

Chapter Eight $\Rightarrow$ Safety & Security

Objectives:-



★ Physical safety issues

E-safety issues:-

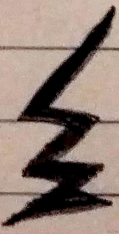
- data protection acts
- personal & sensitive data
- e-safety when using the internet

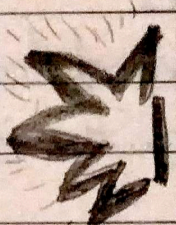
★ Data security:-

- threats to data
- protection of data

Physical Safety:-

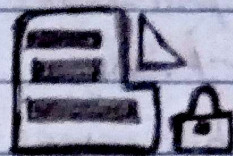
Is concerned with the dangers that could lead to serious injuries or even loss of life

Safety risk	Cause of safety risk	Prevention measures
Electrocution 	• Spilling liquids / drinks	• Don't allow drinks
	• Exposed wires	• Check all wires on a regular basis
	• Unsafe electrical equipment	• Check all equipment on a regular basis
	• Unsafe electricals in the office	• Make use of RCB to prevent electrocution

Safety risk	Cause of safety risk	Prevention measures
Fire hazard 	• Overloaded wall sockets • Overheating of computer equipment- • Exposed wires causing a short-circuit-	• Increase the number of sockets. • Don't cover the cooling vents of computers • Make sure all equipment is fully tested • Ensure there is good room ventilation • Use low-voltage equipment • Have fire extinguishers
Tripping hazard 	• Trailing wires on the floor • Damaged carpets & other flooring	• Use cable ducts • Cover exposed wires and hide wires. • Use wireless connectivity wherever possible.
Personal injury 	• Heavy equipment- unstable or falling from desks • Desks collapsing under weight- /desks	• Use strong enough desks. • Use large desks and tables.

E-Safety: the benefits, risks and responsibilities when using ICT.

Data protection $\Rightarrow$ This is legislation designed to protect individuals and to prevent incorrect or inaccurate data being stored.



Principles of data protection acts:

- Data must be fairly & lawfully processed.
- Data can only be processed for the stated purpose.
- Data must be adequate, relevant and not excessive.
- Data must be accurate.
- Data must not be kept longer than necessary.
- Data must be processed in accordance with the data subject's rights.
- Data must be kept secure.
- Data must not be transferred to another country unless they have adequate protection.

General guidelines to stop data being obtained unlawfully:

- Don't leave personal information lying around on a desk.
- Lock filing cabinets at the end of the day.
- Don't leave data on a computer monitor if it is unattended - log off.
- Use passwords & IDs - passwords difficult to guess.
- Make sure anything sent in an email or fax is not of a sensitive nature.

Using the internet $\Rightarrow$

precautions taken to minimize the danger when using the internet-

- make sure the websites being used can be trusted.
- Only purchase items from websites that offer secure connections.
- Search engines are set to 'safe search' & highest level of security.
- use websites recommended by teachers / parents.
- Be careful what you download.
- Always log out of sites when you have finished using them

Sending & receiving emails $\Rightarrow$

It is important to have an awareness when opening emails

- Open emails or attachments from known sources.
- Make sure the ISP has an effective filtering features.
- Only reply to an email if you know the person who sent it.
- Check that email addresses or website addresses pertaining to come from a genuine company
- Never include your personal data in emails.
- Never send photos of yourself.
- Beware of phishing & pharming.
- Protect your email account by using passwords
- Take care when forwarding emails.
- Manually type in email addresses
- Avoid clicking on hyperlinks within emails
- Avoid using CC or To boxes when sending multiple emails

