The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Staying Current
- Plugins and Add-Ons
- Security Features
- Privacy

Browser Security and Privacy

GUEST EDITOR

Mike Poor is the guest editor for this issue. He is a senior security analyst for the consulting firm InGuardians Inc. (www.inguardians.com). Mike is also a senior instructor for the SANS Institute and the track lead for one of SANS' top courses, SEC503: Intrusion Detection In-Depth.

OVERVIEW

Your Internet browser, such as Internet Explorer, Firefox, Chrome, or Safari, is one of the primary tools you use to interact with the Internet. Cyber attackers know this, which makes your browser one of their primary targets. Also, your browser may collect a great deal of personal information about you that you may not be aware of. In this newsletter we cover the steps you can take to protect both your computer and your privacy.

KEEPING YOUR BROWSER CURRENT

The first step to protecting yourself is always using the latest version of your browser. It does not matter which browser you use; what is important is that you use the most recent version of your browser. Cyber attackers are constantly searching for, and finding, programming errors and other flaws in browsers. These mistakes (often called vulnerabilities) can be exploited, giving attackers access to, and sometimes even complete control, over your system. The companies that developed your browser (such as Microsoft, Google, or Apple) release patches to fix these vulnerabilities. By always having the latest version, you ensure your browser has these known issues fixed. To ensure your browser is updated, make sure the auto-update feature is always enabled in your browser and operating system. Some browsers, such as Chrome, automatically update themselves every time you restart the browser.

PLUGINS AND ADD-ONS

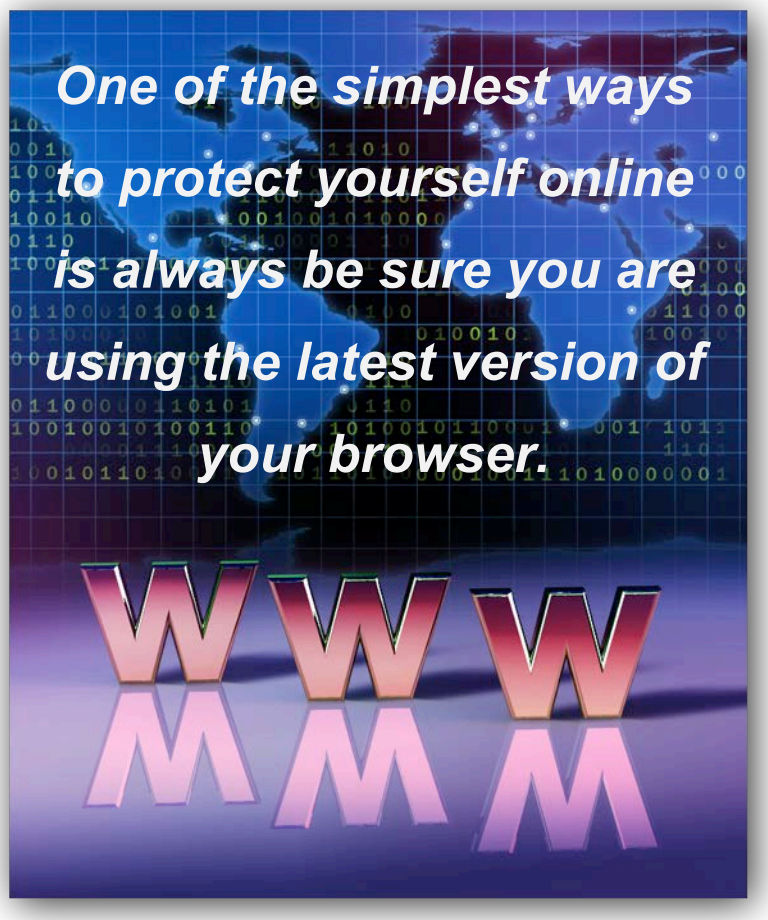
Plugins (sometimes called Add-Ons) are additional programs you can install in your browser. The problem with these additional programs is they can expose you and your system to greater risk. Each program you add to your browser has its own unique vulnerabilities or weaknesses.

Browser Security and Privacy

Install only the plugins you absolutely need and be sure you download them from well known, trusted sites. At times a website may ask you to install a plugin. Be careful -- these can be attempts to fool you to install infected software. When possible, always download and install a plugin from the original vendor's site. For example, always download or update your Flash player from the Adobe site www.adobe.com. Once you have installed a plugin you have to ensure that you keep it up to date, just like your browser. This can be challenging as many plugins have no automatic updating capability; you have to manually check and update them yourself. If that is the case, we recommend you check the status of your browser plugins at least once a month. In the resources section are several trusted websites that will help you do this.

SECURITY FEATURES

Each browser has its own unique security features. Be sure to take a moment and review your browser's security preferences or options. A key feature that almost all browsers support is warning you when you visit potentially malicious websites. Your browser maintains an updated list of thousands of known websites that are malicious or attempt to harm people. If you attempt to visit any of these known malicious websites, your browser will stop you and present a warning banner. When you get a warning banner do not proceed to the site. Keep in mind, though, you still always have to be careful about the websites you visit. Your browser cannot keep up with cyber criminals; it will not know all sites that are malicious.



PRIVACY

You may not realize it, but your browser may store a great deal of information about your online activities, including cookies, cached pages, and history. Cookies are small data files that websites send to your browser and can make using the web easier, such as storing your preferences. But cookies also allow companies to track your movements across the web. Cached pages are stored copies of websites you have recently visited. They are used to improve your system's performance but also might be accessed by unauthorized users. Finally, many browsers save the history of all the websites you have visited to take you more quickly to the websites you visit the most.

© The SANS Institute 2011

Browser Security and Privacy

To protect your privacy you can disable some or all these features. In addition, some browsers support the ability to manually erase any stored data, or automatically erase stored data every time you close your browser. Finally most browsers support a privacy mode where all data collection is turned off, including caching, cookies, and history. This ensures no information is collected about your browsing activities; however, this can also limit your ability to interact with some sites. Check your browser's privacy settings to change any of these features.

Finally, whenever possible make sure your browser connections are encrypted. This helps ensure your online activity cannot be monitored or captured. Encrypted connections are often called HTTPS. For example, sites such as Twitter, Facebook, and Google allow you to set your personal settings to ensure you are always using HTTPS (encryption) when communicating to these sites. In addition, whenever banking or shopping online, make sure your connections are encrypted. To confirm this, look for https:// in the browser and a lock.

RESOURCES

Some of the links shown below have been shortened for greater readability using the TinyURL service. To mitigate security issues, OUCH! always uses TinyURL's preview feature, which shows you the ultimate destination of the link and asks your permission before proceeding to it.

Browser Plugin Check:
http://preview.tinyurl.com/3m9gjr5

Firefox Plugin Check:
http://preview.tinyurl.com/3ojhl69

Chrome Browser Security:
http://preview.tinyurl.com/36sgakv

Internet Explorer 9 Security:
http://preview.tinyurl.com/3ly6wyv

Safari Browser Security:
http://preview.tinyurl.com/aesqpl

Firefox Browser Security:
http://preview.tinyurl.com/6ee3kx6

LEARN MORE

Subscribe to the monthly OUCH! security awareness newsletter, access the OUCH! archives, and learn more about SANS security awareness solutions by visiting us at http://www.securingthehuman.org

OUCH! is published by the SANS Securing The Human program and is distributed under the Creative Commons BY-NC-ND 3.0 license. Permission is granted to distribute this newsletter as long as you reference the source, the distribution is not modified and it is not used for commercial purposes. For translating or more information, please contact ouch@securingthehuman.org.

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Carmen Ruyle Hardy