Guidance for colleagues

Online Safeguarding: The Dark Web

What is it?

The World Web (Open Web):

The world web is the public facing side to the internet which is used commonly. This includes public facing websites and resources. Only 4% of internet information is hosted through the world web.

The Deep Web:

The deep web is hidden from initial public view, and has limited access via search engines. For example, mailing lists held by a company would be part of the deep web. 90% of information is held in the deep web.

The Dark Web:

The dark web refers to an area of the internet that can only be accessed through particular software. This means networks are encrypted repeatedly, making a user anonymous. 6%[1] of internet information is on the dark web. Accessing the dark web is not illegal, but due to its anonymity it is used for criminal purposes.

How do people access the Dark Web?

The Dark Web can be accessed through particular software and programmes. The most common of these is called **TOR** (The Onion Router). The software anonymises the user through directing all requests to a centralised source, and randomly redirecting it. It is known as "The Onion Router" as it promises layers of encryption, meaning a user could not be traced.

[1] https://www.internetmatters.org/hub/guidance/what-is-the-dark-web-advice-for-parents/

Is it illegal?

Accessing software such as TOR is not illegal and not all content on the dark web is illegal. For example 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.

Why would young people use it?

Anonymity – Young people may want to remain anonymous in their online interactions. This might be because they don't trust the surveillance of the internet.

To reach "Hidden Services" – A hidden service is one where not only the user, but also the website itself, has their anonymity protected by **TOR.**

Illegal activity – Young people may access the dark web for illegal purposes. Child Criminal Exploitation includes grooming and coercing children to use the dark web to buy or sell drugs, weapons and stolen items. Young people could also be seeking information around extremist views which is less available on the open web.

Why is it a safeguarding concern?

The anonymity aspect: This could present safeguarding concerns. There are a wide range of "forums" within the dark web that a young person could be accessing anonymously. These include suicide "advice" pages, pages that promote self-harm, pro-bulimia, and pro-anorexia forums. In addition, the level of anonymity that the dark web offers means that perpetrators of child abuse have their identity hidden. This means that policing and investigating these spaces is inherently problematic.

The "hidden services" aspect: The access to hidden services poses a risk to young people as it exposes them to a wide variety of items and content that would not be permissible on the open web. This can include illegal drugs, weapons, explicit imagery or indecent images of children.

The "illegal activity" aspect is a clear safeguarding concern. Being able to access and buy illicit materials puts a young person's safety and physical health at risk. It also connects young people to criminals who may seek to exploit them. For young people who may be seeking information around extremist views, it also connects them with individuals who may seek to exploit them.

What could a young person's use of the dark web tell us as professionals?

Understanding a young person's internet use is an integral part of safeguarding and supporting them. Many young people view their digital self as an extension of their identity and sense of self. Therefore, it's crucial that we are supporting young people digitally.

To access the dark web requires knowledge and know how. To access hidden services and to establish anonymity requires a level of skill, and is likely to not be by chance. Therefore, understanding the motivations as to why a young person is accessing these encrypted parts of the web can tell us a lot and must be taken in context.

How can I talk to young people about this?

Knowledge gaps between professionals and the young people they support may be apparent when it comes to online activity, so building up awareness over such issues could facilitate smoother conversations. Remember, that young people may not necessarily be using the dark web for illicit reasons and that equivalent risks exist on the open web.[2]

Dialogue: Open a dialogue about how young people use and view the internet and avoid expressing judgment about their decisions even if they include use of the dark web. Consider discussing what aspects they enjoy about being connected, what kind of websites they like, ask how they stay safe online and explore what they would do if they saw something that made them uncomfortable.

Privacy: It may be that young people are using TOR as they are concerned about their online privacy. In this case there are alternatives you can explore such as using a Virtual Private Network (VPN[3]) for additional online security. It would also be valuable to discuss how and why some people use privacy to inflict harm.

Support: What is most important is that young people have a trusted adult to talk to and know where to go if the come across something that worries them or makes them feel uncomfortable in the dark or open web and in their use of social media. Make sure they know they can come to you no matter how or where they have accessed concerning content.

What to do if you have concerns:

We have a duty and commitment to safeguarding and promote the welfare of children, young people and adults at risk who use our services, or who we come into contact with; their wellbeing is paramount to the work of The Children's Society. No one agency alone, can safeguard, protect - or identify, target and disrupt the offenders who seek to exploit those with whom we work. For this reason, and in line with the Safeguarding Children, Young People and Adults at Risk Policy and Procedure (December 2019), if you think they may be at immediate risk of harm or abuse, or an offence is being committed, call 999. Please refer to The Children's Society Safeguarding Policy and Procedures for more detailed guidance including information regarding intelligence sharing.

[2] https://www.thinkuknow.co.uk/parents/articles/what-is-the-dark-web/

[3] https://parentinfo.org/article/what-are-virtual-private-networks

There are resources for professionals, young people and parents/carers available through the following links:

https://www.thinkuknow.co.uk/parents/articles/what-is-the-dark-web/

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

https://www.ceop.police.uk/safety-centre/

https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/child-sexual-abuse-and-exploitation?highlight=WyJkYXJrIiwiJ2RhcmsiLCJ3ZWIiLCJ3ZWInIiwiZGFyayB3ZWIiXQ==

https://www.nspcc.org.uk/keeping-children-safe/our-services/nspcc-helpline/