

## What is a hacker?

- A hacker is a person who gets access to a computer system without permission
- They can use this access to:
  - make the computer run different programs such as a virus or a botnet
  - steal information
  - damage files by corrupting or deleting them
- A hacker who misuses computers is known as a 'black hat' hacker



## Reasons for attacking systems

- Fun/challenge
  - Hacking systems can be fun or a challenge
  - There is a sense of achievement
  - Friends may give respect of hacking achievements
- Financial gain
  - Ransoms can be made to prevent attacks from happening
  - Ransomware can be used to encrypt a computer until you pay
- Disruption
  - Attacks such as Denial-of-Service stop websites working
  - Viruses can slow down computers and delete files

## Reasons for attacking systems

- Industrial espionage – spying in companies
  - The aim is to find intellectual property such as designs or blueprints for products, business strategies or software source code
- Personal attack
  - Employees that are unhappy may attack the company
  - Friends / family may attack each other if upset over something
- Information / Data theft
  - Credit card and financial details are stolen to gain money
  - Company information may also be stolen

## Malware

- Malware comes from two words:
  - **Malicious** – to cause an act of harm
  - **Software**
- Malware are executable programs that run on a computer
- One type of malware that exists is a computer virus

## Malware - Viruses and worms

- Computer viruses infect computers
  - They replicate their code in other programs
  - They infect other computers
  - They harm the computer by deleting, corrupting or modifying files
- A worm replicates itself in order to spread to other computers
  - They might cause no damage to the attacked computers
  - They slow down networks and computers



## Malware - Trojan horses

- During the Trojan War there is a story that the Greeks made a wooden horse and hid men inside
  - The Trojans brought the horse into the city, allowing the Greeks to open the city gates letting the army in to destroy Troy
- Computer Trojans are similar:
  - They have a program, game or cracked file which is something the user wants
  - They have negative program code which causes damage, takes control, or provides access to the computer



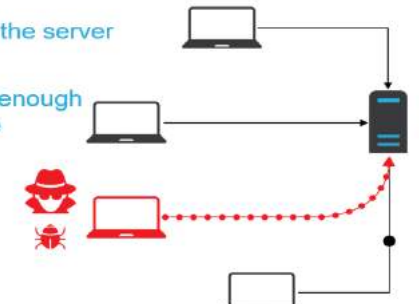
## Malware - ransomware

- Ransomware is software which:
  - Holds a computer hostage by locking or encrypting access to it
  - If the data is encrypted, not even a cyber security professional will be able to recover the data unless backups are available
  - Once a ransom is paid to the attacker, access is restored



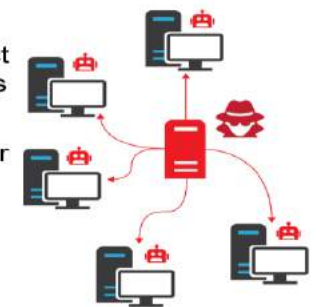
## Denial of Service (DoS)

- In a denial of service attack, a hacker will use or infect a computer so that:
  - it sends as many requests to the server as it can (known as a flood)
  - the server can't respond fast enough so slows down or goes offline
- In a distributed denial of service attack (DDoS), many computers are used to send the requests



## Botnet

- Botnet comes from robot network
- In a botnet, a hacker will first infect machines to make zombie devices
- These computers can then be controlled by one central computer
- This gives a hacker free and anonymous access to computers
- Common uses for botnets are:
  - Denial of service attacks
  - Sending spam



## Social engineering

- Social engineering is the ability to obtain confidential information by asking people for it



## Biometrics

- Every person is unique. You can be uniquely identified by some body parts
- Many smartphones and businesses already make use of biometric data such as:
  - Iris scanners
  - Fingerprint scanners
  - Facial recognition



## Firewalls

- Separate a trusted network from an untrusted network (normally the Internet)
- Data is sent around a network in small packets of information
- These packets are checked to see where they are coming from and going to
  - Packets that don't match filtering rules are dropped
  - This is known as a packet filter
- Firewalls can be run on dedicated hardware or as software

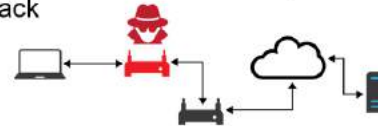
## Shoulder surfing

- Shoulder surfing is the ability to get information or passwords by observing as someone types them in
- The following are two examples:
  - Looking over someone's shoulder
  - Using a CCTV camera



## Man-in-the-middle attack

- A man-in-the-middle attack (MITM) allows the attacker to intercept communications between the user and server. The attacker can then:
  - eavesdrop to find passwords and personal information
  - add different information to a web page or other communication such as email
- Connecting to unencrypted Wi-Fi makes it easy to perform a MITM attack



## Ethical hacking

- A team of cyber security professionals will be employed to try and break into a company's systems
  - Penetration testing will be used to discover weaknesses
- Penetration teams are often employed by industries that deal with large amounts of money or highly valuable intellectual property. They are often used in:
  - Financial companies and banks
  - Pharmaceuticals
  - Military and intelligence services

