The Children's Trust
For children with brain injury

Children's Safety Online

Presented by: Omar Farooq

Inspected and rated Outstanding
CareQuality Commission

Ofsted Outstanding Provider

Online Safety

The online world can be exciting and inspiring it has lots of opportunities to offer young children. However, it is important to manage and minimise the associated risks.

- *What does your children love doing online?*

- *What services and devices do they use?*

The Children's Trust
For children with brain injury

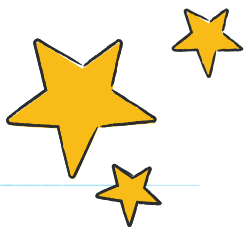
At present there are huge number of issues around online safety, but these can be classified into four areas of risk:

Conduct

Content

Contact

Commerce



Conduct

- Children need to be aware of the impact that their online activity can have on both themselves and other people, and the **digital footprint** that they create on the internet.

- It is easy to feel **anonymous** online and its important that children are aware of who is able to view, and potentially share, the information that they may have posted.

Content

- Some online content is not suitable for children and may be hurtful or harmful. This is true for content accessed and viewed via social network, online games, blogs and websites.

- It is important for children to consider the reliability of online material and be aware that it might not be true or written with a bias.

Contact

- It is important for children to realize that new friends made online may not be who they say they are and that once a friend is added to an online account you may be sharing your personal information with them.

- If you have concerns that your child is, or has been, the subject of inappropriate sexual contact or approach by another person it is vital that you report it to the police.

Commerce

- Risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your students or staff are at risk, please report it to the Anti-Phishing Working Group

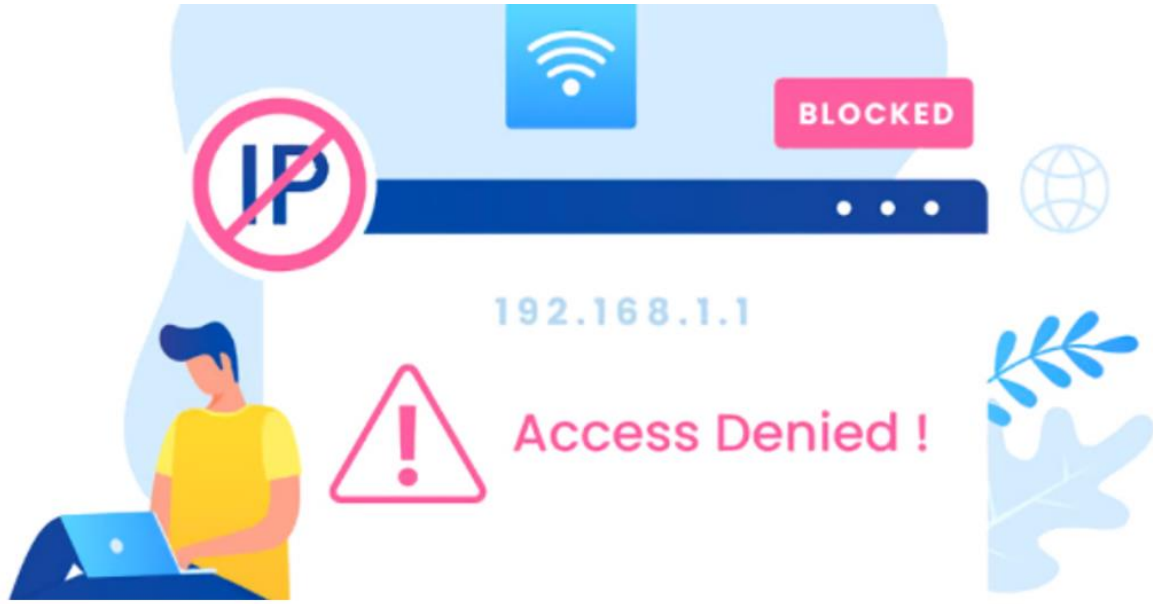
What is IT doing to keep us safe at The Children's Trust ?

