SOPHOS

Top 5 Myths of Safe Web Browsing

By **Chris McCormack**, Product Marketing Manager

There are a lot of misconceptions out there about safe web browsing. You might think you're being safe. But without the facts it's next to impossible to stay protected against today's changing threats. In this paper we describe the top five myths of safe web browsing, what the facts really are, and what you can do to stay secure.

The top five myths of safe web browsing

1. **Myth:** A strict browsing policy that only lets users visit trusted sites keeps us safe.
   Fact: There's no such thing as a trusted site and users may be easily bypassing your policy.
2. **Myth:** Scanning downloaded files for viruses keeps us secure.
   Fact: That won't help you against drive-by infections.
3. **Myth:** Using a secure browser like Chrome offers better protection.
   Fact: Chrome is subject to exploits just like any other browser and the more popular it becomes, the more it will be targeted.
4. **Myth:** Macs are more secure than PCs.
   Fact: Malware is now targeting Macs and having more success than ever.
5. **Myth:** The only way to protect offsite users is with a VPN or cloud service.
   Fact: The best way to protect offsite users is to have web filtering integrated into every laptop.

1. Myth: A strict browsing policy that only lets users visit trusted sites keeps us safe

Fact: Every site presents a risk. There's no such thing as a trusted site anymore. And to make matters worse, anonymizing proxies make it easy for users to bypass most web policies.

The full story: Web threats are no longer the domain of the dark corners of the web such as adult and gambling sites. Hackers have long since moved on to target more mainstream, popular, trusted sites to distribute malware and infect victims. In fact, 80% of infected websites are legitimate trusted sites.[1]

So while blocking inappropriate sites is important from an acceptable-use policy perspective and to reduce your risk surface area, it's not an effective security measure on its own. In addition, you should be aware that anonymizing proxy sites make it easy for users to bypass web filtering policies.

What you can do: In addition to a URL filtering solution, you also need to make sure you have advanced web malware detection to scan all website content as it's accessed. This will catch the latest threats, on any site, before it can become a problem. You also need to have anonymizing proxy protection in your web security solution. Ideally, the kind that can detect anonymizing proxy abuse in real time and stop rogue users dead in their tracks.

1 Websense research report: Security Pros & "Cons", http://www.websense.com/assets/reports/security-pros-and-cons-research-report.pdf

2. Myth: Scanning downloaded files for viruses keeps us secure

Fact: While controlling and scanning downloads on the web is a good start, it's not going to keep your users from getting infected. You may have heard of "drive-by" infections. It's a term used to describe a very common type of silent attack that can infect visitors to websites who do nothing else but visit a page—and they won't even know it's happened.

The full story: Hackers have become experts at exploiting websites using techniques like SQL injection to embed malicious code into even the most trusted legitimate websites. The malicious code is then loaded automatically by the browser whenever someone visits a page on the site—and the visitor has no idea what's going on.

This code can be heavily obfuscated (masked) and change with every page load (polymorphic), making it extremely difficult for traditional web security solutions to detect. And impossible for desktop antivirus to even see. Once the malicious code is downloaded automatically by the browser, it will secretly download an exploit pack that will seek out dozens of known vulnerabilities in browsers, plugins, applications, or the OS to install its payload.

