10.3.9 Web Browser Security Facts

This lesson covers the following topics:

- Manage browser data
- Enhance browser privacy

Manage Browser Data

A *web browser* is an application for retrieving and displaying information on the internet. Web browsers present the possibility of security breaches into an organization's network. There are general actions and browser-specific actions you can take to help harden the network against attacks from the internet.

When using a browser, the following might indicate an unsecured connection or an attack.

- A web document with a URL that contains a new or different domain name than the site you intended to visit.
- A menu bar that includes new commands or is missing common commands.
- The status line of the browser displays an unlocked symbol when SSL should be in use.

Regardless of the browser you are using, clear your private data regularly. Private data can be cleared based on the data's age. You can clear data from the last few hours, the last few weeks, or all time. The type of browser you are using and the types of sites you have visited, will determine the type of data that can be cleared. Most browsers let you clear the following data:

- Browsing history
- Download history
- Cookies and other site data
- Cached images and files
- Passwords
- Autofill form data
- Site permissions
- Hosted app data

The following table lists steps for each browser to clear data.

Browser	Steps
Google Chrome	Steps for the Google Chrome browser are: 1. Select the ellipses (three dots) button on the menu bar. 2. Go to History > History. 3. Select **Clear browsing data**.
Microsoft Edge	Steps for the Microsoft Edge browser are: 1. Select the ellipses (three dots) button on the menu bar. 2. Go to History. 3. Select **Clear Browsing Data.**
Internet Explorer	

	Steps for the Internet Explorer browser are 1. Select the Tools (gear) icon from the menu bar. 2. Select Internet Options. 3. Go to Browsing history. 4. Select **Delete**.

Enhancing Browser Privacy

You can use the following browser settings and guidelines to enhance browsing privacy and security. These may be named and implemented differently in different browsers, but the general ideas are the same.

Settings	Description
Cookies	*Cookies* are text files that save information about preferences, browser settings, and web page preferences. They identify you (or your browser) to websites. Be aware of the following facts about cookies: ▪ Cookies aren't inherently malicious and are often necessary for e-commerce websites. ▪ The use of cookies can constitute a privacy violation because cookies can retain personal information. A hacker could gain access to this information. ▪ Cookies can be misused by malware to collect and report your web surfing activities. ▪ *First-party cookies* are cookies used by the site you are visiting. ▪ *Third-party cookies* are cookies placed by sites linked to the site you are visiting. For example, banner ads on a website might place cookies on the machine to identify ads already seen or ads opened. Secured environments should restrict the use of cookies on all web browsers and other internet service utilities. Cookies can usually be found in the user profile in the file system.
Cache	A *cache* is storage location for information that will be used again, such as images, sounds, web pages, and even usernames and passwords used on websites. In addition to taking up space, data in the cache could be retrieved by someone with access to the computer. To provide some level of protection, you should clear the web browser cache whenever you use a public computer to access the internet, especially when you have accessed sites for retrieving personal data.
Security	Enable the following options to increase security: ▪ Warn me when sites try to install add-ons. ▪ Block reported attack sites. ▪ Block reported web forgeries. It is best practice to always enter passwords and to not have the browser remember them. ▪ Do not select the **Remember passwords for sites** option. ▪ Do not select the **Use a master password** option. When you select this option, all passwords saved on the system are encrypted. You create a master password that retrieves and unencrypts passwords for individual sites.
Add-ons	An *add-on*, also known as a *plug-in* or *browser extension*, is a program that adds functionality and features to a web browser, including extra toolbars and interactive web content. Over time, a browser collects add-ons, some of which could have malicious intent. Secure the browser by reviewing add-ons and uninstalling items that are not appropriate for the environment.

	▪ *Disabling* an add-on disables it for the current user. This allows users to enable or disable add-ons based on their own needs. ▪ *Deleting* an add-on removes it from the system and prevents any user from using it.
General	General information for web browser security includes: ▪ Use the **Always ask me where to save files** option to avoid having files download without your knowledge. By using this option, you will always know when a file is being downloaded to the system. ▪ Enable the **Block Pop-up windows** option. ▪ Turn off **Remember search and form history**. Data you enter into forms, such as your banking account number, will be stored if this option is on. ▪ Turn off **Accept third-party cookies** or accept cookies and specify **ask me every time** so you will know when third-party cookies are created.