



Dark Web Factsheet

The Dark Web – Responding to Incidents and Further Considerations

What is the Dark Web?

If you imagine the internet as an iceberg. The tip is the internet we use every day, in other words, the public web. The deep web is the bit just underneath the surface, that contains things like cloud storage, research and parent data, anything you would need a login to access.

The dark web (a.k.a Tor - The Onion Router) is at the bottom of the iceberg. You need a special Tor browser to access it. The content in there is not indexed by search engines like we use on the surface.

The main attraction of the dark web, is that unlike the public web, the origin of the user is hidden from the server and all the hops in between. This is achieved by bouncing the signal around many different servers. Each server wraps or unwraps the message so it knows who to send it to next (Hence The Onion Router). Each wrapped message is encrypted and so it only knows where to send it to next, not who sent it or where it is ultimately going.

This is a very simplistic description and if you are interested in learning more about how it works, check out this further reading - [Traversals - Surface Web](#).

Or for an even deeper dive, you can check out this book - [Goodreads - The Dark Net](#).

What Are the Risks?

Because the traffic on the dark web cannot be tracked or logged in the same way as the public web, it facilitates the possibility to do business that could put the participants in danger or is not lawful and would be more easily picked up on the public web*.

There are sites on the dark web that look a lot like Amazon, but sell items such as firearms, drugs, weapons and more. Because it is not regulated, there is a risk that you may find content on the dark web that is disturbing, and/or illegal.

The risk of a young person coming into contact with a paedophile on the dark web is apparent, however it is debateable whether the likelihood differs from that on the public web. It is common that predators are more likely to stick to easily accessible sites, where lots of children and young people are.

Child sexual abuse imagery is of course also available, just as it is on the public web. Most of it though is behind a pay wall, meaning users would likely have to use a crypto currency like Bitcoin to access it. Again though, this is not much different than the public web.

** This is not to say that if you conduct illegal business you will not be found out. The police have and will continue to find criminals using data from the darkweb. For example; [bbc.co.uk/news/technology-54247529](https://www.bbc.co.uk/news/technology-54247529)*

What are the Benefits of Using the Dark Web?



A lot of safety and privacy experts would actually advise using the dark web/a Tor browser in order to keep your data secure, as you can also protect your identity on the public web by accessing it through Tor.

On the public web, we are constantly followed around, our data collected to create profiles of who we are, so that information can be sold and used to advertise and sell us products.

Although cookies still function on Tor just as they do on the public web, the browser provides tools to delete those cookies when you exit the browser. You can click a button to "Create a new identity". This means that your true IP address is hidden, combined with deletion of your cookies regularly. This prevents profiles from being built and any offline data being attached to that profile.

The lack of tracing allows room for anonymity that you simply cannot obtain while accessing the web normally. This is vitally important for some, not for illegal activities but for very legitimate ones too.

Journalists in places where reporting may be prohibited for example, may use the dark web in order to share what they are seeing. There are reportedly a number of sites on the dark web dedicated to facilitating this kind of journalism, giving a voice to human rights activists and campaigners.

How to Respond if a Young Person is Using the Dark Web

On the helpline, we have calls from professionals who are very panicked after hearing a young person they work with is using the dark web. The first response is to not overreact. Like any disclosure, avoid shutting down the conversation by being overtly shocked or presuming that they are up to no good.

As we have touched upon, there are some good reasons for some to use the dark web. It is important to consider this and try to get a better understanding from the young person of what their rationale is for using it. We often see that young people with a keen interest in computing and coding will be more inclined to use these spaces. Take an interest in the why and they will likely be able to teach you a thing or two.

Banning, blocking or removing devices may feel like the best way to safeguard, but will probably have an opposite effect for most. Children that are adept at using the web in this way are likely to be able to bypass restrictions and filters. You cannot remove devices forever and when they do eventually get it back, they will not disclose anything to you again, putting them at further risk.

There are some aggravating factors to look out for, that may illicit a stronger response or safeguarding referral:

- **Buying/ selling illegal items** – obviously if there is mention of this, it needs to be investigated further. It is probably very unlikely that a young person would directly disclose this. It's about looking for other indicators such as, having lots of money or new items of clothing/gadgets, just as you would if you suspected this sort of illegal activity offline
- **Special educational needs** - we often hear from professionals working with children on the autistic spectrum (not exclusively), who use the dark web. This is not always a



cause for concern and these children are perhaps more tech savvy than most, but as they have the added vulnerability they may be more susceptible to being in contact with unsavoury characters. This vulnerability is no more apparent than it is on the public web, but it is worth bearing in mind. Continue to have conversations about online safety, specifically focusing on the social aspect that they may struggle with (i.e. not trusting implicitly that people are who they say they are etc). For resources check out; internetmatters.org/inclusive-digital-safety/

- **Excessive use/ compulsion** - spending too much time online is a problem, whether that's playing games, scrolling through social media or accessing forums etc on the dark web. It is important we all (not just young people) have time off, and have other activities / hobbies in our lives. Compulsion needs to be addressed and sometimes therapeutic intervention is needed

If any of these factors are identified and you have serious concerns about the young persons welfare, consult your safeguarding policy / DSL (designated safeguarding lead) and make a referral where needed. You can also call or contact the helpline to talk through any scenarios to get some objective advice: