SOPHOS

The 10 myths of safe web browsing

Are you suffering from misconceptions about safe web browsing? You might think you're being safe, but with a newly infected webpage discovered every few seconds, it's next to impossible to stay up to date on infected sites—no matter how educated or aware of the risks you are.

To start this assessment, ask yourself some questions.

Do you and your users practice safe web browsing? Avoid risky sites? Limit time spent online during work hours? Employ a rock-solid internet access policy? Use a secure browser? Have the experience to know a risky site when you see one?

If you answered "Yes" to any of these questions, you need to read the rest of this report.

By Chris McCormack, Product Marketing Manager, Sophos

A Sophos white paper

May 2010

The 10 myths of safe web browsing

Are you suffering from misconceptions about safe web browsing? You might think you're being safe, but with a newly infected webpage discovered every few seconds, it's next to impossible to stay up to date on infected sites—no matter how educated or aware of the risks you are.

To start this assessment, ask yourself some questions.

Do you and your users practice safe web browsing? Avoid risky sites? Limit time spent online during work hours? Employ a rock-solid internet access policy? Use a secure browser? Have the experience to know a risky site when you see one?

If you answered "Yes" to any of these questions, you need to read the rest of this report.

You are likely suffering from one or more common misconceptions about web security. But don't worry—you are not alone. In the last several years, a lot of misinformation has circulated on both the extent of the risks and what it takes to protect yourself. Some might just eliminate internet access altogether, but cutting yourself off from the Web 2.0 world just isn't practical because it has become a mission critical tool in today's business. Establishing a strict "walled perimeter" with a well-controlled and locked-down internet access policy is not the right solution either. Users will easily bypass it.

Take a quick read through this document. If any of these myths or misconceptions resonates with you, it's time to revisit your web security solution. And take heart in the knowledge that there is a solution.

Myth #1: The web is safe because I've never been infected by malware

You may not even know you're infected. Many web malware attacks are designed to steal personal information and passwords or use your machine for distributing spam, malware or inappropriate content without your knowledge. For example, one Sophos customer recently installed a Web Appliance at its network gateway and immediately flagged more than 50 machines on its network for suspicious behaviour—calling home to a malware network for further instructions.

Myth #2: My users aren't wasting time surfing inappropriate content

Without any kind of web filtering, you really have no idea what users are doing with their internet connection. The fact is that more than 40% of corporate internet use is inappropriate and going unchecked—an average of 1 to 2 hours per day per user. To make matters worse, the potential for employees being exposed to inappropriate content can have serious legal ramifications to any organization. The internet is full of studies related to internet use in the work place, from gambling and pornography to less nefarious activity such as social networking and travel planning. Furthermore, incidents of internet addiction disorder are increasing, with current estimates suggesting up to 5% to 10% of internet surfers have some form of web dependency.

Myth #3: We control web usage and our users can't get around our policy

Anonymizing proxies make it easy for employees to circumvent your web filtering policy and visit any site they like. Anonymizing proxies are readily available and regularly exploited by school kids and employees alike. Hundreds of new anonymizing proxies are published daily to keep ahead of web security companies and resourceful users have even been known to setup their own private proxy at home to enable them to surf the web freely and unchecked. If you don't think this is an issue, you can simply Google "bypass web filter" to see there are over 1.8 million ways to do this.

Myth #4: Only porn, gambling, and other "dodgy" sites are dangerous

Hijacked trusted sites represent more than 83% of malware hosting sites. That's correct. The majority of infected sites are websites that you trust and visit daily—they've just been hacked to distribute malware. Why? Because these sites are popular, high-traffic venues that silently distribute malware to unsuspecting visitors. Download the infected sites list to see just a small sampling of these kinds of sites.

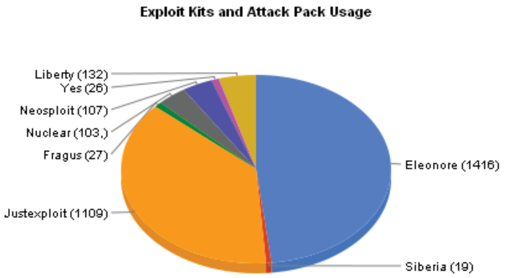
Myth #5: Only naive users get infected with malware and viruses

Malware from drive-by downloads happens automatically without any user action, other than visiting the site. Therefore, it doesn't matter what level of computer expertise you have. The fact is, if you are visiting sites on the internet, you are at risk. The infected sites list provides just a small sampling of recently infected sites that distribute malware. If you visit sites like these, you are at risk.

Myth #6: You can only get infected if you download files.

