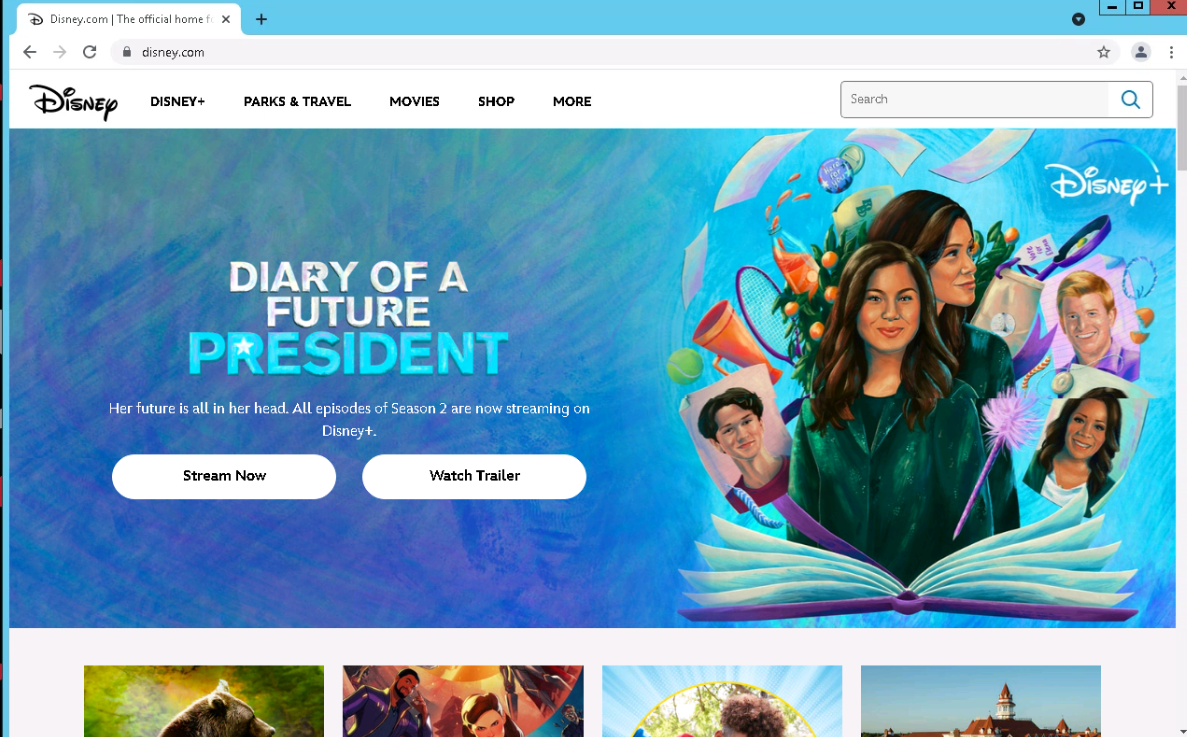
# Cybersecurity

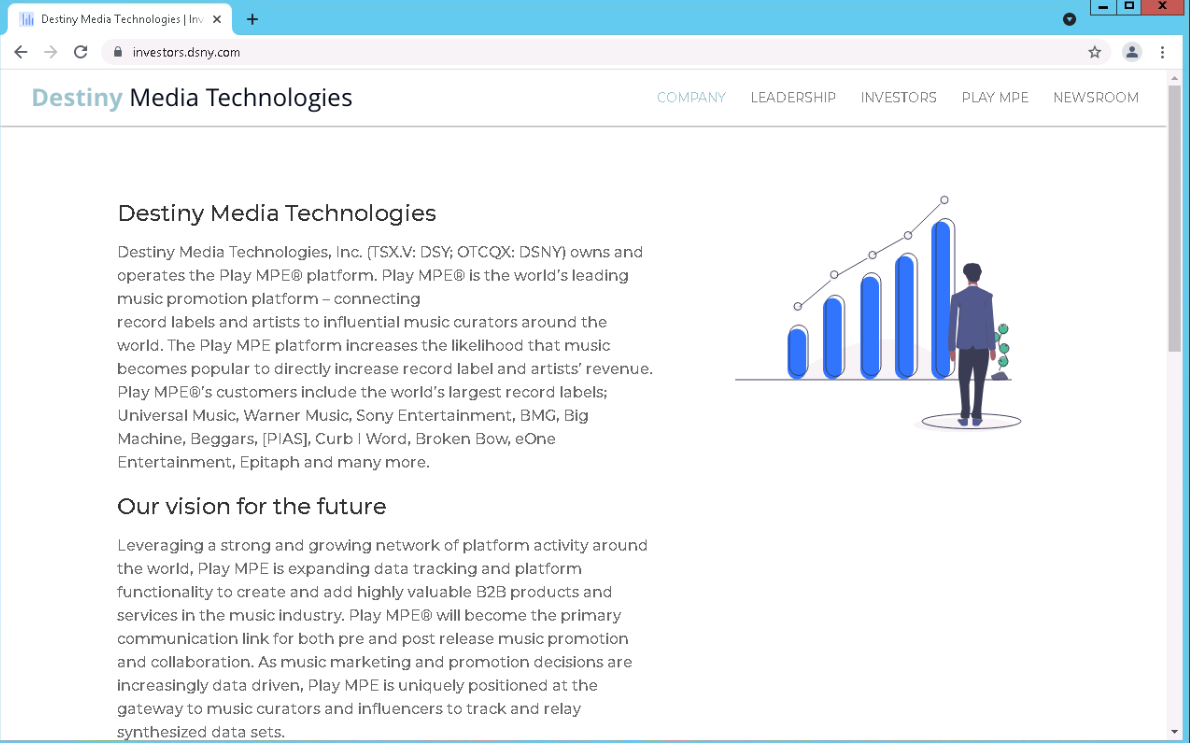
## Activity 1.2.4: Securing Your Browser

