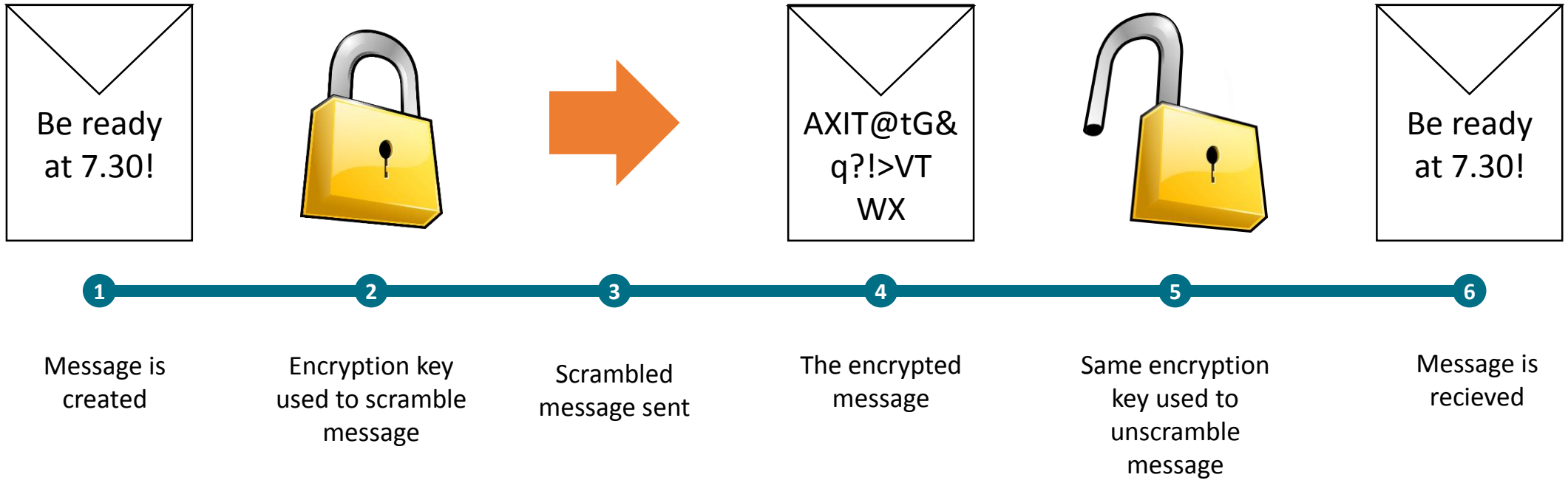
- Many companies use the **cloud** as **online storage** so **backups** are **stored** on **servers managed** by external **companies** which **charge businesses** to back up the data.

- The **cost** of this can be **lower** than paying for your own **staff** to run back-up systems.

Encryption

- **Encryption** helps to **prevent data** being used by **unauthorised** people.
- Encryption software **scrambles data** when it is stored or **transmitted** between computers **over networks**.
- Encryption software uses an **encryption** code or **key** to **scramble** the contents of data files.
- The correct **code** is **needed** to **unscramble** to message at the other end.
- If the file is accessed by anyone else without the proper code to unscramble it, the data will be meaningless.

Encryption


Be ready at 7.30!
AXIT@tG& q?!>VT WX
Be ready at 7.30!
1
2
3
4
5
6
Message is created
Encryption key used to scramble message
Scrambled message sent
The encrypted message
Same encryption key used to unscramble message
Message is recieved