Most malware infections now occur through a "drive-by" download. Hackers inject the malicious code into the actual web page content, then it downloads and executes automatically within the browser as a by-product of simply viewing the web page. The malware is typically part of a professional exploit kit marketed and sold to hackers that leverages known exploits in the browser, operating system or plug-ins to infect the computer and download more malware. Again, it does all of this without a user having to do anything other than visit a hijacked web site.

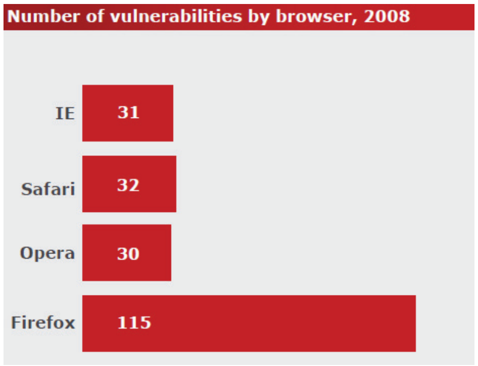
This graph shows the most popular exploit kits used in drive-by download attacks.



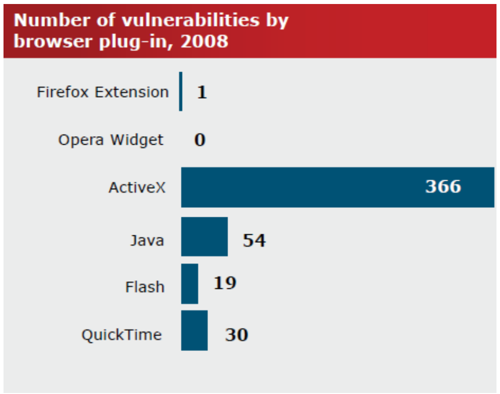
Source: http://www.blade-defender.org/eval-lab/

Myth #7: Firefox is more secure than Internet Explorer

All browsers are equally at risk because all browsers are essentially an execution environment for JavaScript, which is the programming language of the web and therefore used by all malware authors to initiate an attack. In addition, many exploits leverage plug-ins such as Adobe Acrobat reader software, which runs across all browsers. Although the more popular browsers may get more publicity about unpatched exploits, it's the unpublicized exploits you should be most concerned about. The fact is, there is no safe browser; when security research firm Secunia tabulated the number of browser exploits reported in 2008, Firefox was actually the least secure by a large margin:



Source: http://secunia.com/gfx/Secunia2008Report.pdf



Source: http://secunia.com/gfx/Secunia2008Report.pdf

Myth #8: When the lock icon appears in the browser, it's secure.

The lock icon indicates there is an SSL encrypted connection between the browser and the server to protect the interception of personal sensitive information. It does not provide any security from malware. In fact, it's the opposite because most web security products are completely blind to encrypted connections: it's the perfect vehicle for malware to infiltrate a machine. Furthermore, some malware can exploit vulnerabilities to spoof SSL certificates to make users feel more secure or enable devious connections to fake banking sites. There are numerous recent examples of hackers creating elaborate phishing schemes that emulate bank, credit card, or PayPal sites complete with spoofed SSL certificates that are extremely difficult for the average user to identify as fraudulent. This is becoming an increasingly important security risk.

Myth #9: Web security requires a trade-off between security and freedom

While the internet has become a mission critical tool for many job functions, whether it's Facebook for HR or Twitter for PR, it's completely unnecessary to create a trade-off between access and security. A suitable web security solution provides the freedom to grant access to sites that your users need while keeping your organization secure. Policy settings for groups or individuals don't need to be complex—a few quick steps through a wizard are all a user needs to secure and enable your organization.

When evaluating a web security solution, be sure to focus on the administration tasks you will use most often, such as establishing special policies for users or groups. How easy are these tasks? How much time do they take? How many steps are involved? Is documentation required to navigate through the process? Ask these questions and more.

Myth #10: Endpoint security solutions can't protect against web threats

Typically, this has been the case because the web browser is essentially its own execution environment: it downloads content, renders it, and executes scripts all without any visibility outside the browser to endpoint security products. However, this is changing. As a result, it's opening up a whole new approach to web security, particularly for mobile workers who are operating beyond the traditional boundaries of the corporate network. Be sure to check out the new Sophos Live Protection Web Filtering, which is part of our new Endpoint 9.5 security solution. Live Protection enables real-time malicious site filtering at the endpoint to protect mobile or remote workers who may be operating off the corporate network.

Now that we've busted several common myth's and exposed the truth about web security risks, you're probably thinking "Ok, how do I protect my organization and users?". Good question. Fortunately, there's a simple answer: Visit Sophos.com for more tips, tricks and expert advice.

Boston, USA | Oxford, UK

© Copyright 2010. Sophos

*All registered trademarks and copyrights are understood and recognized by Sophos.
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.*

SOPHOS
WWW.SOPHOS.COM