

The Dark Web

Next steps

- Discuss how this might impact on your team or your service users
- Complete your team [action plan](#)

Find out more from:

- CEOP at www.ceop.police.uk
- Internet matters at www.internetmatters.org
- MSB website www.manchestersafeguardingboards.co.uk

Perspective

- children or adults can also access sites with indecent images, selling drugs or weapons on the 'open web'
- Sex offenders are more likely to approach children in the 'open web' than the 'dark web' - they tend to use the dark web to meet online & discuss their strategy to take advantage of children.

Background

According to statistics, we can only search 4% of the online content that is public; this is the '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 (incorrectly) used interchangeably. The dark web was created by US military researchers to facilitate completely anonymous information exchange. Access does not require any particular skill or equipment & is typically done via TOR.

Why it matters

In the digital world we live & work in, we can no longer think of 'e-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 & illegal images; or be able to purchase illegal items such as drugs, firearms or extreme pornography.
Predators can use the dark web to groom or recruit the vulnerable.



Deep Web:

- part of the World Wide Web hidden from public view
- content is not indexed by usual search engines - mainly consists of databases e.g. web mail or online banking.

Dark Web:

- part of the www that is only accessible through special software
- commonly TOR (The Onion Router) - the icon is a stylised onion (layers symbolise levels of security)



How is the Dark Web policed?

CEOP, part of the National Crime Agency, uses experts, including forensic professionals & covert internet investigators, to track illegal activity on the dark web. CEOP gets over 1,300 reports a month, mostly from industry groups and internet service providers.

Why use the Dark Web?

Reasons include to:

- hide ones identity
- avoid being found
- access dubious content
- avoid having personal data collected
- engage in criminal activity
- access hidden services – TOR isn't hidden but sites & users under it are hidden under layers of dark net encryption
- facilitate criminal activities - trading in the black market or buying illegal products e.g. weapons or drugs
- access forums & media exchanges e.g. for paedophiles or terrorists.

Unless you carry out unlawful acts, it is not illegal to use the dark web or TOR - the anonymity offered can be legitimate. In some countries it is used by dissidents, journalists & whistle-blowers to champion groups & ideas which may be censored in repressive regimes.