The Children's Trust
For children with brain injury

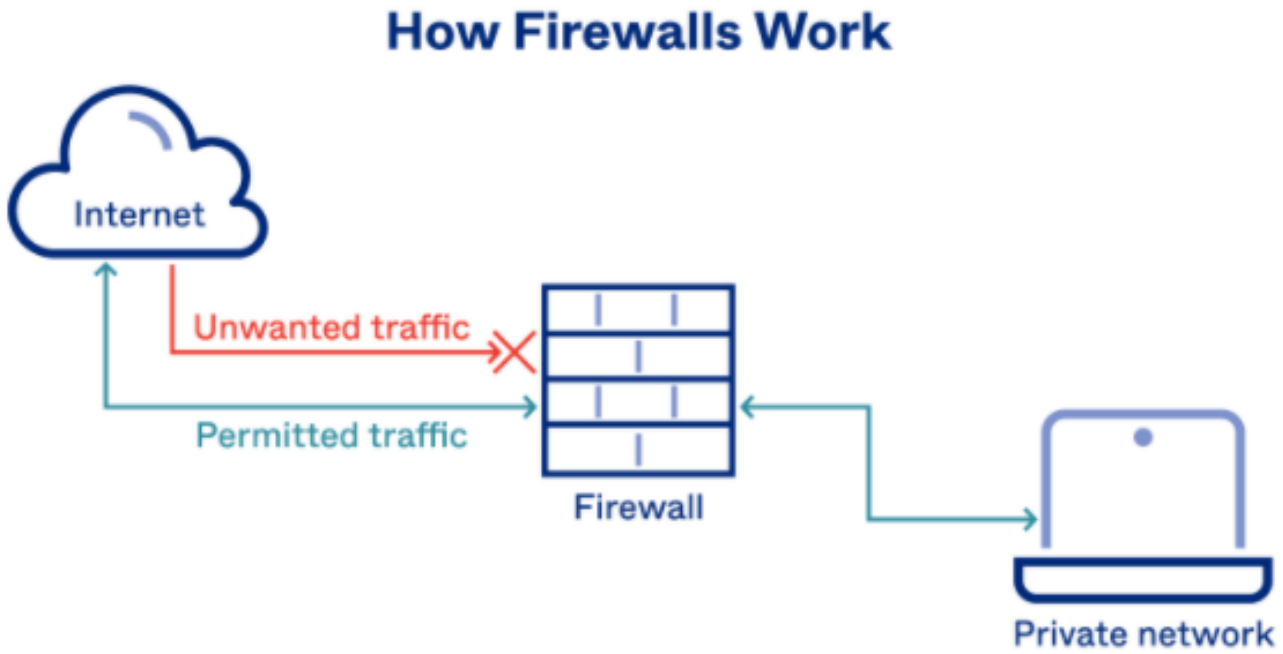
There are various online security measures that we have taken to ensure our network is safe from potential harmful contents. (Also safe from viruses and cyber attacks.)

They are the following:

- Firewall
- Web/Content Filtering
- Antivirus
- Microsoft Defender - ATP
- Maintain Backups
- Security Patches
- Data/Email Encryption
- Potentially Unwanted Programs PUPs
- Password – MFA
- Network Monitoring



