IT Fundamentals

Unit - Networking

Lesson 3.5.1 - Web Browsers

IT Fundamentals Objectives (FC0-U61)

Objective 3.5 - Given a scenario, configure and use web browsers.

- Caching/clearing
- Deactivate client-side scripting
- Browser add-ons/extensions
    - Add
    - Remove
    - Enable/disable
- Private browsing
- Proxy settings
- Certificates
    - Valid
    - Invalid
- Popup blockers
- Script blockers
- Compatible browser for application(s)

Cyber Connections

- **Networks & Internet**

Grade Level(s)

8, 9

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Teacher Notes:

Web Browsers

What is a web browser? A ***web browser***, more commonly known as just a browser, is how user's are able to access the world wide web. A browser will get all the data and package it back for the user with the main purpose being a convenient way for someone to browse the web. These are very common in today's world, common browsers are Google Chrome, Firefox, Internet Explorer, Safari, etc. All web browsers can be configured and set-up in certain ways to benefit the user. This lesson focuses on these settings.

Cache and Scripting

Cache is a browser's way to store data from previously visited web pages. The purpose is to save time loading that same website when a user visits the page at a later date. An example might be an image that is always on a webpage, if it's stored in cache, the browser does not have to receive the data for that picture, but rather just load it from the cache. Sometimes the cache will store too much data and slow a browser down (and take up storage on a computer), so it needs to be cleared, or erased/emptied. Another reason to erase the cache is for privacy concerns, cache stores data from previously visited web pages, some people do not like having this data stored.

Another tool of a browser to save bandwidth is client-side scripting. This is code that needs to be executed on a website, but instead of executing this script through the web server, it's executed by the browser. This saves bandwidth by not having to send the executed data back and forth. The most common client-side scripting is JavaScript. If a user wants to, they can disable (deactivate) client-side scripting for the browser.

Add-ons

Almost every browser today allows add-ons (also known as extensions). This extends the ability of a web browser and allows it to do much more. An add-on can be a cache manager application that would allow a user to manage their cache easier. Ad blockers have become very common extensions for web browsers, these extensions can block advertisements from appearing on websites. The user has the ability to add and remove these extensions for their browser as well as the power to enable and/or disable them for periods of time and/or for certain websites.

Teacher Notes:

Incognito Mode

Browsers have the ability to start a temporary session that does not track the user's data. This is called ***private browsing***. When a user is using a private session, no cache is being stored, cookies are not being stored, browsing history is not tracked, etc. This does not mean that someone monitoring network activity can't see what this user is doing, it simply does not store the data in the browser. A user might notice that their accounts are not logged in to while in a private browsing mode because no data is being traced. A common use for this might be if a husband is searching for a gift for their wife. This would not leave a trail behind that the wife might accidentally stumble upon and spoil the surprise.

Proxies

Proxies are servers that network traffic is routed through. It's basically like connecting a computer through a different computer that processing the internet requests. Schools will implement proxy servers to prevent kids from accessing adult content websites. Some adults might do this in a home network as well to stop their children from stumbling upon malicious websites. Proxies are usually easy to set up in a browser's settings.

Certificates

How are we able to trust the websites that we stumble upon? Well, one major way is through certificates. ***Certificates*** are done through 3rd parties (that are trusted by the browser/user) to verify that a website can be trusted. If a certificate is valid, then the website can be trusted. If the certificate is invalid, that does not mean the website can not be trusted, but rather that it has not been checked by a third party and verified.

Blockers

Web browsers allow users to stop annoying pop-ups and scripts that could be malicious with blockers. A ***pop-up*** blocker does what it sounds like, it blocks the annoying pop-ups and/or gives the user the ability to close them. This is obviously for the convenience of the user. ***Script blockers*** can block scripts so malicious scripts can not run in the background without the knowledge of the user.

Teacher Notes:

Browser Compatibility

Not all browsers are built the same. Thus, websites and web applications have to have browser compatibility. This is to make sure that their websites and applications can be accessed and used across all browsers. Sometimes, certain websites will say that it can not be loading on a certain browser and/or the page loads better on one browser versus another.