Copy and paste screenshots and/or answer questions from the activity.

#4 Screenshot of disny.com



#5 Screenshot of dsny.com



#9 What do you think are some types of sites that should always use HTTPS

Any site you perform purchases on or input personal information

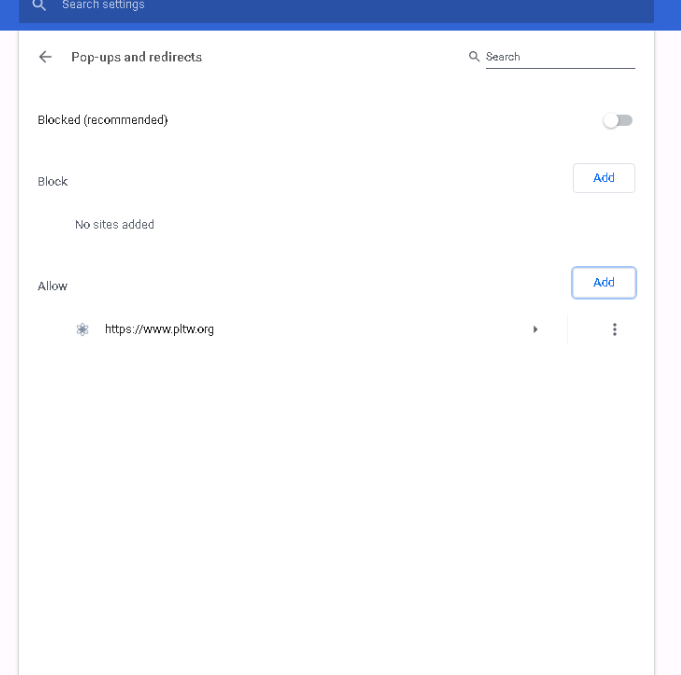
#14 What you think the Chrome settings should be for the following content types?

Location: Only while using

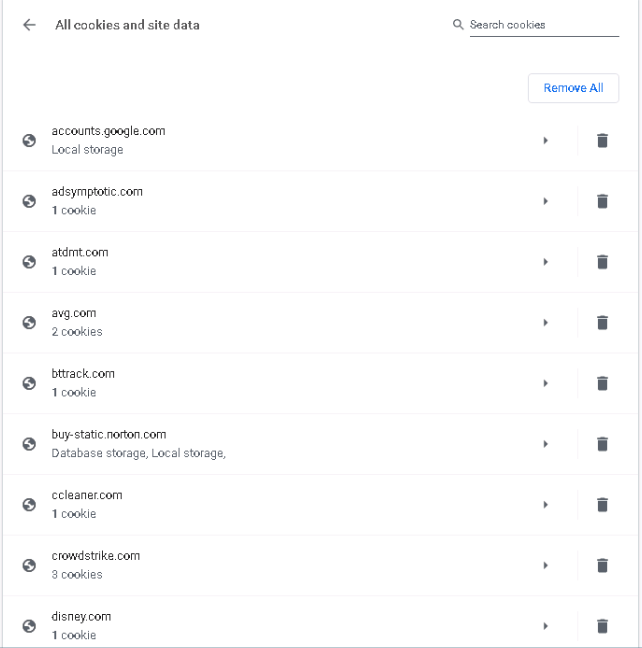
Camera: Only when asked

Flash: Only when asked

#18 Screenshot of settings

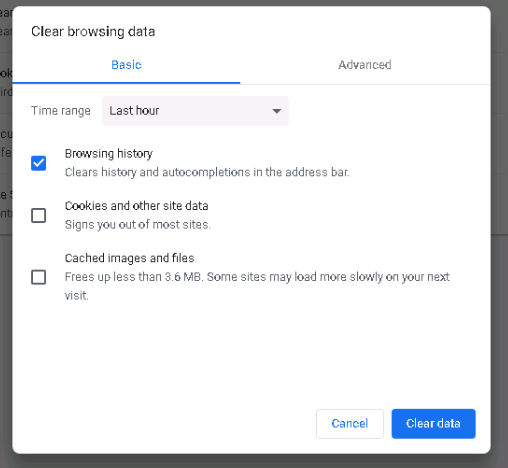


#21 Screenshot of settings



#26 What does the browser say will happen if you clear Browsing history? If you clear

cookies and other site data?