Social media ⇒

The following list shows some of the ways to protect yourself

- Don't post or give out personal information to people you don't know.
- Don't send out photos of yourself to people you don't know.
- Use privacy settings when posting photos of yourself on social media sites.
- None of the photos you post can link you to place or another address.
- Don't post photos in some form of school uniform.
- Maintain privacy settings to stop 'non-friends' from contacting you & access your profile.
- Make friends with very well-known people to other friends.
- Avoid using or forwarding messages containing inappropriate language.
- Be very vigilant when using social sites / chat rooms:
 - Block / report anybody using inappropriate language
 - Don't enter private chat rooms
 - Never arrange to meet anyone on your own
 - Avoid the misuse of images
 - Always respect people's confidentiality
 - Be careful with the language used

~

Online Gaming $\Rightarrow$

Some of the risks associated with online gaming:

- Predators
- Cyberbullying
- use of webcams
- voice - masking technology
- Online games are also a source of cyber attacks on a user's computer or mobile phone
- Violence in the game itself.

{ Main principles of data protection acts }

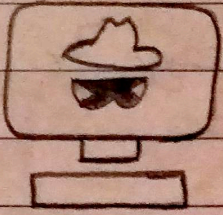
- Data must be fairly & lawfully processed.
- Data can only be processed for the stated purpose.
- Data must be adequate, relevant & not excessive.
- Data must be accurate.
- Data must not be kept longer than necessary.
- Data must be processed with the data subject's rights.
- Data must be kept secure.
- Data must not be transferred to another country, unless they have adequate protection.

{ Guidelines about how to stop data being obtained unlawfully }

- Don't leave personal info lying around on a desk.
- Lock filing cabinets at the end of the day or when you leave.
- Log off from the computer if away from your desk.
- Use passwords and IDs which should be kept secure.
- Make sure that anything sent by email or fax is not sensitive data.

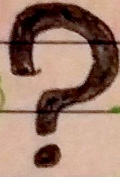
Security of Data

Hacking $\Rightarrow$ the act of gaining unauthorized access to a computer system



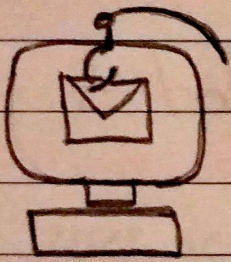
- can lead to identity theft or misuse of personal information.
- data can be deleted, changed or corrupted

What to do?



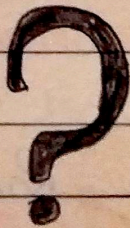
- use firewalls
- strong passwords & IDs
- anti-hacking software
- use users IDs & passwords.

Phishing $\Rightarrow$ sending out legitimate-looking emails to users contain links or attachments. By clicking on them it will take us to a fake website or ask about personal information



- can gain personal data such as bank account
- can lead to fraud or identity theft.

What to do?



- ISPs or web browser filter out-phishing emails.

- User should be cautious when opening emails & attachments.

- Don't click on executable attachments that end in .exe .com .php

Smishing $\Rightarrow$ SMS phishing uses the SMS system of mobile phones to send fake text messages, often contain a URL or telephone number.

Vishing $\Rightarrow$ voice phishing uses voicemail message to trick the user into calling the telephone number.

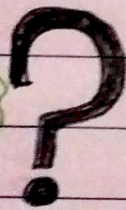
~

Pharming $\Rightarrow$ malicious code installed on a user's computer or on a web server, the code will redirect the user to a fake website



- can gain personal data when they visit fake website.
- can lead to fraud or identity theft

