Browser Hardening

Browser Hardening

In this reading, you will learn how to harden browsers for enhanced internet security. The methods presented include evaluating sources for trustworthiness, SSL certificates, password managers, and browser security best practices. Techniques for browser hardening are important components in enterprise-level IT security policies. These techniques can also be used to improve internet security for organizations of any size and for individual users.

Identifying trusted versus untrusted sources

Some cybercriminals monitor SEO search terms for popular software downloads. Then they create fake websites to pose as hosts for these popular downloads. They might even use advertising and stolen logos of trusted companies to make the sites appear to be legitimate businesses. However, the downloadable files available on the cybercriminals' websites are usually malicious software. Unaware of the deception, users download and install the malware. In some cases, the users don't even need to download a file. Savvy cybercriminals can design web pages that have the ability to infect users' devices simply upon visiting the sites.

To guard against threats like this, there are checks you can perform to evaluate websites:

- **Use antivirus and anti-malware software and browser extensions.** Run antivirus and anti-malware scans regularly and scan downloaded files. Ensure antivirus and anti-malware browser extensions are enabled when surfing the web.
- **Check for SSL certificates.** See the "Secure connections and sites" section below.
- **Ensure the URL displayed in the address bar shows the correct domain name.** For example, Google websites use the Google.com domain name.
- **Search for negative reviews of the website from trusted sources.** Be wary of websites that have few to no reviews. They may not have been active long enough to build a bad reputation. Cybercriminals will create new websites when they get too many negative reviews on their older sites.
- **Don't automatically trust website links provided by people or organizations you trust.** They may not be aware that they are passing along links to malicious websites and files.

- **Use hashing algorithms for downloaded files.** Compare the developer-provided hash value of the original file to the hash value of the downloaded copy to ensure the two values match.

Secure connections and sites

Secure Socket Layer (SSL) certificates are issued by trusted certificate authorities (CA), such as DigiCert. An SSL certificate indicates that any data submitted through a website will be encrypted. A website with a valid SSL certificate has been inspected and verified by the CA. You can find SSL certificates by performing the following steps:

1. Check the URL in the address bar. The URL should begin with the **https://** protocol. If you see **http://** without the “s”, then the website is not secure.
2. Click on the closed padlock icon in the address bar to the left of the URL. An open lock indicates that the website is not secure.
3. A pop-up menu should open. Websites with SSL certificates will have a menu option labeled “Connection is secure.” Click on this menu item.
4. A new pop-up menu will appear with a link to check the certificate information. The layout and wording of this pop-up will vary depending on which browser you are using. When you review the certificate, look for the following items:4
    a. **The name of the issuer** - Make sure it is a trusted certificate authority.
    b. **The domain it was issued to** - This name should match the website domain name.
    c. **The expiration date** - The certificate should not have passed its expiration date.

Note that cybercriminals can obtain SSL certificates too. So, this is not a guarantee that the site is safe. CAs also vary in how thorough they are in their inspections.

Password managers

Password managers are software programs that encrypt and retain passwords in secure cloud storage or locally on users’ personal computing devices. There are a wide variety of activities users perform online that require unique and complex passwords, such as banking, managing health records, filing taxes, and more. It can be difficult for users to keep track of so many different logins and passwords. Fortunately, password managers can help.

- **Advantages of using a password manager:**
    - It provides only one password for a user to remember;

- Can generate and store secure passwords that are difficult for cybercriminal tools to crack;
- Is more secure than keeping passwords written down on paper or in an unencrypted file on a computer; and
- Work across multiple devices and operating systems.

- **Disadvantages of using a password manager:**
  - It can expose all of the user's account credentials if a cybercriminal obtains the master password to the password manager;
  - Can be very difficult for a user to regain access to the password manager account if the master password is lost or forgotten;
  - Requires the user to learn a new method for logging in to their various accounts in order to retrieve passwords from the password manager software; and
  - Often requires a fee or subscription for password management services.

A few of the top brands for password manager applications include Bitwarden, Last Pass, and 1Password. Please see the Resource section at the end of this reading for more information.

Browser settings

Browser settings can be configured for additional safety measures. Some additional options for hardening browsers include:

1. Use pop-up blockers: Disable Web Browser Pop-up Blockers
2. Clear browsing data and cache: Clear your web browser's cache, cookies, and history
3. Use private-browsing mode: How to Turn on Incognito Mode in Your Browser
4. Sign-in/browser data synchronization:
   a. Turn sync on and off in Chrome
   b. Disable Firefox Sync
   c. Change and customize sync settings in Microsoft Edge
5. Use ad blockers: How to block ads

Key takeaways

You learned about multiple steps you can take to harden a browser and protect your online security:

- **Identify if sources can be trusted or not:**

    - Use antivirus and anti-malware software and browser extensions.
    - Check for SSL certificates.
    - Ensure the URL displayed in the address bar shows the correct domain name.
    - Search for negative reviews of the website from trusted sources.
    - Don’t automatically trust website links provided by people or organizations you trust.
- **Use a password manager**
- **Configure your browser settings:**
    - Use pop-up blockers.
    - Clear browsing data and cache.
    - Use private-browsing mode.
    - Sign-in/browser data synchronization.
    - Use ad blockers.

Resources for more information

To learn more about hardening bowsers for safer web surfing, please visit the following articles:

- Dubious downloads: How to check if a website and its files are malicious - Provides information on evaluating websites and downloads for the presence of malware.
- The Best Password Managers to Secure Your Digital Life - Compares and contrasts the top password managers on the market.
- Avoiding Social Engineering and Phishing Attacks - Tips for avoiding an array of internet scams.
- Blocking Unnecessary Advertising Web Content - From the United States National Security Agency Cybersecurity Information, notice about ad-blocking through network functions, at the host level, and other concerns.
- Securing Web Browsers and Defending Against Malvertising for Federal Agencies - From the United States Cybersecurity and Infrastructure Security Agency, guide for protecting computing systems from malvertising.
- Browser sync—what are the risks of turning it on? - Explains the security threats associated with having browsers set to synchronize account data across multiple devices.
- List of Participants - Microsoft Trusted Root Program - Microsoft’s list of trusted Certificate Authorities and the common names of the issued certificates