#28

|  |  |
| --- | --- |
| Not Saved or Visible | Saved and/or Visible |
| * Browsing history * Cookies and Site data * Information entered in forms | * Websites you visit * Your employers or schools * ISP |
|  |  |

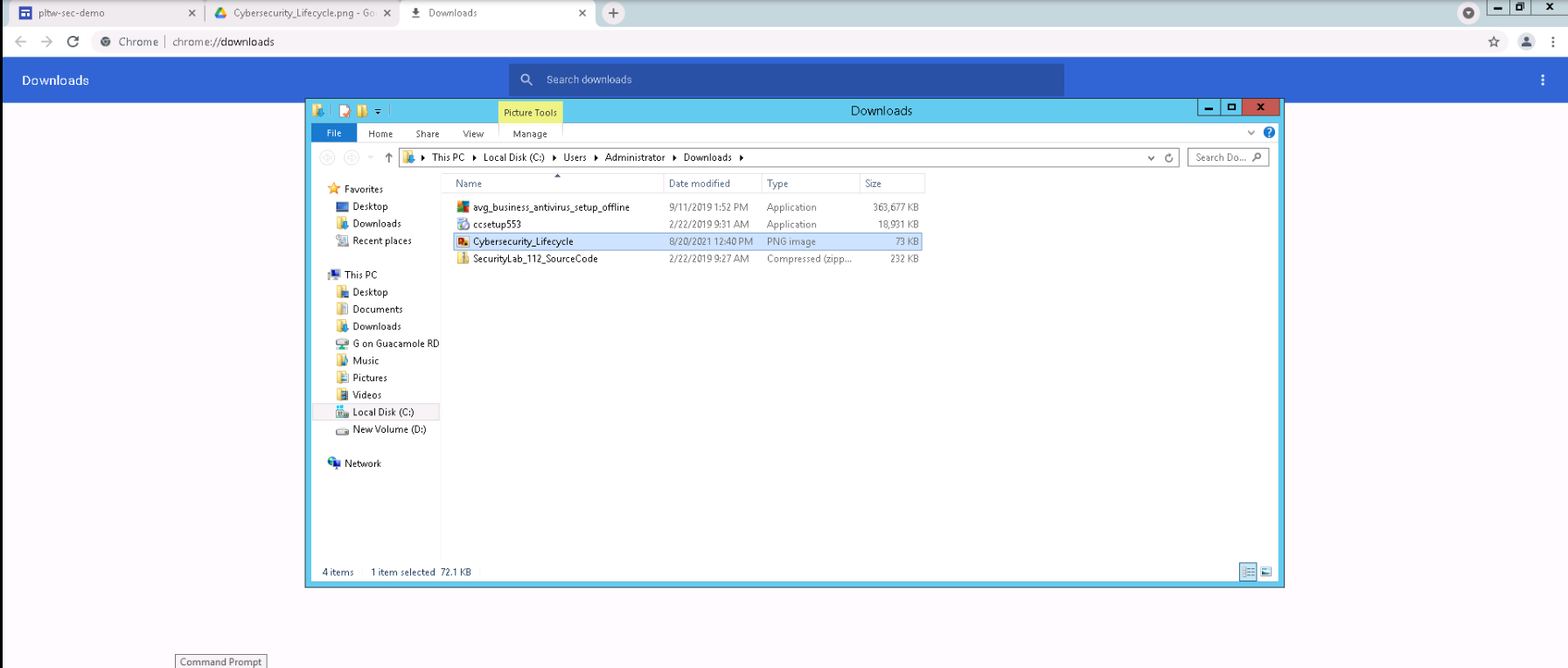
#36 Screenshot of error message



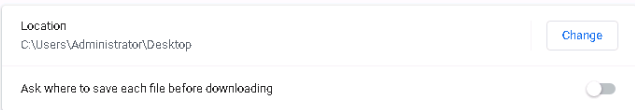
#37 Screenshot of certificate (add to your Computer Science Notebook)

See 36

#41 Record the location of the downloaded files



#43 Record this new location as shown in Chrome Settings



#45 Screenshot of downloaded file with file type visible



Conclusion Question #2-- How does having weak security on your browser represent the weakest link in a network?

“7” – Mr. Eaton