



Cyber-Security Newsletter

January 2009

STEPHEN F. AUSTIN STATE UNIVERSITY

INFORMATION TECHNOLOGY SECURITY OFFICE

Web Browsers & Pop-Ups

A web browser is a software application that allows the user to view and interact with content on a webpage. There are a number of different web browsers-- Internet Explorer, Firefox, Opera, and Safari are the most prevalent. Plug-ins, also known as add-ons, are applications that extend the functionality of browsers. Some of the more familiar plug-ins include Flash Player, Java, Media Player, QuickTime Player, Shockwave Player, RealOne Player and Acrobat Reader. Based on how a web page was designed, certain plug-ins, may be required to view some content.

We've all experienced Pop-up windows, or "pop-ups," while browsing the Internet. Pop-ups may appear without any interaction or prompting by the end user. They can be innocuous, such as when used for advertising, but they can be used for malicious purposes as well. This tip will discuss what pop-ups are and what you can do to keep them from affecting the security of your computer and data.

How Can Your Browser Put You At Risk?

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

Traditionally, browser-based attacks originated from "bad" websites but due to poor security coding of web applications or vulnerabilities in the software supporting web sites, attackers have recently been successful in compromising large numbers of trusted web sites to deliver malicious payloads to unsuspecting visitors.

Hackers add scripts that do not change the website's appearance. These scripts may "silently" redirect you to another web site without you even knowing about it. This redirect to another web site may cause malicious programs to be downloaded to your computer. These programs are generally designed to allow remote control of your computer by the attacker and to capture personal information, often related to obtaining credit card, banking information and data used for identify theft. Ensure you are using the most secure version of your web browser.

What are Pop-Ups?

Pop-ups are often used for advertising, to entice you to click on the pop-up ad. Pop-ups can also be used in other ways, such as on a "Help" section of an online form. The pop-up can be read without interfering with the form or page you are already visiting. This technique, for example, could be used on banking or ecommerce sites so as to not interfere with the current transaction or form request.

Occasionally you may encounter a "pop-under" which instead of opening on top of whatever website you are viewing it will open underneath the current web page. That way when you close your browser window you'll be greeted with an unexpected window.

While there are legitimate uses for pop-ups, they can also be used maliciously to entice you to click the pop-up window, which then downloads spyware or malicious code without your knowledge. These kinds of pop-ups often claim to "detect a virus on your computer" or claim to be a "spyware alert!" or offer a "free product" such as laptop or an anti-virus program.

Usually pop-ups are executed through JavaScript, a very popular way of adding content to websites. They can also be executed through online flash programs, though these are more difficult to stop.



Web Browsers & Pop-Ups—What to do?

What Can You Do To Protect Yourself From Browser Attacks and Pop-Ups?

- Keep your browser(s) updated and patched.
- Keep your operating system updated and patched.
- Use anti-virus and antispyware software and keep them up to date.
- Keep your applications (programs) updated and patched, particularly if they work with your browser such as multi-media programs used for viewing videos.
- Install a firewall between your computer and the Internet and keep it updated and patched.
- Block pop-up windows, some of which may be malicious and hide attacks. This may block malicious software from being downloaded to your computer.
- Tighten the security settings on your browsers. Check the settings in the security, privacy, and content sections in your browser. The minimum level should be medium. Consider disabling JavaScript, Java, and ActiveX controls.
- Never click inside the pop-up window to close it, even if it has a button or tab that says “Close,” “No Thank You,” or anything else. Instead, either click on the “X” at the top right corner of the title bar, or depending on your browser or operating system you can hold down the “Alt” key then press “F4” to close the currently opened window.

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 really need ActiveX controls or you require JavaScript be enabled, set your browser to prompt you before running scripts. If you find that you need to lower your security settings to be able to access what you need, lower them temporarily, then reset them.

Check Your Credit Card or Bank Statements

Many Reporting Mysterious Tiny Charges on Credit Card Statements (January 11 & 12, 2009): According to numerous postings at online forums, people have begun finding US \$0.25 charges on their credit card bills; the charges appear to come from companies called Adele Services and GFDL. There are two possible explanations. First, thieves could be testing the validity of stolen credit card information, and second, thieves could be trying to make money by stealing tiny amounts from millions of people. Credit card holders are urged to check their statements for suspicious charges. (*SANS NewsBites January 13, 2009 Vol. 11, Num. 3*)

http://www.boston.com/business/personalfinance/articles/2009/01/11/mysterious_credit_card_charge_may_have_hit_millions_of_users?mode=PF

http://voices.washingtonpost.com/securityfix/2009/01/tiny_charges_often_precede_big.html?wprss=securityfix

Last Words—Remote Access & Your Responsibilities



Over the winter break, many remotely accessed the network through the Cisco VPN Client or dialup. As a reminder, it is the responsibility of the University employees and contractors with remote access privileges to the University's network to ensure your remote access connection is given the same consideration as your on-site connection to the University network. General access to the Internet for recreational use by immediate household members through the University Network on personal computers is allowed. However, the University employee or contractor is responsible to ensure the family member does not violate any University policies, does not perform illegal activities, and does not use the access for outside business. The University has received infringement notices for copyright violations. Remote access users bear the responsibility for the consequences should the access be misused. Any machine or device connecting to the University internal networks via remote access methods must use the most up-to-date anti-virus software (which can be downloaded under mySFA) and be patched with latest software updates. The current version of the Symantec Anti-Virus Enterprise Edition is version 10.x and the virus definitions should not be more than 7 days old. In

addition, it is recommended to use Secunia Online Software Inspector (www.secunia.com) to inspect your home pc or laptop for insecure versions and missing security updates on a regular basis. Personal equipment that is used to connect to University's networks must meet the same requirements of University-owned equipment for remote access.

Email your topic suggestions, questions, and comments to itsecurity@sfasu.edu

