The Deep Web

What is the Deep Web?
The deep web refers to sites and pages that are not indexed by search engines such as Google or Bing, and many of them require some form of authentication before they can be viewed. Examples of the deep web include email accounts, cloud storage, Spotify libraries, cryptocurrency wallets, online student portals and bank accounts. All of these require you to first log into an account before you can view them. Imagine if these pages were all available in search engines! Your Netflix dashboard is another example of a deep web site. While Netflix's homepage is accessible to anyone, your personal dashboard can only be opened if the correct login info is provided and is not available to anyone who searches for it. News articles that are behind paywalls are also part of the deep web. This is because you need to pay a subscription fee before you can read the articles.

The "deep web" is extremely large and is estimated to be around 500 times bigger than the "normal internet". In other words it accounts for around 99.8% of all websites. To have an idea of the size of the deep web:

- More than 350 billion emails are sent daily, contributing to the growing size of the deep web.
- There are more than 1 million academic papers uploaded on the Social Science Research Network. They are stored on the deep web as you can only access them with an account.
- Facebook's 3 billion users, Instagram's 2 billion users and TikTok's 2 billion users have uploaded trillions of photos and videos over the years, and they are all on the deep web.

Search engines can't find deep web pages because they don't have any inbound or outbound links connecting them to other pages. It would be like trying to locate a hidden room that doesn't have any doors and isn't on any maps. Deep web pages are purposely hidden from traditional search engines in order to protect their content. For instance, the exact URL of your bank account dashboard is not available to any search engine. This makes it more difficult for hackers to gain access to your bank account. For the same reason, most deep web pages are protected by subscriptions and logins.

Is the Deep Web Dangerous?
The deep web is not inherently more dangerous than the normal internet. While there are many deep web sites that are safe to view, there are also many pages that are dangerous or best avoided. It is recommended to secure your connection every time you visit. For example:

1. Use reliable antivirus software.
2. Use a VPN.
3. Use strong, unique passwords.
4. Use two-factor authentication for all accounts, if available.

The biggest dangers associated with the deep web are data leaks and targeted hacking. These incidents can access and expose personal information and unfortunately are becoming more common:

- In 2022, the popular fantasy sports and betting platform DraftKings was hacked. The hackers accessed player accounts, stealing around $300,000. Players' account balances are stored on company servers on the deep web, making them a lucrative target for cyber-criminals.
- In January 2023, sports and fashion giant JD Sports suffered a "data breach" and the personal information of around 10 million customers was stolen from the deep web.
- In July 2023, the popular game Roblox saw a data breach that affected not just players but developers too.

Note: A "data breach" is similar to a "cyber attack". It is unauthorized access to computer systems, networks or databases. "Breached data" can include personal information, financial records or intellectual property. The consequences of a data breach can be financial losses, reputational damage, legal implications and potential harm to victims. This can include individual people, small businesses and multinational enterprises.

What is the "dark web"?
The most secretive section of the deep web is called the "dark web", which contains many illegal sites. The biggest attraction of the deep web is that it offers total anonymity, and a way to bypass internet censorship and tracking. Many people use it to sell drugs, weapons, illegal porn, or stolen credit card information. The dark web is significantly smaller than the deep web, and estimates suggest that the dark web only makes up around 0.01% of the deep web.

How do we explore the dark web?
To access the deep web, you need to use TOR (The Onion Router) browser, which is free and easy to install from here: https://www.torproject.org/download/
One of the primary functions of the TOR browser is that it allows access to "onion" pages, which are encrypted many times for maximum privacy. TOR also lets users connect to normal websites anonymously, so that their internet service providers cannot see what they're browsing. Also, the websites cannot identify the location of the users who are browsing their pages. On the TOR browser, the connection requests are re-routed and encrypted many times before reaching their destination. For example, if a user in Singapore is trying to connect to a website in London, the request on a TOR browser could be routed from Singapore to New York to Sydney to Capetown, and then to London, making it nearly impossible to know the geographical origin of the request. As a consequence of this, loading pages in the TOR browser is generally slower than in other browsers. Due to its guaranteed privacy and anonymity, the TOR service is used extensively by journalists and law enforcement agencies. The TOR browser was originally created by the North American government.

All pages on the deep web have a 56 character name and an "onion" extension. For example:

http://7dyt46wpwwlccc5nyp3m3xng6pdx3rdcknul57x6raxwf4enpw3nymqd.onion/

If you don't know the specific address of a deep web site, then there is no way of finding it. There are a number of deep web search engines to help you navigate, but their results are extremely limited and don't give access to private data (for example bank accounts and Netflix home pages). Here are two examples:

Ahmia: http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/
Torch: http://torchdeedp3i2jigzjdmfpn5ttjhthh5wbmda2rr3jvqjg5p77c54dqd.onion/

Final thoughts
Search engines don't index deep web pages for good reason. You don't want your bank information or private photos popping up in users' search queries. While most deep web pages are safe, the real danger lies in hackers attempting to steal and sell the data stored there. Dark web sites also pose a great level of risk in terms of malware infections, credential theft, and more.

They say that the deep web is similar to a black hole. If you don't take care, you can go deeper and deeper, and you might go so far, that your life will never be the same!