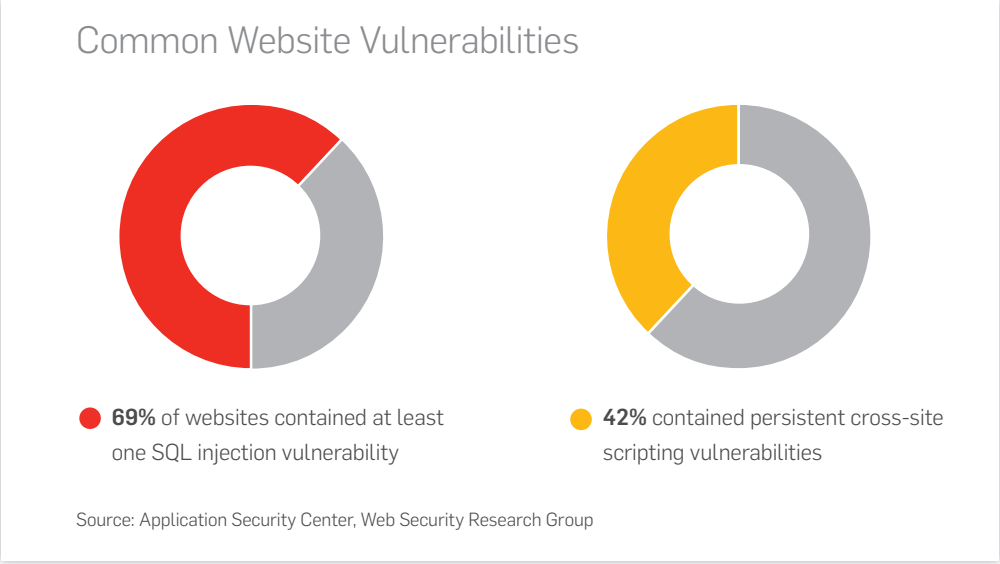


Figure 1: Hackers commonly exploit websites by embedding malicious code using techniques like SQL injection or cross-site scripting.

What you can do: Make sure you have advanced multi-layered web protection to provide a coordinated defense. It must include essential URL filtering, but also scan all downloaded website content as it's accessed. It must be able to deobfuscate and emulate JavaScript in real time to detect any suspicious behavior. Don't rely on signature-based malware detection—it's completely ineffective at protecting your organization from modern web threats.

3. Myth: Using a secure browser like Google Chrome offers better protection

Fact: Even though Chrome is considered among the most secure, every browser has new vulnerabilities all the time. Hackers are constantly testing new exploits, and the best ones are the ones we haven't heard about.

The full story: Chrome is widely considered among the most secure browsers available today, a reputation that Firefox once had. But we wouldn't recommend putting your security on the line based on reputation. In fact, hackers have exposed vulnerabilities in the browser, proving Chrome isn't impenetrable.[2]

It's the vulnerabilities we haven't heard about that should concern you the most. It's not surprising that as a browser like Chrome becomes more popular with users, it also becomes more of a target to hackers. Hackers make money from exploiting vulnerabilities and infecting systems. So more people using a given browser means more opportunity for the hackers.

Figure 2: Chrome is vulnerable to exploits like any other browser. A competitor at the annual Pwn2Own conference managed to hack Chrome in just five minutes.

What you can do: All of today's browsers represent a security risk, but there are a few steps you can take to improve your chances of avoiding infection. First, use application control to limit the number of browsers supported in your organization to as few as possible. Keep those supported browsers fully patched at all times with a vulnerability management solution. This will keep your risk surface area to a minimum. Finally, make sure you have advanced web malware detection at work that can stop threats in real time, no matter what browser you're using.

2 Naked Security blog, http://nakedsecurity.sophos.com/2012/03/08/chrome-pw2own-vulnerabilit/

4. Myth: Macs are more secure than PCs

Fact: Mac OS X is a completely different operating system from Windows, and has many built-in security features. However, as we've seen recently, hackers have found creative ways to infect Mac users with malware.

The full story: We've all seen the news about Mac malware attacks from Flashback[3] exploiting a Java vulnerability, and Sabpab,[4] a Trojan that exploits Microsoft Word on the Mac. As Macs become more popular both at home and in the workplace, they will be targeted more by hackers and malware. In fact, at Sophos we're actively tracking dozens of OS X threats daily, many of them new. Our antivirus protection for the Mac seeks them out and blocks them.

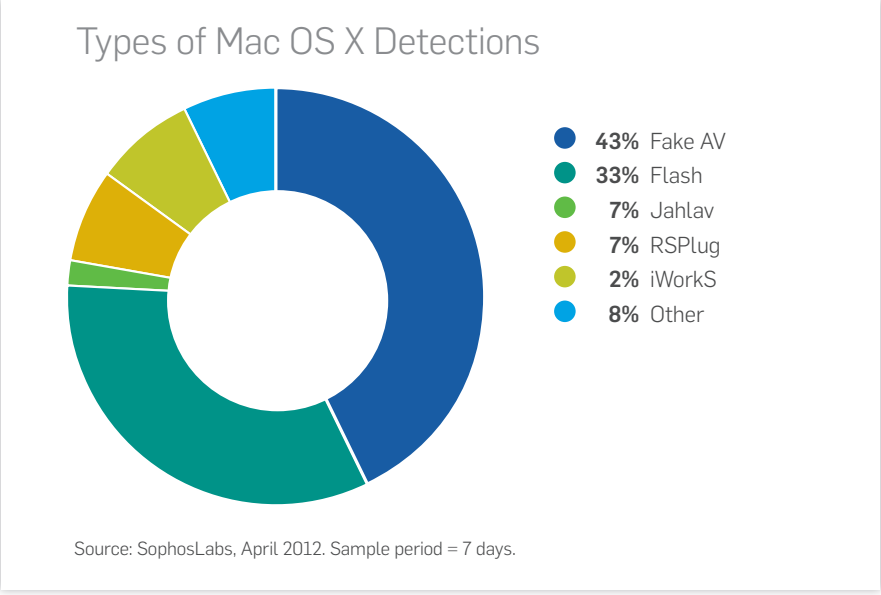


Figure 3: Numerous types of Mac OS X specific threats are detected daily by SophosLabs.