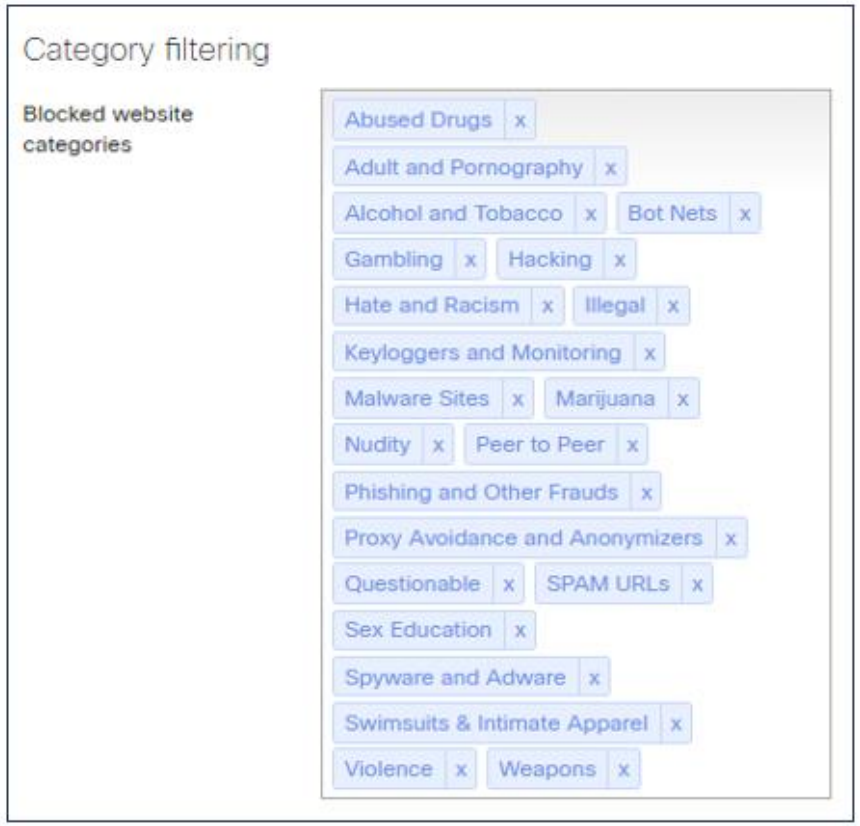
Firewall



- It creates a barrier between your system and external sources.
- Firewall is a hardware security appliance which blocks any unwanted traffic and threats such as malware and application-layer attacks.
- First Line of defense in security.

Web/Content Filtering

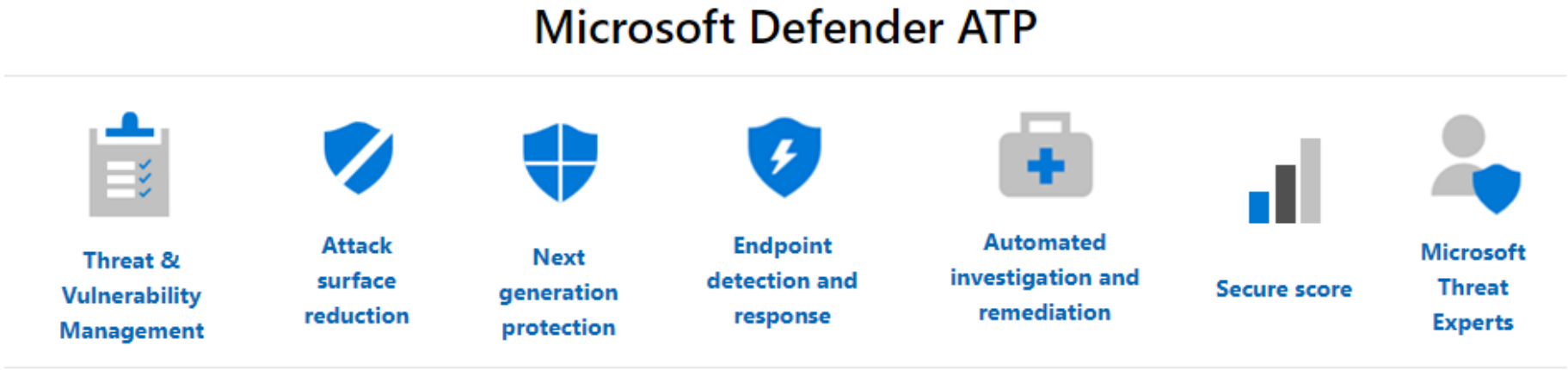
- An Internet content filtering tool gives organizations the ability to prevent web users visiting online destinations that may harbor hidden security risks or unacceptable content. For example, some of the categories are drugs, gambling, illegal activities.



Antivirus

- An Antivirus is a software which is designed to detect and destroy malicious code from your computer. It prevents malware from causing damage to your device.
  Modern antivirus products update themselves automatically, to provide protection against the latest viruses and other types of malware.

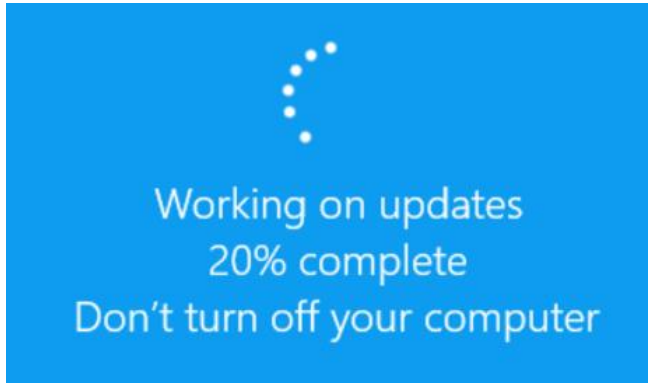
The Children's Trust
For children with brain injury



- Microsoft Defender – ATP Advanced Threat Protection is a **Cloud-based email filtering service** that can help protect us from unknown malware and viruses.

Security Patches - UPDATES

- A security patch update is an update that is often pushed from a software developer to all the devices that have the software.
- Mainly these updates are to fix or improve the program.
- This includes fixing security vulnerabilities and other bugs



Data/Email Encryption

- Email encryption is encryption of email messages to protect the content from being read by entities other than the intended recipients

Potentially Unwanted Programs PUPs

- As much as potentially unwanted programs don't pose serious risks to your devices, they can still be involved in an array of suspicious and unwanted activities. A PUP will sometimes function as a form of adware.

