The internet comprises of three different layers: the surface web, the deep web and the dark web.

The top layer, the surface web, are web pages that show up using search engines such as Google, Bing, Yahoo, etc. Search engines like Google, search and index websites because of links. They use links to rank search results according to things like relevancy, inbound links, and keywords. So, surface web is the regular browsers we use.

The dark web is the part of the internet that isn't visible to search engines. It requires the use of an anonymizing browser called Tor to be accessed. Deep web are the parts of the web not indexed or searchable by search engines. The content of the deep web can be located and accessed by a direct URL or IP address, but this may require a password or other security access to get past public-website pages. The Deep web covers many common uses such as mail, online banking, private or otherwise restricted access social-media pages and profiles, some web forums that require registration and services that users must pay for (protected by paywalls). In short, the deep web are web pages which search engines can't access and are therefore hidden. They are accessed via passwords and authorization. The dark web was created by the US government to allow spies to exchange information anonymously.

US military researchers developed the technology, known as Tor also called The Onion Router in the 1990s and released it into the public domain for everyone to use.

Tools and services of dark web consists of:

1) Infection or attacks (malware, DDoS, Botnets)
2) Access (Trojans, Keyloggers, exploits)
3) Espionage (services, customization and targeting)
4) Support services such as tutorials
5) Credentials
6) Phishing

7) Refunds
8) Customer, Operational and financial data
9) Intellectual property/trade secrets

Dark web mostly consists of:

1) Stolen information
2) Illicit substances
3) Disturbing and dangerous items and services

Tor is known for providing online anonymity, so it can be effective for sharing sensitive information. User should always have his Tor and Tor applications updated. Device's operating system should also be up-to-date.

User shouldn't use his/her regular email on websites when using Tor. While Tor is designed with anonymity in mind, providing user's regular email address could expose user's identity. To buy items on the dark web, one uses cryptocurrencies like bitcoin, Ethereum and ripple. User shouldn't use Tor on a public network. They should use a virtual private network (VPN) which can encrypt your data and help protect your online privacy.

Precautions to take while on the dark web:

1) Viruses
2) Hackers
3) Webcam and microphone hijacking