

7 Minute Briefing: The Dark Web



7

What to do

Understanding a person's internet use is an integral part of safeguarding and supporting them. People may not necessarily be using the dark web for illicit reasons; equivalent risks on the open web.

Open a dialogue with people – make sure they know who they can go to no matter how or where they have accessed concerning content.

If you have a concern, refer to the **Right Help Right Time Guidance** for a young person or how to report a **concern** for an adult, or call 999 in an emergency.

6

Questions to Consider

Do you know how the vulnerable people you work with use the internet?

How do you build your own awareness to facilitate dialogue?

Find out more from: www.ceop.police.uk

<https://www.internetmatters.org/hub/guidance/what-is-the-dark-web-advice-for-parents/>

<https://www.thinkuknow.co.uk/parents/articles/dark-web-explained/>

5

Safeguarding concerns

Anonymity: there are a range of dark web forums that people could access anonymously suicide 'advice' pages, pages that promote self-harm, pro-bulimia and pro-anorexia forums. Perpetrators of child abuse can hide their identity. Policing the dark web is inherently problematic.

Hidden services: access to hidden services exposes people to a wide variety of items and content that is unlawful.

Illegal activity: accessing/buying illicit materials puts people at risk, including being exploited by criminals and those seeking to radicalise them.

4

Reasons people use the Dark Web

Hide their identity, access dubious content, avoid having personal data collected, engage in criminal activity, access hidden services, access forums and media exchanges e.g., for paedophiles or terrorists.

Criminal Exploitation includes grooming and coercing individuals to use their dark web to buy or sell drugs, weapons and stolen items. People could also use the dark web to seek information around extremist views which is less available on the open web.

1

Introduction

We can only search 4% of online content that is public; this is the Open or Surface Web. Roughly 90% of content represents the Deep Web and 6% the Dark Web. The terms 'dark web', 'dark net' & 'deep web' are often used interchangeably – many definitions include the dark web as part of the deep web.

The **dark web** was created by US military researchers to facilitate anonymous information exchange. No special skill or equipment is needed and it is typically done via special software and programmes.

2

Why it matters?

In the digital world we live and work in, we can no longer think of online safety as a separate entity when safeguarding children or adults. The online world and the 'real' world are so integrated that digital safeguarding IS safeguarding.

Anyone accessing the dark web can be exposed to criminality or disturbing and illegal images; or be able to purchase illegal items.

3

Information

Deep Web: hidden from public view with limited access via search engines – mainly intranet sites, password protected areas of sites, e.g., social media profiles, online banking pages etc.

Dark Web: only accessible through special software, commonly TOR (The Onion Router). Networks are encrypted repeatedly, making a user anonymous. The dark web is not illegal and not all content is illegal, e.g., the anonymity of the dark web can be used for whistleblowing. However, due to the level of privacy it provides, many illegal activities and transactions take place within the dark web.