Password - MFA

Multi-factor authentication is when a user must provide two or more pieces of evidence to verify their identity to gain access to an app or emails etc.

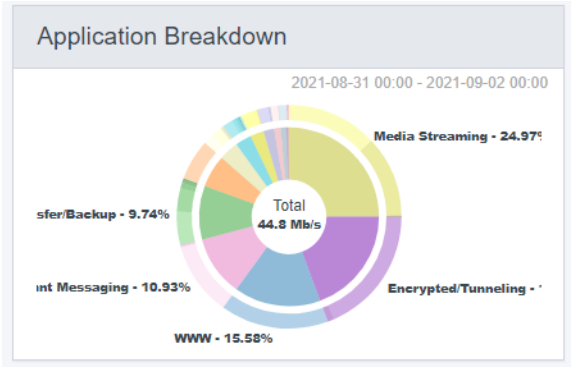
In addition to your password these can be:

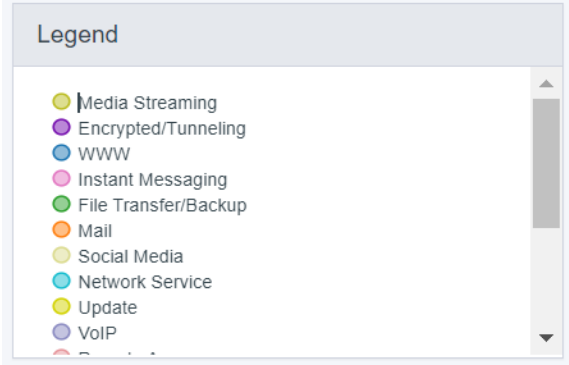
Something you have – Cell phone, USB or key card
or
Something you are – Fingerprints, Iris scan or some other biometric data prove.

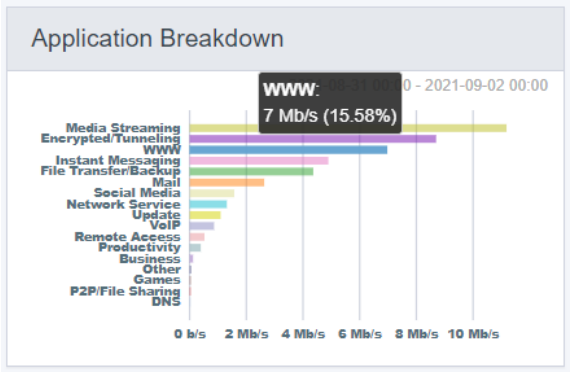
Network Monitoring & Scanning

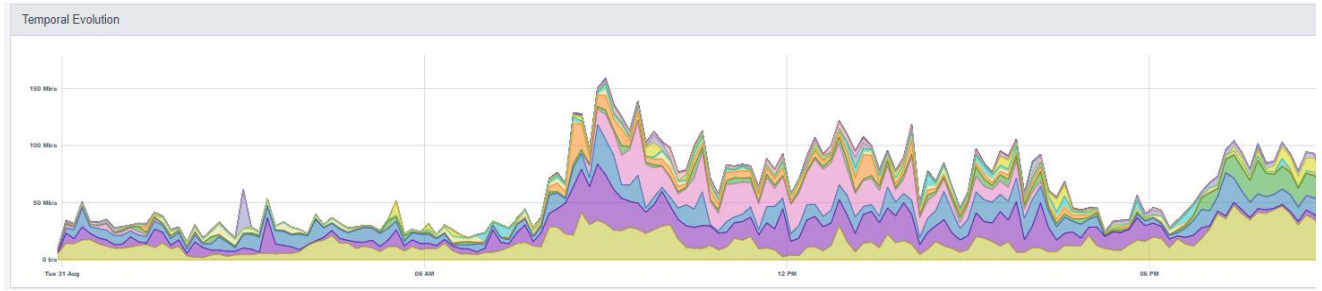
The Children's Trust
For children with brain injury

- Here in IT we have 'Network Monitoring Tool' which constantly monitors our network performance, and it detects any unusual behavior and notifies IT administrators.
- We regularly scan our entire network internally and externally as well as websites where the system picks up any vulnerabilities.









- When using the Internet, its important that you keep personal information safe and not share it with strangers.