What is the dark web? Busy readers guide.

Darkweb is the part of the World Wide Web that is only accessible utilising specialised software, allowing users and website operators to remain anonymous or untraceable. You've probably associated the dark web with criminal activity - a place where people buy drugs, guns, and credit card details.

But what exactly is it, how does it work, and how can you make sure your details don't end up there?

There are three layers of the web: surface, deep and dark.

There's more to the internet than meets the surface.

For most of us, the internet consists of whatever we can find using search engines like Google – this is known as the surface web.

But the surface web is estimated only to contain around 4% of all online content. So where is the other 96%?

Beneath the surface web lies the deep web. The deep web contains all the content that doesn't show up in search results, for example, your work intranet, your online bank account, and government documents. We use the deep web all the time, though you might not know it. Every time you log in to an online account, you're accessing the deep web.

While most (if not all) of this content is perfectly legal, it's classified information that isn't meant for public access. For this reason, it's hidden from search engines' results.

But there's more. Beneath the deep web lies the dark web: the internet's secret underside.

The dark web is a series of private networks.

The dark web is a series of private networks that can only be accessed via specialised software. The most popular software is called "Tor" (The Onion Router). This is why dark websites are accessed using Tor end in .onion instead of .com.

When people use the dark web, their location and usage are concealed. The US government actually invented it as a way to help their own spies remain untraceable. However, due to its anonymity, it's become a popular playground for criminal activity.

It's full of dark marketplaces selling everything from drugs to people's identities.- **CAN THIS BE REMOVED AS ITS REPEATED BELOW?**

Criminals use the dark web as a marketplace for selling anything and everything illegal: drugs, weapons, illicit pornography, people's personal information, and more. The most famous of these marketplaces was called Silk Road (this was taken down by authorities in 2013).

However, it's important to note that the dark web isn't only used for criminal activity. It's also used by whistleblowers, activists and political dissidents to discuss things in secret.

If your identity ends up on the dark web, you're at risk of identity fraud.

When a hacker steals your personal information (and there are many ways they can do this), the dark web is where it ends up being sold and potentially used to commit identity fraud.

While credit card details are the most commonly traded, fraudsters also sell login details to Netflix, Uber and Spotify accounts for as little as £2.50. Hackers will trade your social media passwords, your PayPal login details and even online dating profiles (although these aren't worth very much).

Some dark websites specialise in stitching together all of your stolen details to create a 'fullz' (scammer slang for a full identity package). If a scammer has a full identity set with all your details and passwords, it could cost around £900.

The effects of identity fraud can be wide-reaching

Once someone has bought your personal details, they're then ready to commit identity fraud.

There are many ways they could do this: opening credit cards and loans in your name, buying goods with your money, or committing other crimes and reporting your name to the police.

Resolving this kind of fraud can take up a significant amount of your time and money. That's not to mention the emotional impact identity fraud can have. In essence, victims often end up feeling isolated, embarrassed and scared of using the internet.