SANS OUCH!

SANS Institute Security Newsletter for Computer Users

November 2010

Get security advice online at: http://www.sans.org/newsletters/ouch/updates/

In This Issue:

[Editor's Note: (Wyman) The publication of the November OUCH! was delayed. We apologize for any inconvenience this may have caused.]

Browser Safety

What is a web browser? Everybody uses a web browser to access the Internet. That fact alone makes the web browser a tempting target for Bad Guys who want to take over your computer and use it for their own nefarious purposes by installing malicious software, or "malware."

Why is important for me to know about malware? In the past, a user had to take some specific action, like opening an email attachment, for their computer to become infected with malware. Lately, simply visiting a website can cause your computer to become infected. This type of "drive-by download" is accomplished using features built into web browsers that allow them to run scripts. Scripts are really small computer programs that normally do useful things, like display a video, allow you to choose from a menu and maintain a shopping cart, among others. Unfortunately, scripts can also be used to install malware on your computer without your knowledge or consent.

What can I do to keep my browser safe? We have assembled a variety of measures and tools that you, the computer user, can use to make your web browsing experience safer by limiting the impact of scripts and helping you to avoid potentially harmful websites.

How much will it cost? All of the suggestions can be implemented at no cost.

What's the downside? We will look at how each recommendation can negatively impact your browsing experience.

General Browser Security Tips

Keep your browser up-to-date. The Bad Guys are constantly identifying new vulnerabilities and weaknesses in browsers and browser makers are constantly releasing updates to fix them. Running the latest version of your browser ensures that you have the benefit of the latest security technology. If you have concerns or questions about upgrading or run into a compatibility problem, contact IT at the office or your computer support provider.

Be careful about browser plug-ins. Plug-ins are browser extras--small, downloadable programs that add functionality to your browser. When you browse to a website, you may receive a message onscreen that in order to work with the site, you have to download and install a browser plug-in. "Just click here." But think before you click. Remember that any software you install will need to be updated, and may contain security vulnerabilities. Do you know that this website and the plug-in are trustworthy? If you don't know or aren't sure, don't click. Do you really need that plug-in? The fewer plug-ins you have installed, the safer your browser will be.

Check that your browser and plug-ins are up-to-date. Qualys has published a website that will do a quick check on your browser to help you identify common security issues. Visit https://browsercheck.qualys.com/ and install the plug-in (Yes, this one's safe!). Then click the "Scan Now" button. Note that Javascript is also required. An onscreen report tells you whether or not your browser and commonly installed plug-ins are up-to-date and provides you with a convenient way to update any found to be out-of-date.

Consider using Web of Trust (WOT). The Web of Trust is a cooperative venture that warns users of potentially dangerous websites. When you do a Google search, a circular indicator will appear next to each search result that has been rated by the service. Red indicates a site that is probably dangerous, yellow a potentially dangerous site, and green a site that is probably safe to use. Once you've logged in to a website, the same indicator appears in the title bar of the browser. Keep in mind that WOT ratings are based on votes cast by members of the Internet community, and while not necessarily authoritative, can provide useful information about websites to avoid. More information: http://www.mywot.com/

Tips for Internet Explorer

Microsoft's Internet Explorer (IE) is one of the most commonly used browsers. Protect your computer by running the latest version whenever possible. Right now that's IE8. If upgrading to IE8 is not possible, here are some tips for improving the security of IE7.

#1. Prevent Data Execution (DEP): Bad Guys exploit vulnerabilities in IE to infiltrate your computer with malware masquerading as data. Microsoft has published a "Fix It" site to turn on Data Execution Prevention (DEP) for IE7 at http://support.microsoft.com/kb/2458511#FixItForMeAlways
Click the button marked "Enable the application compatibility database."
Note: The DEP fix is not needed for IE8 and later versions.
Ease of implementation: Moderate
Impact on browsing: Minimal

#2. Turn on the Phishing Filter: Microsoft includes a Phishing Filter in IE that detects when a website is not exactly what it appears to be. If the site you are visiting is on the list of reported phishing websites, IE will display a warning web page and a notification on the address bar. From the warning web page, you can continue or close the page. If the website contains characteristics common to a phishing site but isn't on the list, IE will notify you in the address bar that it might be a phishing website.
You can turn on the Phishing Filter from the Tools menu in IE.
More Information:
https://www.microsoft.com/mscorp/safety/technologies/antiphishing/at_glance.mspx
Ease of implementation: Moderate
Impact on browsing: Minimal

#3. Increase IE Security Settings: The Internet Options menu in IE contains a Security tab that gives you a great deal of control over the behavior of IE when you visit a website. The default setting of "Medium-high" for the Internet Zone will prompt you before downloading any content that IE assesses as unsafe. By changing this setting to "High," you can effectively block all scripts from running on any web page you visit. While this is the safest possible setting, it can severely impact the performance of a website. To allow scripts to run on sites you trust, you can add them to the Trusted Sites Zone, one site at a time or whole domains at once using a wildcard (*). For example, entering http://*.sans.org would allow you to browse the entire SANS website without any prompts.
More Information: http://support.microsoft.com/kb/174360
Ease of implementation: Difficult
Impact on browsing: Severe

Tips for Firefox

The comments and suggestions below relate specifically to Firefox 3.6, the current version. The security suggestions below take the form of "Add-ons" that are downloaded and added to Firefox using the Tools menu.

