SEMtech!

Student Engagement & Mentoring in Technology

The Deep & Dark Web

You have probably read news about the nefarious dark or deep web happenings. Unfortunately, the two terms are often confused but have distinct meanings. The web can be divided into 3 broad segments: the ***surface*****, deep, and** ***dark web*****.**

Content that is freely available for anyone to access is part of the ***surface web***. Public blogs, news sites, and public Twitter are all examples of surface web content. The surface web is indexed by search engines, and sometimes, the surface web is defined as content that can be found by the search engine.

The ***deep web*** is web content that cannot be accessed without logging in to a website or web service. Most Internet users access deep web content on a regular basis. Checking your bank balance, reading your e-mail through websites like Gmail, logging into Facebook, and looking at your personal shopping history on Amazon are all examples of deep web activities. The deep web content is not publicly available and generally requires a password. Most users don't want their e-mail or bank balances to be publicly available, so there's a good reason why this type of content isn't public and cannot be indexed by search engines.

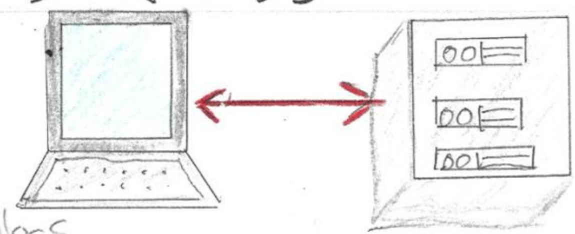
The ***dark web*** is web content that requires specialized software to access. You cannot access the dark web using only a standard web browser; the most prevalent dark web technology is Tor (the onion router). Through encryption and relays, Tor allows for anonymous access to the web, preventing a user's ISP from monitoring which sites are accessed and preventing sites from knowing their visitor's IP addresses. Additionally, Tor enables users to access websites, known as onion services, which cannot be accessed without Tor. These sites are part of the dark web. Tour hides the IP addresses of onion services, making them anonymous. As you might expect, the anonymity of the dark web is sometimes exploited for criminal purposes. However, there are legitimate uses for the privacy afforded by the dark web, such as whistleblowing and political discussions. Use caution when accessing content on the dark web.

SEMtech!

Student Engagement & Mentoring in Technology

DEEP WEB / Dark WEB

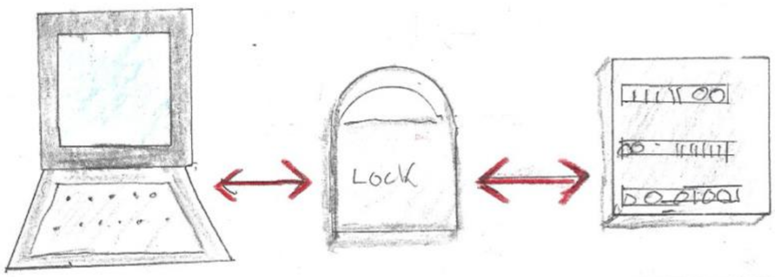
Surface WEB



content is freely available for anyone to access. Public Blogs, News Sites, Public twitter, etc
content can be found with Serch Engine

DEEP WEB

content is reached thru logging in. Banking, email, Facebook, shopping history content is not publicly available and requires a password for access



Dark WEB

Content that requires specialized Software to access. TOR is an onion router. Goes through a system of encryption and relays. TOR allows anonymous access to the WEB, Preventing ISPs from tracking. AND sites can't get IP address of Visitors. Users acces sites known as Onion Services. Also can be used for Political conversations and whistle blowing

Study Guide: Understanding the Web Layers – Surface, Deep, and Dark Web

1. Surface Web

Definition:
The portion of the internet that is freely available and indexable by standard search engines (e.g., Google, Bing).

Key Characteristics:

- Public content is accessible by anyone.
- No login required.
- Indexed by search engines.
- Examples:
  - Public blogs
  - News websites
  - Public social media profiles (e.g., public Twitter)

Use Cases:
Research, general browsing, public communication.

---

2. Deep Web

Definition:
Content on the internet that is not indexed by standard search engines and requires authentication to access.

Key Characteristics:

- Not publicly accessible without login or credentials.
- Content is behind a wall (password protection, session ID, etc.).
- Examples:
  - Banking portals
  - Email accounts
  - Private Facebook messages or shopping history

Access Method:
Requires specific credentials (username/password).

Use Cases:
Personal data management, secure business portals, private cloud storage.

---

3. Dark Web

Definition:
A segment of the Deep Web that requires specialized tools (e.g., Tor browser) to access. Designed to anonymize user activity and site hosting.

Key Characteristics:

- Accessed using special software such as **Tor (The Onion Router)**.
- Employs **encryption** and **relays** for anonymity.
- Prevents ISPs and websites from tracking IP addresses.
- Not indexed by search engines.
- Sites often have `.onion` domains.

Examples of Use:

- Anonymous communication
- Whistleblowing platforms
- Political activism under repressive regimes
- Illicit trade (note: this is illegal and unethical use)

Security & Ethical Note: While the **technology enables privacy**, it can also be misused. Education should emphasize **ethical behavior, digital citizenship, and legal awareness**.

Key Terms & Concepts

Term	Definition
Surface Web	Freely accessible, indexable portion of the internet.
Deep Web	Content not indexed by search engines, usually behind authentication.
Dark Web	Encrypted network requiring special tools (e.g., Tor) for anonymous access.
Tor	A network that anonymizes internet traffic by routing it through nodes.
onion	A domain used for services accessible via the Tor network.
Encryption	Method of securing data so that only authorized parties can access it.
Relays	Servers used in Tor to pass encrypted traffic between nodes.

Study Tips

- **Compare and contrast** each web layer using examples.
- Understand **ethical boundaries** in exploring or discussing the Dark Web.
- Practice explaining how **Tor** works in simple terms.
- Review how these concepts align with **cybersecurity principles** like privacy, anonymity, and data protection.