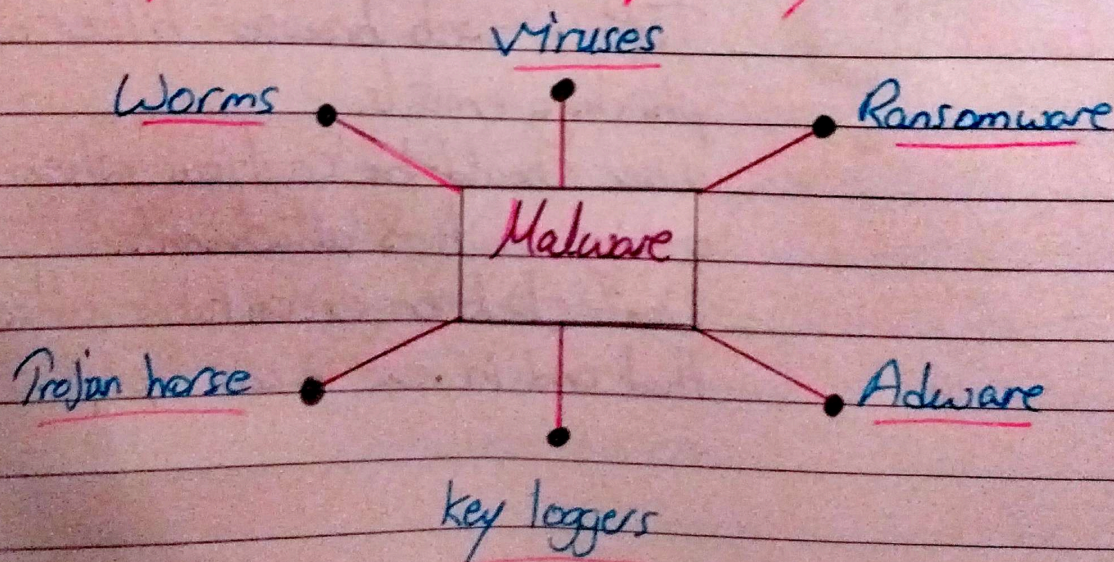
What to do?



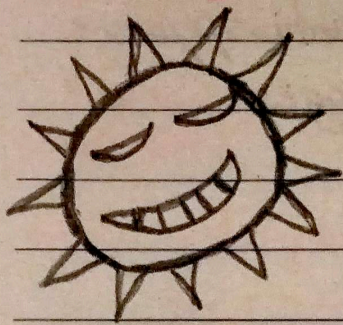
- use anti-spyware
- user should always be alert & look out for clues.

~

Malware $\Rightarrow$ one of the biggest risks to the integrity and security of data on a computer system

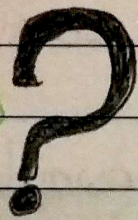


Virus $\Rightarrow$ program code or software that replicates itself written by a human and could cause delete / corrupting files.

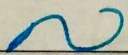


- can cause the computer to crash, stop functioning
- the software can delete files or data
- the software can corrupt operating system files

What to do

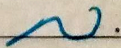


- Install anti-virus and update it regularly
- don't use software from unknown sources
- Be careful when opening emails or attachments



Worm $\Rightarrow$ stand-alone virus can replicate itself with the intention of spreading to other computers

- uses networks to search out computers with weak security
- arrive as message attachments
- when one user opens a worm-infested email, the whole network will be infected.



Trojan horse $\Rightarrow$ malicious programs often disguised as legitimate software, they replace all or part of the software

- need to be executed by the end-user
- arrives by email attachment or downloaded from website.
- Spyware and ransomware are often installed via Trojan horse malware



Key logging software (Spyware) $\Rightarrow$ software that gather information by monitoring all the activity on user's computer

- monitor the key presses
- key loggers can be detected and removed by anti-spyware
- some key loggers work by capturing screen images (screen recorders)

Adware $\Rightarrow$ software that floods a user's computer with unwanted advertising usually in the form of pop-ups

- adware can highlight weaknesses in a user's security defences
- can be hard to remove
- can hijack a browser and create its own default search requests

Ransomware $\Rightarrow$ program that encrypts the data on a user's computer and a decryption key is sent back to the user once they pay a sum of money

- These programs are often sent via trojan horse or by social engineering.
- Ransomware either encrypts files straight-away or it waits for a while to determine how much of a ransom the victim can afford

Card fraud → is the illegal use of a credit or debit card. This can be due to:-

- Shoulder surfing
- Card Cloning
- Key logging software

1	2	3	Cancel
4	5	6	Clear
7	8	9	Enter

Shoulder surfing is a form of data theft by stealing personal info from a victim when they are using cash machine examples:-

