The Dark Web

01 Background:

Developed by the American Military in the 1990s as post nuclear attack network; a secure and anonymous method of accessing 'hidden' internet sites and exchanging material, 'peer to peer'. Encryption makes IP addresses extremely difficult to trace

02 Why it matters:

Those accessing the dark web can be exposed to criminality; disturbing and illegal imagery. It also enables the purchase of illegal items such as drugs, firearms and extreme pornography. Predators use the dark Web to groom/recruit the vulnerable.

03 Access:

Does not require any particular skill or equipment. It is typically achieved through the 'Onion Router' or TOR , the icon of which is a stylised onion, the layers of which symbolise the levels of security

04 Types of Abuse:

The dark web is used for facilitating serious crimes. It is also used by predators to persuade vulnerable, often isolated individuals to engage in sexual activity, which can then be used to blackmail them. It is also used by radicalisers to recruit for and encourage terrorism.

05 Key Issues:

It is not illegal to use the dark web. In many countries it is used by dissidents, journalists and whistleblowers to champion legitimate groups and ideas which may be censured in repressive regimes. The anonymity it offers can therefore be legitimate.

06 How to respond:

Be careful not to overreact. Consider the guidance at 7 and technical solutions.

Does the person understand their own vulnerability in that environment to exploitation, fraud, social media blackmail or radicalisation.

07 What to do?

Consider contacting CEOP; report hidden sites, they can be removed: advice and counselling for those who may be affected.

www.ceop.police.uk

Northumberland
Strategic Safeguarding Partnership