A website is a series of files, interconnected to turn text into images, and potentially animate and style them. The three main languages used to create websites are HTML, CSS, and JavaScript. HTML is used to turn text into images, so that they can be viewed in a web browser. CSS is used to style these HTML elements in much easier, cleaner way. JavaScript is used to animate HTML elements. For example, JavaScript is used to add functionality to dropdown menus, and it allows users to upload things to the website. By having all of these files stored locally on your computer, you have to leave your computer on to leave the server running, otherwise other people can’t access your website. Large websites like Facebook and Twitter have their own dedicated server computers that have the website’s files installed, so that anyone can access the website at anytime from anywhere. What I just described is a static website. These are websites in which every page stays the same. Say, for example, I created a static website with a homepage and a second page. They would contain the same content forever, unless I went into the code and changed it myself. Dynamic websites, such as news sites and Facebook, allow users to post information, and change their home pages accordingly. Although dynamic websites take much more time and effort to code, they have more functionality than standard static websites can ever have. Since accessing websites involves users sending their information to servers, there are several security risks that come along with the several joys of accessing websites. Man-in-the-middle attacks involve people intercepting data sent between a user and the server. These “men in the middle” can intercept really important data, such as bank account information. These people can also alter the information sent between the user and the server. For example, the hacker can intercept data from a transaction in a bank, and alter the information that the user is sending so that the user transfers more money, and the hacker can change the person to whom the user is sending money. However, this only applies to poorly secured websites. Most major websites use highly effective security measures. Strong passwords prevent hackers from brute-forcing websites on a regular computer. SSL prevents man-in-the-middle attacks. DAL prevents hackers from accessing the websites’ databases. The list goes on and on, however there are an infinitesimal amount of security measures that can possibly be taken to secure a website. Maintaining a website is almost like taking care of a baby – you have to be extremely cautious in exposing it to harm, however, in the long run, it all pays off, as you will end up with a well-developed website.

Sources:

<https://nycda.com/blog/how-the-internet-works/>

<https://rocketmedia.com/blog/static-vs-dynamic-websites>

<https://blog.sucuri.net/2015/05/website-security-how-do-websites-get-hacked.html>

<https://www.owasp.org/index.php/Man-in-the-middle_attack>

https://www.whitehatsec.com/blog/top-10-proactive-web-application-security-measures/