- somebody watching you key in data such as PIN
- somebody listening when you are giving details over the phone
- use of tiny digital cameras placed near the keyboard on the ATM

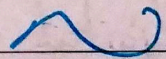
Ways to overcome this risk

- when using ATMs shield the keyboard with your other hand.
- when using a mobile device never key in data in a public place or speak card details
- If you are using a public place make sure you are near security cameras which could record passwords or other data

Card cloning is the copying of a credit or debit card which uses a magnetic stripe using electronic device known as a Skimmer

↳ This is a data capture device that allows a criminal to record all data stored on the magnetic stripe on a card then copied to the magnetic stripe of a false card

Note ⇒ Smart cards contain microchip give more security
But there are other type of devices used to read these smart cards are known as Shimmer



Protection of data

Biometrics $\Rightarrow$ relies on certain unique characteristics of human beings examples.

- Fingerprint scans
- Signature recognition
- Retina scans
- Iris recognition
- Face recognition
- Voice recognition

Biometrics is used in a number of applications as a security device

Very Important

Technique	Advantages	Disadvantages
Fingerprint Scans	• very high accuracy • very easy to use • small storage requirements for data. • one of the most developed techniques.	• for some people it is intrusive because related to criminal identification • make mistake if skin is dirty or damaged.
Signature recognition	• non-intrusive • requires little time to verify. • low-cost technology.	• There may be problems with signature verification • high error rate
Retina Scans	• very high accuracy • no known way to replicate a person's retina pattern	• very intrusive • can be relatively slow to verify retina scans. • very expensive to setup & install.

Technique	Advantages	Disadvantages
Iris Recognition	• very high accuracy • verification time is less than five seconds.	• very intrusive • uses a lot of memory for storing data. • very expensive to setup & install.
Face Recognition	• non-intrusive method • inexpensive method	• affected by changes in lighting, hair, age ---
Voice Recognition	• non-intrusive • verification time is less than five seconds • inexpensive technology	• person's voice can be easily recorded • low accuracy • Illness can change a person's voice.

Digital Certificates $\Rightarrow$ is a pair of files stored on a user's computer, used to ensure security of data sent over the internet. each pair of files is divided into:-

- public key - can be accessed by anyone
- private key - known to the computer user only

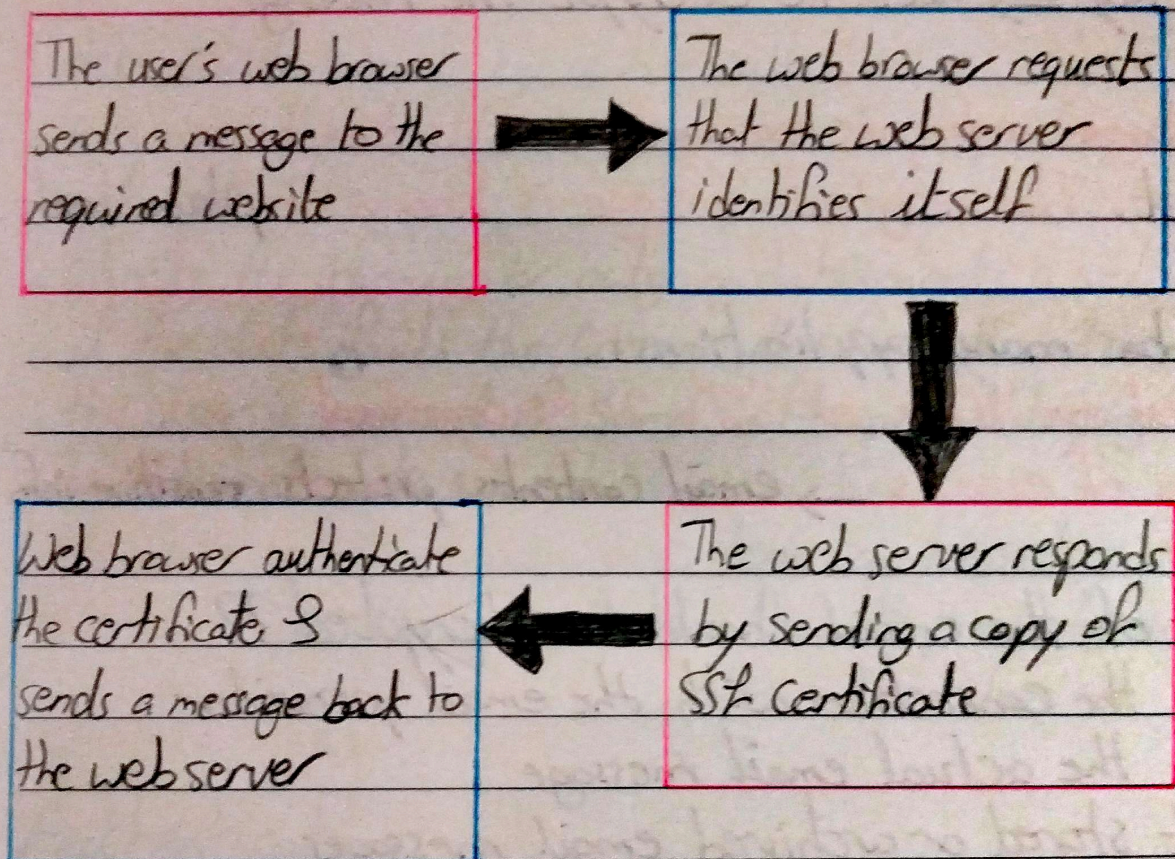
The digital certificate is made up of six parts:-

