|  |  |
| --- | --- |
|  | CIS-1290 Principles of Information Security |

Topic 6 Assignment 2

|  |  |
| --- | --- |
| To: | Mike MacDonald |
| From: | Christopher Sigouin |
| Date: | March 7, 2015 |
| Subject: | Exercise 5. Examining the contents of security and privacy tabs in a browser |
|  |  |

In the following exercise I review the functionality and ability of a browser to handle content filtering and protection of unwanted items as described. Instead of using Internet Explorer I chose to review the browser Chromium. Chromium is an open source web browser project that Google Chrome is derived from, so there would likely be similarities in privacy and security options. The exercise description is below:

*Using a Microsoft Windows XP, Vista, or 7 system, open Internet Explorer. Click*

*Internet Options on the Tools menu. Examine the contents of the Security and Privacy*

*tabs. How can these tabs be configured to provide: (a) content filtering and (b) protec-*

*tion from unwanted items like cookies?*

**Content Filtering:**

Chromium has many options in its content filtering section located in “Settings”. The following below are main headings listed under content filtering. Each section has options that can be enabled via a radio button or checkbox in some cases. The options are described below the headings:

Cookies

Can allow all cookies (recommended), keep them until the browser closes, block all sites cookies and data, whitelist/blacklist specific URLs cookie data and search for specific types of cookies stored

Images

Ability to show all images, not show images at all or whitelist/blacklist specific URLs image data

JavaScript

Allow all sites to run JavaScript, not allow any site to run JavaScript or whitelist/blacklist specific URLs JavaScript ability to run on the browser

Handlers

Allow sites to be the default handlers for protocols ( ie. mailto: will open your email client or webcal: will add events to a calendar program ), not allow any site to handle protocols or manage each handler by specification

Plug-ins

Run all plug-ins automatically, click to play, block by default (but will allow to run if you manually run a plug-in), whitelist/blacklist specific URLs ability to run plug-ins

Pop-ups

Allow all sites to show pop-ups, not allow any pop-ups and whitelist/blacklist specific URLs ability to cause pop-ups

Location

Allows all sites to track your physical location, ask when a site tries to track, do not allow any site to track and whitelist/blacklist specific URLs ability to track

Notifications

Allow all sites to show desktop notifications, ask when a site tries to show a notification, do not allow any site to show notifications and whitelist/blacklist specific URLs ability to show notifications

Fullscreen

Whitelist/Blacklist specific URLs ability to allow a fullscreen effect

Mouse cursor

Allow all sites to disable the mouse cursor, ask when a site tries to disable it, do not allow any site to disable the mouse cursor and whitelist/blacklist specific URLs ability to disable the mouse cursor

Media

Allows what device to use for a Microphone / Camera is the website allows it. Can also specify to ask if a site requires the use of the devices, not allow any site to use them or whitelist/blacklist specific URLs ability to use them

Unsandboxed plug-in access

Allows all sites to use a plug-in to access your computer, ask when a site wants to use a plug-in for access, not allow any site to use a plug-in for access and whitelist/blacklist specific URLs ability to run plug-ins for access

Automatic Downloads

Allows all sites to download multiple files automatically, ask when a site downloads multiple files automatically, do not allow any sites to download and whitelist/blacklist specific URLs ability to download multiple files automatically

Zoom Levels

Shows any zoom levels set for specific websites

**Protection from unwanted items (i.e. Cookies):**

Two sections allow a user to protect themselves specifically from cookies within Chromium. The “Cookies” section under content settings as described above can manage the ability to accept them and keep their data.

Another option to manage them would be “Clear browsing data” which is located next to the content settings option. In this section a user can manually select what to remove from the browsers collected data and specify by the timeframe since the data was collected. One option is to remove cookies and other site and plug-in data, but other options are available as well including a popular one for removing browsing history.