## Phishing

- Phishing is a type of social engineering technique
- Emails, texts or phone calls are sent to users commonly pretending to be from a bank or website
  - The 'From' email address may be forged
- These messages will try to get personal information such as:
  - Usernames
  - Passwords
  - Credit cards details
  - Other personal information



## Pharming

- Pharming is a way of redirecting a legitimate websites' visitors to a fake website run by a hacker
  - The hacker can then use this site to discover usernames and passwords or other personal information
- A Domain Name System (DNS) server is what translates a web address into an IP address
  - The hacker changes the entry to point to their server instead



## Making good passwords

- Increase password length
- Use characters other than lowercase ones such as:
  - Uppercase
  - Numbers
  - Symbols such as #("\$%)
- Use truly random passwords: X^&Q32/4Lz
- Never write down a password
- Never share a password with anyone
- Change default passwords

## Anti-virus software & Encryption

- Anti-virus software will detect malware such as viruses, worms, trojans, and spyware
  - When a virus is detected it is sent to the anti-virus company
  - They verify it is malware then create a signature of the virus
  - They then add it to their virus database and tell computers to run an update
- Viruses can morph to avoid detection. This makes it harder to create a signature
- Encryption is used to keep data secret and only possible to read by people or computers who have the key or password required to view it
- Encryption encodes the data so that it can only be read with a password
  - Passwords that decode encrypted data are often referred to as keys



## Computer Misuse Act 1990 (CMA1990)

- The computer misuse act is a law. **It must be followed.**
- It ensure that people do not use computers to commit crimes.
- It was first introduced in 1990
- There are 3 rules that make up the CMA 1990
  - A computer can not be accessed without the persons permission
  - Data and files can not be accessed, removed or changed without the persons permission
  - A computer can not be used to commit or intend to commit a crime

## Computer viruses

- A computer virus is very much like a normal virus like a cold or the flu. However, computer viruses are code that have been created to damage a computer or 'make it sick'. This stops the computer being used correctly.
- Computer viruses can damage the data and files on a computer or reduce its security so that people can then hack into them.
- **Viruses can get onto your computer through naughty websites, downloading software, opening email attachments from people you don't know or from an infected storage device.**
- To stop a computer virus, make sure that you have ant virus software on your computer and that it is updated!
- Don't go on or download from naughty websites.

## Grooming

There's a chance that your child may meet people online that aren't who they say they are. Grooming is a word used to describe people befriending children in order to take advantage of them for sexual purposes.

## Cyberbullying

is when someone bullies others using electronic means, this might involve social media and messaging services on the internet, accessed on a mobile phone, tablet or gaming platform.

## Sexting

The term 'sexting' is used to describe the sending and receiving of sexually explicit photos, messages and video clips, by text, email or posting them on social networking sites.

**Radicalisation** – the process by which a person comes to support terrorism and forms of extremism leading to terrorism

**Extremism** – a vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs.

**Terrorism** – an action that endangers or causes serious violence damage or disruption and is intended to influence the Government or to intimidate the public and is made with the intention of advancing a political, religious or ideological cause.

### Spotting the signs of radicalisation

Radicalisation can be really difficult to spot. Signs that may indicate a child is being radicalised include:

- isolating themselves from family and friend
- stalking as if from a scripted speech
- unwillingness or inability to discuss their views
- a sudden disrespectful attitude towards others
- increased levels of anger
- increased secretiveness, especially around internet use

• **Health:** this concerns your own individual physical and mental health when using IT

• **Safety:** This concerns everyone's safety when using IT



# HTML

<code>&lt;u&gt; &lt;/u&gt;</code>	Underlines the text
<code>&lt;head&gt;&lt;/head&gt;</code>	Encloses the head of the HTML document
<code>&lt;body&gt;&lt;/body&gt;</code>	Encloses the body of the HTML document
<code>&lt;p&gt;&lt;/p&gt;</code>	Creates a new paragraph of text
<code>&lt;h1&gt;&lt;/h1&gt;</code>	Formats the text to heading 1
<code>&lt;a href="http://www.google.com"&gt;&lt;/a&gt;</code>	Creates a link to another webpage
<code>&lt;b&gt;&lt;/b&gt;</code>	Makes the text <b>BOLD</b>
<code>&lt;i&gt;&lt;/i&gt;</code>	Makes the text <i>italic</i>

HTML (Hypertext Markup Language)  
HTML is the language for describing web pages.

CSS (Cascading Style Sheets)  
A style sheet is a file that describes how a HTML file should look.

The difference: HTML describes a webpage but CSS describes how it will look.

`< >` = opening tag  
`</>` = closing tag

Image

``

Paragraph (left align)

`<p align="left"> example <br>`

Paragraph (right align)

`<p align="right"> example <br>`

Paragraph (centre align)

`<p align="center"> example <br>`