- The sender's email
- The name of the digital certificate owner
- serial number
- expiry date
- public key
- digital signature of certificate authority

Secure sockets Layer SSL:-

is a type of protocol that allows data to be sent & received securely over the internet.

user will know if SSL is being applied when they see https or small pad lock



Examples of where SSL would be used:-

- online banking
- online shopping
- sending & receiving emails
- using cloud storage
- social networking site.

~

Encryption:

- used to protect data in case it has been hacked
- will not prevent hacking but makes the data meaningless

Encryption key $\Rightarrow$ used to encrypt the message

Decryption key $\Rightarrow$ used to decrypt the message

When a message undergoes encryption it is known as Cypher script. The original message is known as plain text

Encryption has many applications:-

- data stored on HDDs or SSDs is encrypted
- encryption of emails $\rightarrow$ email contents protects sensitive info

Which part of the email should be encrypted??

- $\rightarrow$ Encrypt the connection with the email provider
- $\rightarrow$ Encrypt the actual email message
- $\rightarrow$ Encrypt stored or archived email messages

Note Encrypting only sensitive data is bad practice



This indicates to a hacker which emails they should target

~

Firewalls

can be software or hardware (known as gateway). It sits between the user's computer & an external network help to keep potentially destructive forces away from a user's computer & help prevent viruses or hackers entering the user's computer.

{ Tasks carried out by a firewall: }

- examine the traffic between user's computer and a public network.
- checks the incoming or outgoing data meets a set of criteria.
- if the data fails the criteria, the firewall will block the traffic.
- the user is warned if some software is trying to access an external data source.

* criteria can be set so that the firewall prevents access to undesirable sites. *

~.

Authentication

the ability of a user to prove who they are. Three common factors used in authentication:-

- something you know - password or pin -
- something you have - mobile phone or tablet -
- something which is unique to you - biometrics -

Two-factor authentication → form of verification which requires two methods of authentication to verify who a user is.

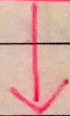
It is used when a user makes an online purchase using credit / debit card.

~
User IDs & passwords

Passwords are used to restrict access to data or systems. They should be hard to break.

Some ways to protect the passwords :-

- Run anti-spyware
- Change passwords on regular basis
- Passwords shouldn't be easy to break
- Make a password strong but also easy to remember



- at least one capital letter
- at least one numerical value
- at least one special character such as @

~