State of Oklahoma

Monthly Security Tips NEWSLETTER

February 2012 Volume 7, Issue 2

Securing Your Web Browser

From the Desk of CPT Jeff Elliott, Oklahoma Office of Homeland Security

What is a web browser?
The web browser is a software application that allows you to view and interact with content on a webpage, such as text, graphics or other material. Internet Explorer, Firefox and Safari are some of the most commonly used browsers. Plug-ins, also known as add-ons, are applications that extend the functionality of browsers. Some of the plug-ins you may be familiar with include Flash Player, Java, Media Player, QuickTime Player, Shockwave Player, RealOne Player and Acrobat Reader. Certain plug-ins may be required to view content depending on how a web page is designed.

Web browsers—and related plug-ins—are primary tools for interacting with the Internet, making them prime targets for cyber attacks. It is important to understand the risks and know what steps you can take to help minimize the likelihood of a successful attack.

Keep in mind that mobile devices also utilize web browsers. As the use of mobile devices increases, these devices may also become targets of browser-based attacks.

How can your web browser be attacked?
Without the appropriate security patches applied, web browsers are as vulnerable to attack or exploit as other software. A fully patched web browser can still be vulnerable to attack or exploit if the browser plug-ins are not updated. It's important to remember that plug-ins are not automatically updated when the browser is patched.

Cyber attackers are constantly searching for and finding programming errors and other flaws in web browsers and associated plug-ins. These vulnerabilities can be exploited, giving cyber criminals access to—and sometimes control over—your computer system.

Browser-based attacks can also originate from websites due to poor security coding of web applications or vulnerabilities in the software that supports websites. Attackers have been successful in compromising large numbers of trusted websites to deliver malicious applications to unsuspecting visitors. Attackers are then able to add scripts to a compromised website so that the website's appearance does not change. These scripts may "silently" redirect you to another website without you even knowing about it. This redirection to another website may cause malicious programs to be downloaded to your computer. These programs are often designed to allow remote control of your computer by the attacker and to capture personal and confidential information such as credit card numbers, banking information and other data used for identify theft.

What can you do to protect against web browser attacks?
Below are a number of key steps you can take. Your information technology department and security office may have these implemented in your organization's environment, but we encourage you to also apply these steps to your home computers/devices. This is especially critical if employees access their work network from their home computer.

- Keep your browser(s) updated and patched, and set to auto update.

- Keep your operating system updated and patched.
- Use anti-virus and anti-spyware software and keep them updated.
- Install a firewall and keep it updated and patched.
- Keep your applications (programs) updated and patched, particularly if they work with your browser (such as multi-media programs and plug-ins used to enable running of videos, for example)
- Block pop-up windows, as this may help prevent malicious software from being downloaded to your computer. (Note that the process for blocking varies depending on the browser you are using. Please refer to the links below for specific details.)
- Consider disabling JavaScript, Java, and ActiveX controls when not being used. Activate these features when necessary.

Please note, a number of these tips may impede your use of the Internet or limit what content you can access. If you find that you need ActiveX controls or you require JavaScript be enabled, set your browser to prompt you before running scripts.

To learn more about web browser attacks visit:

- US-CERT Security Tip: www.us-cert.gov/cas/tips/ST05-001.html
- Carnegie Mellon CERT: Securing Your Web Browser: www.cert.org/tech_tips/securing_browser/
- McAfee -- Web Browsers: An Emerging Platform Under Attack: www.mcafee.com/in/resources/white-papers/wp-web-browser-emerge-under-attack.pdf

To learn more about web browser security settings, please visit:

- Qualys Browser Check: https://browsercheck.qualys.com/
- Firefox – Check Your Plug-In: www.mozilla.org/en-US/plugincheck/
- Firefox Browser Security: www.mozilla.org/en-US/firefox/features/#advancedsecurity
- Google Chrome and Browser Security: www.google.com/chrome/intl/en/more/security.html
- Internet Explorer 9 Security Settings: www.microsoft.com/security/pc-security/ie9.aspx
- Safari Security and Privacy: www.apple.com/safari/features.html#security

For more monthly cyber security newsletter tips, visit: www.msisac.org/awareness/news/

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Brought to you by:

MS-ISAC
MULTI-STATE Information Sharing & Analysis Center™
A DIVISION OF CENTER FOR INTERNET SECURITY