(DARK - WEB)

The Dark Web

The internet has changed in many ways since it first became publicly accessible in the 1990s. One of the most controversial developments is the growth of the so-called dark web.

This is the part of the World Wide Web that allows users to remain anonymous. You may be concerned about your child visiting the dark web, especially as press reports often associate it with dangerous, or illegal, online activity.

The Dark Web

However, it is not always used for illicit activity and the problem does not come from the technology itself, but rather from the ways in which people use it.

Being aware of the basic facts about these parts of the internet can help you to have open and realistic conversations with your child, especially if you are concerned about them using the dark web.

What are the different parts of the internet?

Surface Web

Exploring The Hidden Internet

4%

Deep Web

90%

Legal Documents

Government Records

Scientific Reports

Academic Records

Financial Records

Dark Web

6%

Drugs

Tor

Illegal Info

What are the different parts of the internet?

The deep web is the part of the internet which is generally hidden from public view.

Unlike the open web, the deep web is not accessed via the usual search engines.

Much of it is very ordinary; organisations have websites that can only be read by authorised people such as their employees, with their information password-protected.

What are the different parts of the internet?

The dark web is generally accessed using dedicated software, with the best known being TOR (The Onion Router).

Around 2.5 million people use TOR every day. It provides anonymising software which can be accessed via a Google search and then downloaded free of charge.

TOR itself is not the dark web but is a way to browse both the open and dark web, without anyone being able to identify the user or track their activity.

Why do people use TOR to access the dark web?

To access 'hidden services'

A hidden service is one where not only the user, but also the website itself, has their anonymity protected by TOR.

This means that the IP address of the site cannot be identified, hiding information about its host, location or content.

Studies suggest that the majority of TOR hidden service activity is illicit. For example, [a study in 2014](#) found that nearly 60% of hidden services contain illegal content such as drugs, weapons and stolen goods.
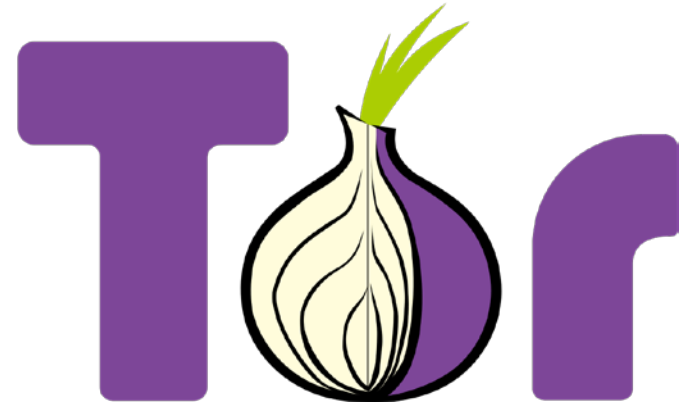
How do I know if my child is accessing the dark web?

You may see the logo to the right on your desktop or placed in a folder somewhere on your computer.

You may see your child accessing a web browser that looks different to the one you would usually use.

TOR often uses Mozilla Firefox as the basis of its browser.

I've just discovered that my child is using TOR. What should I do?

It is important to keep a sense of perspective. There are many reasons for using TOR, and it does not automatically mean that they are doing anything dangerous or illegal.

In many ways, the risks of the dark web are the same as those that may be encountered in the open web. Young people in both environments may access pornography, indecent images of children, or sites selling drugs and weapons.

It is important to have open conversations with your child to help them develop safer behaviours online. Explain to your child that there is a lot of illegal content in the dark web, and that you do not want them to be exposed to this.

Respect their desire for privacy

Many young people are concerned with political matters such as internet privacy and security.

There may be alternatives you could explore such as the use of a [VPN (Virtual Private Network)](#) as a potential means of providing an additional layer of security to their online activities.

In addition, encouraging young people to use privacy filters on social media, think critically about what they share online, and control who is on their friends and contacts lists, is a good way to help them maintain their online profile discreetly.

Get support and be supportive

You can use the [Thinkuknow website](#) to explore strategies that your child can use to help them to stay safe online, as well as tips on managing their online lives.

Above all, young people should know where to go if they come across something that worries them or makes them feel uncomfortable, in both the open and dark webs. Make sure they know they can come to you if they need to, regardless of where on the internet it may have occurred.

In addition, ensure they know how to [report to NCA-CEOP](#) if they are concerned about sexual abuse and exploitation online.

Further Reading

[What is the dark web and is it a threat?](#)

[Don't be afraid of the dark net](#)