*C18742005 - Steven Aherne*

*TU856/4 | CMPU4007 – Advanced Security 1*

*Advanced security 1*

Lab 1

**Part A**

* Browser Extensions:
  + ZoneAlarm Web Secure – Offers a safe search engine showing which sites are secure or not. Scans emails and sites before you insert credentials preventing phishing attacks. It also sanitises downloaded files that contain malicious content.
  + HTTPS Everywhere – Forces sites to use HTTPS connections instead of HTTP for a more secure connection.
  + Web of Trust – Identifies sites which are not safe through the use of red, green, and orange icons.
  + Privacy Badger – Learns and blocks secret trackers and cookies. It also monitors third parties and ad networks.
  + uBlock Origin – Blocks ads from loading on a page and blocks trackers leading to a faster browser experience.
  + LastPass Password Manager – Creates and stores complicated and long passwords for all of your accounts based on predefined criteria set by you.
  + Disconnect – Visually shows you which sites are tracking you in real time and offers the ability to block these.
* Bitedefender Antivirus plus – Keeps a database of known malicious sites and software and can prevent these from loading on your machine.
* Express VPN – Encrypts your data and requests before they reach the internet. These are then sent to a VPN server before sending them to their online destination meaning sites cannot track your location.
* VirtualBox – Using a sandbox environment ensures that anything malicious that does manage to get through the above defences only has access to the sandboxed area.

There are many reasons why we are tracked by every click that we make. The most common of these being our visible IP address, cookies, and sign-ins. Our IP address allows parties to track where our device is on the internet, and because our homes usually use a single IP address, trackers can sometimes map our IP to our physical location. Most websites use cookies to track who we are and some other information about us that advertising networks use extensively. Signing in to any account is the easiest way sites track our activities. Most sites will also not allow you to access their content without an account, making it very easy to track their members when they are signed in. Unfortunately, it is not entirely possible to prevent being tracked completely when online. Information such as our IP address can always be traced back to us and many sites, whether malicious or not, have found ways around being blocked from using cookies.

**Part B**

The deep web is a term for websites and contents that are unidentifiable or not indexed by search engines. Sites on the deep web may be locked behind passwords, pay walls, security walls, or may just instruct crawlers not to list them. These sites can be thought of as being just below the surface of the web resulting in the name the deep web.

No special tools are required to access the deep web. It can be accessed using most browsers such as Chrome, Firefox, Safari and many others. We can use special search engines such as Ahmia or Torch to access deep web sites making it possible to reach sites out of bounds by regular search engines.

Many of the dangers associated with the deep web are similar to that of regular web browsing. Malicious software in the form of downloads, trackers, viruses and other common dangers are associated with the deep web. Because of this, it is advised to have a strong antivirus installed on your machine. The use of a VPN, ad blocker, and tracker blocker are also a good idea to have installed before accessing the deep web. It is completely legal to access the deep web and approximately 90% of sites can be thought of as being part of the deep web, but as of today it is unknown exactly how large the deep web is.