The Internet and Safe Space

The internet is a set of wires that are connected to a series of computers. The user requests information via a web browser, and a server responds with the requested data. Similar to the Boston MBTA system, the train represents the data being transmitted. The subway tunnels, represent the fiber wires that run underground throughout the world. Finally, the fibers transmit information from one computer to another. When a user makes a request for information, an outbound message is sent to a server. The server, then transmits the information back to the user who made the request. Similar to how the train moves about throughout the city, the data is transferred outbound and inbound within the fiber. As the flow of information moves along, it passes through a series of checkpoints like ISP, DNS, and ect. This process is similar to how a train makes various stops along the subway line before reaching its final destination.

When using the internet, a user must be aware that everything they do is tracked by their Internet service provider and often times their information is sold to the highest bidder without your consent. In order to protect yourself from this there are many ways to protect your information.

1. A VPN, or virtual private network, is a useful tool to keep your identity and information private. It is recommended a higher-quality paid VPN as free ones are likely selling your information rather than protect it. Best VPNs do not log your history and do not have affiliations with governments. VPNs hide your geographic location and changes your computer’s IP address so it is harder to be tracked.

2. Browser Plug-ins add additional safety features. These can be downloaded and installed onto your browser. (The best browsers to use are Google Chrome and Mozilla Firefox).

a) User Agent Spoofer - this plug-in hides your Operating System and other identifying information, which nefarious sources can use to identify you even when using a VPN.

b) Privacy Badger - this plug-in stops your computer from being tracked across different websites.

c) UBlock Origin - this plug-in stops ads on websites you visit.

3. Consider getting a password manager. You should set one strong master password with 3 special characters, one sentence, and 3 more special characters. The manager helps you create passwords for all of your accounts and stores them for you. A good example of this is LastPass.

4. To safely access the internet you can use a browser called Tor. This allows your request to be encrypted, so your ISP will not see that request. This may be slower but it’s worth your security.

5. Also, when surfing the web, going on websites that have https rather than http is safer because it encrypts your data.