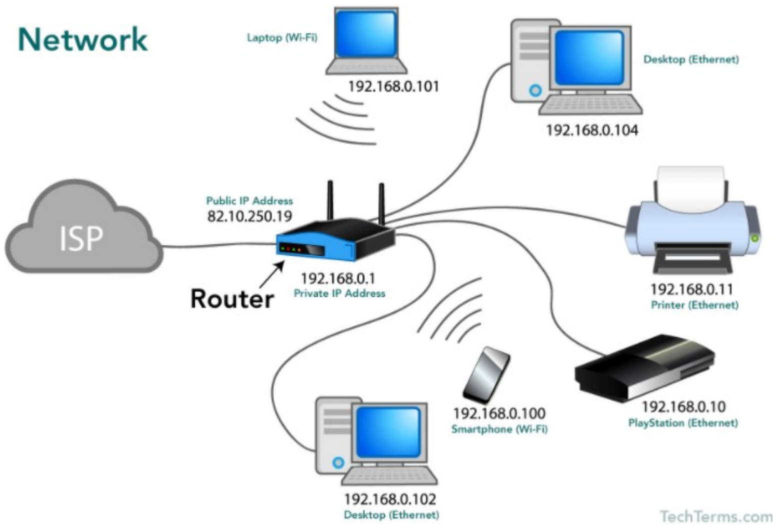
Year 9 E-Safety / Cyber Security Knowledge Organiser

In this topic, you will be taught to understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting your online identity and privacy; recognise inappropriate content, contact and conduct, and know how to report concerns and what to do to prevent network issues.

Lesson Topics
Healthy Relationships
Threats to the network
Emails and Social Engineering
Online privacy
Surveillance
Legislation
Social Media



Forms of Network attack

Networks operate on the principles of communication and sharing. Unfortunately, these principles mean that network **traffic** and **data** risk being accessed by people who have no authority to do so (ie hackers).

A network attack is an attempt to gain access to, steal, modify or delete data on a network. Such attacks take several forms:

Active - where the hacker attempts to modify or delete data, or to prevent a network from operating correctly. An example of this is denial of service (DOS) attacks on the internet, which use many internet enabled computers to force a **web server** offline.

- Eavesdropping (passive) - where the hacker monitors a network in order to gain information. An example of this is wiretapping, where communications are monitored.
- External - where someone outside of an organisation attempts to hack its network.
- Internal - where someone within an organisation attempts to hack its network.

The number of network attacks is growing daily.

Ways to prevent computer security threats

Firewall

Firewalls enforce rules about what data packets will be allowed to enter or leave a network. Firewalls are incorporated into a wide variety of networked devices to filter traffic and lower the security risk from malicious packets traveling over the public internet.

Antivirus

Antivirus software was originally designed to detect and remove viruses from computers, but also protect against other types of malicious software, such as keyloggers, browser hijackers, Trojan horses, worms, rootkits, spyware, adware, botnets and ransomware.

Antispyware

Antispyware software detects and prevents unwanted spyware program installations. Detection may be either rules-based or based on downloaded definition files that identify currently active spyware programs.

Strong passwords

Passwords that are easy to guess are a security risk. Simply making sure employees are using passwords that are sufficient length and a mix of character types can be a huge detractor for hackers.

Poor network policies tend not to have:

- levels of access to prevent users from accessing sensitive data unless they are authorised to do so

rules preventing the connection of external devices such as USB memory sticks which may contain and transmit **viruses**

- regulation regarding secure passwords, for example using a number of letters, numbers and symbols
- rules to govern what websites can and cannot be visited
- methods to prevent any user wirelessly connecting an unsecured laptop, tablet or smartphone
- controls on what facilities can be accessed remotely (away from the organisation)
- a formal backup procedure that is adhered to
- a regular maintenance programme that is followed

A network manager must attempt to prevent and thwart all these types of threat, and remain aware of new threats as they emerge.

Sexting - send (someone) sexually explicit photographs or messages via mobile phone.

Indecent - not conforming with generally accepted standards of behaviour, especially in relation to sexual matters.

Bystander - a person who is present at an event or incident but does not take part

Consent - permission for something to happen or agreement to do something.

Portray - describe (someone or something) in a particular way.

Cyberbullying - the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.

Peer Pressure - influence from members of one's peer group (friends or people of around the same age)

Conform - comply with (or follow) rules, standards, or laws

Victim - a person harmed or injured as a result of a crime, accident, or other event or action

Stereotype - a widely held but fixed and oversimplified image or idea of a particular type of person or thing.

Self Esteem - confidence in one's own worth or abilities; self-respect

Realistic - representing things in a way that is accurate and true to life

Idealised - regard or represent as perfect or better than in reality

Strategies - a plan of action designed to achieve a long-term or overall aim

Homophobia - encompasses a range of negative attitudes and feelings toward homosexuality or people who are identified or perceived as being lesbian, gay,

Advice - guidance or recommendations offered with regard to future action

Firewall—monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules.

Antivirus— a program designed to prevent, search for, detect, and remove software viruses, and other malicious software

Anti Spyware—designed to prevent and detect unwanted spyware program installations and to remove those programs if installed.

Malware—term for any type of malicious software designed to harm or exploit any programmable device or network.

SQL—stands for Structured Query Language. *SQL* is used to communicate with a database.

Worm—A computer *worm* is a type of malware that spreads copies of itself from computer to computer

Pharming—the fraudulent practice of directing internet users to a bogus website that mimics the appearance of a legitimate one, in order to obtain personal information such as passwords, account numbers, etc.

Shouldering—is looking at someone's information over their **shoulder**, for example looking at someone enter their PIN in a shop or at a cashpoint.

Adware—software that automatically displays or downloads advertising material such as banners or pop-ups

Virus—**s** is a type of malicious code or program written to alter the way a **computer** operates and is designed to spread from one **computer** to another.

Rootkit—a type of malware that are designed so that they can remain hidden on your computer, they enable administrator-level access to a computer .

Spyware—enables a user to obtain information about another's computer activities by transmitting data from their hard drive.

Trojan—a type of malware that is often disguised as legitimate software. *Trojans* can be employed by cyber-thieves and hackers trying to gain access to a computer or network

GDPR—General *Data Protection Regulation* (*GDPR*) is the toughest privacy and security law, it protect people’s data and how it is accessed

Vulnerability—when a network is in a state of being exposed to the possibility of being attacked or harmed

SPAM—s digital **junk** mail: unsolicited communications sent in bulk over the internet or through email

Packet Sniffers— is a piece of hardware or software used to monitor network traffic

Encryption— is a way of scrambling data so that only authorised parties can understand the information.

Network—A network consists of multiple devices that communicate with one another. It can be as small as two computers or as large as billions of devices.

Social engineering, - psychological manipulation of people into divulging confidential information.

Life jacking— a variation on Clickjacking in which malicious coding is associated with a Facebook Like button. The most common purposes of like-jacking include identity theft and the dissemination of viruses, social spam and hoaxes.

Botnet—*Botnets* are networks of hijacked computer devices used to carry out various scams and cyberattacks

Click Jacking—is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element

DDOS— A distributed denial-of-service (*DDoS*) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network

Ransomware—a type of malicious software designed to block access to a computer system until a sum of money is paid

Remote Access—the ability for an authorised person to access a computer or a network from a geographical distance through a network connection

Phishing—is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution

Malware is malicious **software** that is designed to **hack** a system. Malware can take many different forms.

Data Packet—is a unit of data made into a single package that travels along a given network path