Browsers

Overview

Browsers such as Google Chrome, Microsoft Edge, Apple Safari, or Mozilla Firefox are one of the most common ways people interact with the Internet. We use them for reading the news, checking email, shopping online, watching videos, and playing games. As a result, browsers are also a target for cyber attackers.
Many people assume browsing online is safe if you only visit well-known, trusted websites. However, it is quite easy to accidentally click on or visit an unsafe web page, sometimes without even knowing it. In addition, the very websites you know and trust can be hacked, with cyber attackers installing malicious software on them. Finally, today's browsers have many new features, which often can be confusing, and if misconfigured, expose you to even more dangers.

Securely Leveraging Your Browser

Here are key steps to protecting yourself:

Updating: Always use the latest version of your browser. Updated browsers have the latest security patches and are much more secure. With today's computers this has become much easier as you simply enable automatic updating on your system. Or for some browsers you simply restart your browser whenever it tells you there is a new update. After an update, check for new security features from which you can benefit.

Warnings: Today's browsers can often recognize certain malicious websites designed to cause you harm. If your browser warns you that the website you are about to visit is dangerous, close your browser tab and find what you need on a different website.

Syncing: Never sync your work browser with your personal browser or any personal accounts. Syncing is when you enable browsers on different devices to talk to each other and share your browsing information, such as your browsing history, bookmarks, and saved content.

Passwords: Many browsers support the option of saving your passwords to different sites. Instead of storing your passwords in your browser, we recommend you use a dedicated password manager. Password managers are a separate security application that have far more security features and functionality.

Plug-ins: Plug-ins or extensions are small pieces of software added to browsers that can add functionality. However, each new plug-in you add can also add more vulnerabilities. For your work computer, only add plug-ins that are authorized and approved, and just like your browser, keep them updated. Remove plug-ins that you no longer need or use.

Privacy Mode: Most browsers offer a privacy option (also referred to as "incognito mode"). This means when you open a browser tab in privacy mode, you limit what information is collected about you. For example, your browser does not collect cookies, does not track browsing history, and will not store nor distribute sensitive information about you.

Live Chat: Some websites now offer a live chat feature where you can ask questions. Only engage in these online chats with known, trusted websites. In addition, limit the information you share during a live chat session, as you have no idea who is collecting your information, what they are doing with it, and to whom they may be selling it or sharing it.

Beware of Remote Control: Fraudulent websites will attempt to hack your computer by posting a fake security pop-up warning to your browser that your computer is infected and pressuring you for an online chat session to fix your computer. They will then urgently request that you allow them to install a remote agent to allow them to fix your computer. In reality your computer is just fine. Instead, they are attempting to trick you into installing malicious software so they can steal your passwords and your data, and track all of your online activity.

Log Off: When you are finished visiting a website, be sure to log off to remove sensitive login and password information before closing the browser.

Guest Editor

Dean Parsons is the CEO of ICS Defense Force, with over 20 years IT/ICS cyber defense experience. He is also a Certified SANS instructor for ICS515 and co-author / instructor of ICS418, teaching active cyber defense, incident response, leadership and risk management for industrial control systems. www.linkedin.com/in/dean-parsons-cybersecurity.

Resources

Password Managers: https://www.sans.org/newsletters/ouch/password-managers/
Updating: https://www.sans.org/newsletters/ouch/the-power-of-updating/
Social Engineering: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Protecting Your Digital Footprint: https://www.sans.org/newsletters/ouch/privacy/