# 8.5.6 Internet Explorer Security Facts

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 your network against attacks from the Internet.

When using a browser, look for the following that might indicate an unsecured connection or an attack:

- The loading of a Web document with a URL containing 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 displaying an unlocked symbol when SSL should be in use.

Regardless of the browser you are using, clear your private data regularly.

The following browser settings and guidelines can be used to enhance the privacy and security of a system for browsing the web. These may be named and implemented differently in different browsers, but the general ideas are the same.

| Settings | Description |
|---|---|
| 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.<br>- *Disabling* an add-on disables it for the current user. This allows users to enable or disable add-ons based on their own needs.<br>- *Deleting* an add-on removes it from the system and prevents any user from using it. |
| Cookies | *Cookies* are text files that are stored on a computer to save information about your preferences, browser settings, and Web page preferences. They identify you (or your browser) to Web sites. Be aware of the following facts about cookies:<br>- Cookies aren't inherently malicious and are often necessary for e-commerce Web sites.<br>- The use of cookies can constitute a privacy violation because cookies can retain personal information and can be used by attackers to discover this information.<br>- Cookies can be misused by malware to collect and report a user's Web surfing activities.<br>- *First-party cookies* are cookies used by the site you are visiting.<br>- *Third-party cookies* are cookies placed by sites linked to the site you are visiting. For example, banner ads on a Web site might place cookies on your machine to identify ads you have already seen or ads you have clicked.<br>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. |
| Security | Enable the following options to increase security:<br>- Warn me when sites try to install add-ons.<br>- Block reported attack sites.<br>- Block reported web forgeries.<br>It is best practice not to have the browser remember passwords.<br>- Do not select the **Remember passwords for sites** option.<br>- Do not select the **Use a master password** option. When you select this option, all of the passwords saved on the system are encrypted. A user creates a master password that must be entered for the system to retrieve and unencrypt passwords for individual sites. |
| Cache | A *cache* is storage location for information that will be used again, such as images, sounds, Web pages, and even user names and passwords used on Web sites. In addition to taking up space, data in the cache could be retrieved by someone with access to your 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. |
| General | - 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.<br>- Enable the **Block Pop-up windows** option.<br>- 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.<br>- 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. |