What you can do: If you haven't already, deploy a Mac antivirus solution. Ideally, your solution should be lightweight and easy to manage alongside your other platforms. It should be backed by a global threat analysis labs operation that actively monitors Mac threats. Make sure your Mac applications and add-ons are fully patched and up to date at all times to reduce the number of potential vulnerabilities.

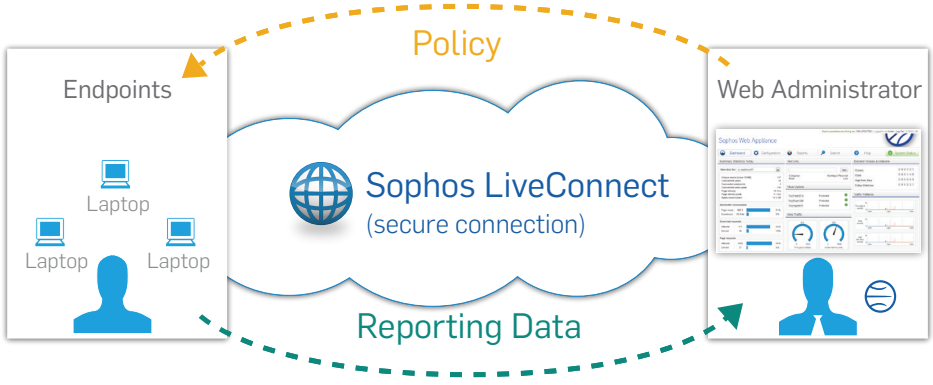
3 Naked Security blog, http://nakedsecurity.sophos.com/2012/04/13/apple-pumps-out-yet-another-java-update/
4 Naked Security blog, http://nakedsecurity.sophos.com/2012/04/16/sabpab-trojan-mac-word/

5. Myth: The only way to protect offsite users is with a VPN or cloud service

Fact: That used to be true, but not anymore.

The full story: In the past, you had to redirect your users' web surfing through a cloud service or back through your secure web gateway with a VPN connection to keep them secure. As you probably know, this can be terribly complex, expensive, and full of problems like latency, loss of localization, and bandwidth consumption. The good news is, there is a better way. Integrating web policy enforcement and web content scanning directly into the network layer on your laptops is by far the most effective, efficient, scalable, and affordable way to stay protected on the web wherever users go.

What you can do: Adopt a web protection solution that integrates web security directly into the endpoint on all your laptops—keeping your road warriors, remote workers, and other offsite users safe wherever they happen to be. You'll keep users secure while still having complete visibility and policy control over users everywhere they go.



LiveConnect enables instant policy and reporting updates everywhere users go by seamlessly connecting your endpoints and management console through the cloud.

Figure 4: You need web protection that provides your offsite users direct access to the web while still allowing you to update policy or view activity as if they were right in the office.

Web protection capabilities you need

By dispelling these myths and following our recommended remedies, you'll be better equipped to keep your organization secure against today's changing web threats. In summary, here's what you should be looking for in an effective web protection solution:

- Advanced real-time web malware protection that goes beyond signatures
- Multi-layer protection that uses URL filtering, behavioral analysis, and HIPS to stop threats
- Application control and vulnerability management to reduce your risk surface area
- Endpoint protection for all your platforms, including Macs
- Web protection that travels with users for secure web access from anywhere
- 24/7 global web threat intelligence with the latest web-specific detection technologies
- Complete IT administrator control and visibility no matter where users are
- Reduced network complexity without the downsides of a SaaS or proxy solution, such as backhauling, latency and a single point of failure
- Seamless scalability for easy expansion over time

A successful web protection solution combines the best elements of endpoint, cloud and gateway solutions to provide a better, more secure web experience. Look for a solution that integrates web protection into the endpoint to provide complete web protection, everywhere users go.

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia & New Zealand Sales:
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Boston, USA | Oxford, UK

A Sophos Whitepaper 4.12v1.dNA

SOPHOS