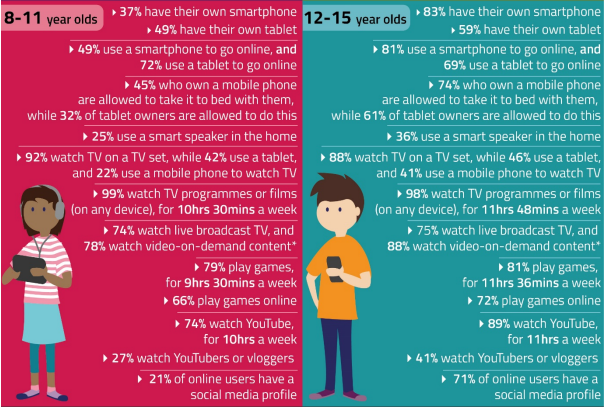
**Target Audience**

11-17

In today’s age, adults and children are using the internet for a magnitude of different purposes from communications and the exchange of information to listening to music and streaming your favourite show to social media and gaming.

In an Ofcom Children and parents: Media use and attitudes report published in 2019 revealing half of all 10 year olds in the UK had their own smartphones with internet access with that number doubling on the previous year and more children and young adults watch VoD (Video on Demand) than watch broadcast TV.

With that number rising it has resulted in more children being exposed to harmful online content, half of the 12-15 year olds surveyed said they had seen something hateful/disturbing online up a third from 2016 making it evident that awareness of cyber security and basic online best practises is essential.



(Ofcom, 2019)

Unfortunately, even with so many positive attributes, there are still many potentially negative effects from using the internet. With the general cyber security knowledge being low and the age of internet users getting lower and lower, it becomes more and more important to educate children and young adults about the dangers and negative impacts that can occur.

These can include but not limited to;

1. Fraud
2. Social Engineering
3. Viruses
4. Cyberbullying
5. Phishing
6. Pornography/Gambling/Harmful Content
7. Eavesdropping

(Amankwa, 2021)

Along with the need of understanding the basics of protecting yourself online there is a shortage of cyber security professionals around the UK, Europe and globally. An International Information System Security Certification Consortium report suggests part of the reason coming from the lack of recruiting and training of young people and highlights that only 35% of cyber security professionals globally are under the age of 40.

In an article published by the University of Bristol *Bringing Cyber to School: Integrating Cybersecurity Into Secondary School Education*, arguing the only way to counter this is to teach cyber security at a younger age to bridge the skill gap and to incentivize students into taking a career in cyber security. The U.K. National Audit Office revealed in 2013 that it could take up to two decades for this to be rectified.

(Pencheva, Hallett and Rashid, 2020)

# References

Amankwa, E., 2021. Relevance of Cybersecurity Education at Pedagogy Levels in Schools. *Journal of Information Security*, 12(04), pp.233-249.

Ofcom.org.uk. 2019. *Children and parents: Media use and attitudes report 2019*. [online] Available at: <https://www.ofcom.org.uk/\_\_data/assets/pdf\_file/0023/190616/children-media-use-attitudes-2019-report.pdf>

Pencheva, D., Hallett, J. and Rashid, A., 2020. Bringing Cyber to School: Integrating Cybersecurity Into Secondary School Education. *IEEE Security & Privacy*, 18(2), pp.68-74.