#1. NoScript: This add-on blocks scripts from running in Firefox. When you visit a website that wants to run scripts, NoScript will display a warning at the bottom of the screen, and give you the opportunity to allow scripts to run on a temporary or permanent basis. Not allowing the scripts to run can severely impact the performance of many web pages. After you have used NoScript for a while, it will learn about the web pages you visit frequently and will not be as "pesky."
More information: http://noscript.net/
Ease of implementation: Moderate
Impact on browsing: Moderate to severe

#2. HTTPS Everywhere: You are probably familiar with HTTPS from using encrypted secure sites like those for online banking. Many websites offer some limited support for encryption over HTTPS, but make it difficult to use. HTTPS Everywhere attempts to make a secure connection to many of the most popular sites on the Internet even if you don't specifically ask for it. If it fails to make a secure connection, it defaults to an unencrypted HTTP connection and your browser continues to function as if nothing had happened.
More information: https://www.eff.org/https-everywhere
Ease of implementation: Moderate
Impact on browsing: Minimal

#3. Adblock Plus: Adblock Plus is an extension for Firefox, Thunderbird, and several other applications with the primary goal of removing advertisements. It works by comparing ads that are about to be displayed with a set of filters that describe undesirable advertising. When you install Adblock Plus, it sets up a subscription to a basic set of filters that will meet the needs of most users. Many additional sets of filters are available for your use.
More information: http://adblockplus.org/en/
Ease of implementation: Moderate
Impact on browsing: Moderate

Patches and Updates Roundup

Operating Systems/Applications

Windows & PC Office: http://update.microsoft.com & http://www.microsoft.com/security/updates/bulletins/201009.aspx

Mac Office: http://www.microsoft.com/mac/help.mspx?CTT=PageView&clr=99-0-0&ep=7&target=ffe35357-8f25-4df8-a0a3-c258526c64ea1033

OS X: http://support.apple.com/kb/HT1338

iPad: http://www.ehow.com/how_6256127_update-restore-apple-ipad.html

iPhone, iPod & iPod touch: http://support.apple.com/kb/HT1414

iPod: http://support.apple.com/kb/HT1483

Windows Adobe Reader: http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Windows

OS X Adobe Reader: http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Macintosh

Flash Player: http://get.adobe.com/flashplayer/

Firefox: http://www.mozilla.com/en-US/firefox/update/

Safari: http://www.ehow.com/how_2033324_update-safari.html

Opera: http://www.opera.com/

Chrome: http://www.google.com/support/chrome/bin/answer.py?hl=en&answer=95414

Java: http://www.java.com/en/download/manual.jsp

Windows iTunes: http://www.ehow.com/how_2016273_update-itunes-pc.html

OSX iTunes: http://www.ehow.com/how_2016270_update-itunesmac.html

Security Suites

Symantec: http://service1.symantec.com/SUPPORT/sharedtech.nsf/docid/2002021908382713

Norton: http://www.symantec.com/business/security_response/definitions/download/detail.jsp?gid=n95

McAfee: http://www.mcafee.com/apps/downloads/security_updates/dat.asp

Kaspersky: http://www.kaspersky.com/avupdates

AVG: http://free.avg.com/us-en/download-update

Panda: http://www.pandasecurity.com/homeusers/downloads/clients/

PC Tools: http://www.downloadatoz.com/pc-tools-internet-security/smart-update.html

BitDefender: http://www.bitdefender.com/site/view/Desktop-Products-Updates.html

Avast: http://www.avast.com/download-update

Webroot: http://support.webroot.com

Trend Micro: http://esupport.trendmicro.com/Pages/How-to-update-Trend-Micro-Internet-Security-Pro-2010.aspx

Microsoft Security Essentials:
http://www.microsoft.com/security/portal/Definitions/HowToMSE.aspx

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzer, Alicia Beard, Alan Paller
Email: OUCH@sans.org
OUCH! Security Information Service: http://www.sans.org/newsletters/ouch/updates/
Download the formatted version of the OUCH!: https://www.sans.org/newsletters/ouch