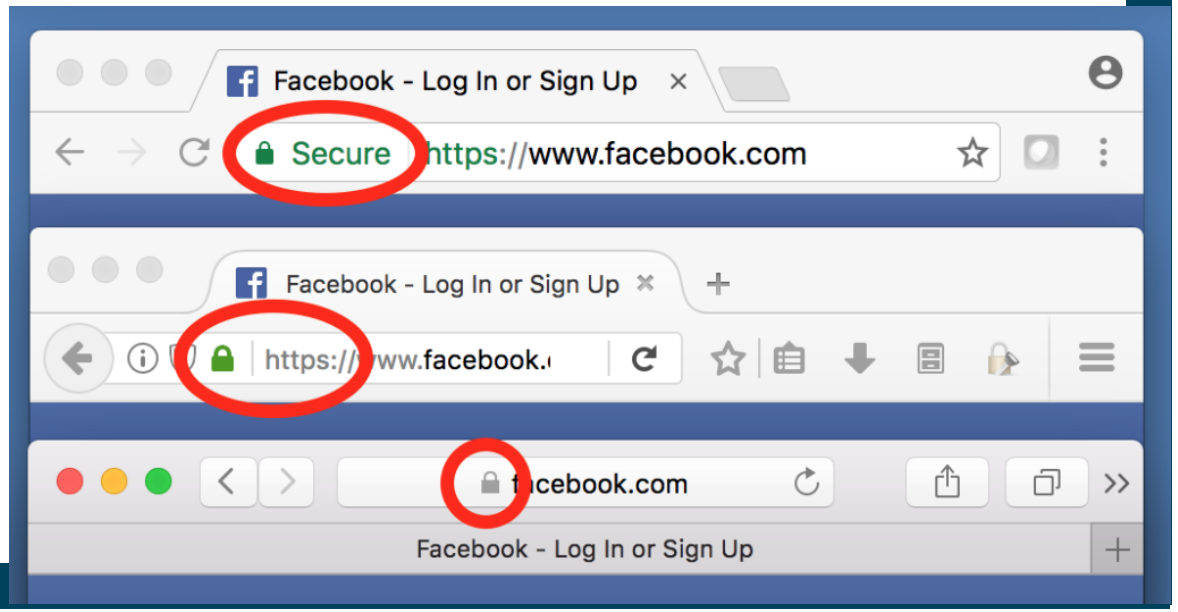
Encryption

- Digital **signatures** are an **example** of **encryption** and are used to check that a **website** or message is **authentic**.

- The data held by businesses about their customers and their financial details are encrypted when stored, so that if stole, the details can not be used.

Encryption

- When customers buy items online or when they **enter personal details** into any website, the data **should** be **encrypted** before being transmitted.
- This will keep the details from being read or used by others even if they are intercepted.
- A secure website using encryption will use https instead of http in the URL and will show a small padlock symbol.
- Different web browsers will show the use of https in different ways.



Secure Destruction of Data

- When **data** is **no longer required**, it **should** be **securely destroyed** to make sure that no data falls into the wrong hands.

- **Even** if the **data** is **deleted** using the **operating systems** software, it can still be **located** and used from the **physical device**, for example a laptop's hard drive.

- The way in which data can be securely destroyed will depend on what data is to be destroyed and the storage device. These ways are:
  - **Overwriting data**
  - **Magnetic wipe**
  - **Physical destruction**

Overwriting Data

- The data to be **securely destroyed** is **written over** with random meaningless data.
- This meaningless data is usually **binary**, consisting of 1's and 0's.
- **Meaningless data** is **written** to **all areas** of the storage device.
- This method is **usually used** with the **physical storage** devices.
- When the data has been **overwritten** the **storage device** can be **reused**.

Magnetic Wipe

- This means that the **magnetic field** part of a storage device is **removed**.
- This makes all the **data stored** on the storage **device unusable**.
- This is because the **wipe** also **removes** all the basic **commands** stored on the storage device that **make** the storage **device operate**.

Physical Destruction

- The most secure way to securely delete data is through the **physical destruction** of a **storage device**.
- This may mean that it is so thoroughly destroyed that the **data cannot** be **recovered**.
- Examples of physical destruction is the use of a **hard drive shredder**, similar to a paper shredder or to use a drill or hammer through the hard drive.
- It is also important that paper-based forms that contain personal or confidential data are securely destroyed.