SOPHOS

simple + secure

Five tips to reduce risk from modern web threats

By **Chris McCormack**, Product Marketing Manager
and **Chester Wisniewski**, Senior Security Advisor

Modern web threats can infect your network, subvert systems into botnets or steal sensitive data. To meet these challenges to your security, you need to put in place user education and awareness, preventive measures and a modern web security solution. This guide covers five essential preventive measures you should implement to reduce your risk and keep ahead of the threats as much as possible.

Five tips

Threats from the web are constantly changing. At SophosLabs we've seen 150,000 new pieces of malware every day since the start of 2011, more than one new threat every second. But you can improve your web protection when you observe some best practices.

1. Keep your systems patched and up to date

2. Standardize your web software

3. Secure your browsers

4. Enforce a strong password policy

5. Use an effective web security solution

Follow these five tips to reduce your risk and stay ahead of the threats.

1. Keep your systems patched and up to date

Keeping systems fully up to date—including the operating system, web browsers, browser plugins, media players, PDF readers and other applications—can be a time-consuming ongoing task. Yet patching is incredibly effective—90% of attacks can be prevented with an existing patch.

Most web malware comes from commercially available exploit packs that target unpatched systems. These packs contain dozens of different vulnerability testers, redirectors and exploit code to find and attack vulnerabilities.

The most common targets for these web-based exploit packs are web browsers such as Internet Explorer, Firefox, Safari, Chrome and Opera. Other targets include common cross-browser plugins such as PDF readers, Flash players, QuickTime and Java Runtime Environment, as well as operating systems.

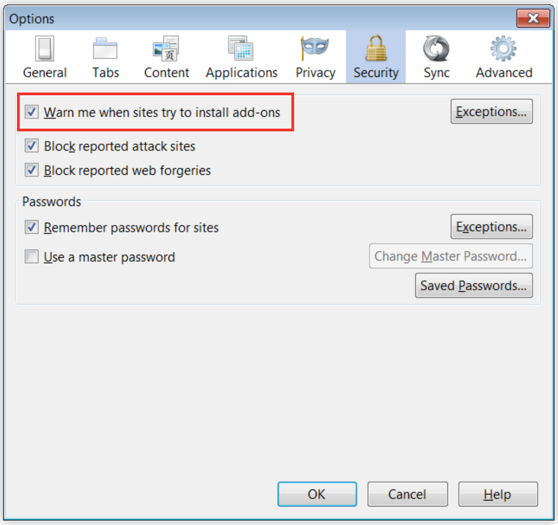
Patches are critical to the security and efficient operation of your IT infrastructure, so it's worth making an investment in system patches. One way to make patching easy is to keep auto-updating turned on for applications that support it. You should encourage your users to apply all updates as soon as they are prompted.

2. Standardize your web software

The more platforms and software you have, the more opportunities you give hackers to find vulnerabilities in unpatched applications. Patching becomes more difficult if you don't know what software is running on your network, or you have no control over which browsers, plugins and media players employees use. Limit the number of Internet tools, applications and plugins in your organization to a standardized set and enforce their use as policy.

Your policy should require users to access the Internet with a common set of tools that meet these minimum requirements:

- **Browser:** Stick with a single mainstream browser. Popular browsers invite more exploits but their vendors also have more resources to address vulnerabilities and provide patches more often.
- **PDF reader:** Use a single mainstream PDF reader. Keep it patched with the auto-update feature enabled, and advise users to install patches as soon as they become available.
- **Media player:** Avoid unnecessary media player add-ons and codec packs. If possible, stick with what your operating system provides and keep your OS patched.
- **Plugins, add-ons and toolbars:** Avoid unnecessary browser plugins and toolbars. They only increase the attack surface area. You can block unnecessary browser add-ons by configuring the browser with the settings shown in Figure 1.



☑ Warn me when sites try to install add-ons

☑ Block reported attack sites

☑ Block reported web forgeries

Passwords

☑ Remember passwords for sites

□ Use a master password

Figure 1: Use settings to control add-ons

3. Secure your browsers

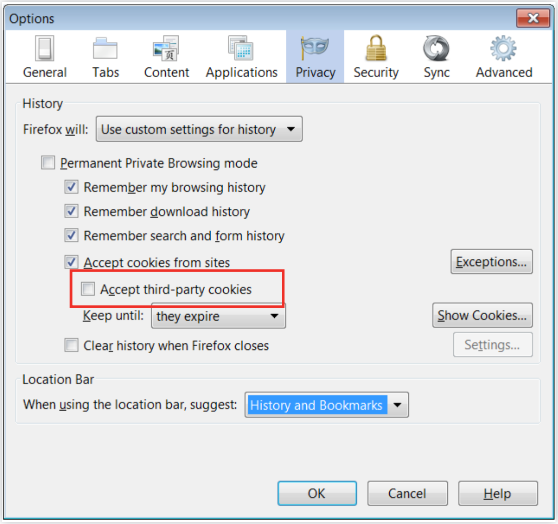
Familiarize yourself with the security, privacy and content settings that all browsers have in order to understand the trade-offs between security and usability. Some settings merely increase the level of prompting—annoying users without adding any tangible security—while others can be important to limiting exploits and threats. Set up your browsers accordingly.

Here are some common browser elements you can control through settings, and the trade-offs involved.

Cookies: Cybercriminals can exploit cookies in some malicious ways, but they are an important component of Internet usability. Turning them off altogether is not a viable option, but it's important for you to control third-party cookie activity. To check that your browser is blocking third-party cookies, use settings such as the one shown in Figure 2.

Autocomplete: The autocomplete or autofill feature saves keystrokes by storing information you recently typed, such as search terms, recently visited websites and your personal information (e.g., name, email, address, phone number). Although this data is obfuscated, some malware targets autocomplete data in order to steal passwords or other personally identifiable information.

Additionally, using autocomplete for login information poses a big risk if you your laptop is lost or stolen, allowing criminals to access your accounts.



History

Firefox will: Use custom settings for history

□ Permanent Private Browsing mode

☑ Remember my browsing history

☑ Remember download history

☑ Remember search and form history

☑ Accept cookies from sites

□ Accept third-party cookies

Keep until: they expire

□ Clear history when Firefox closes

Location Bar

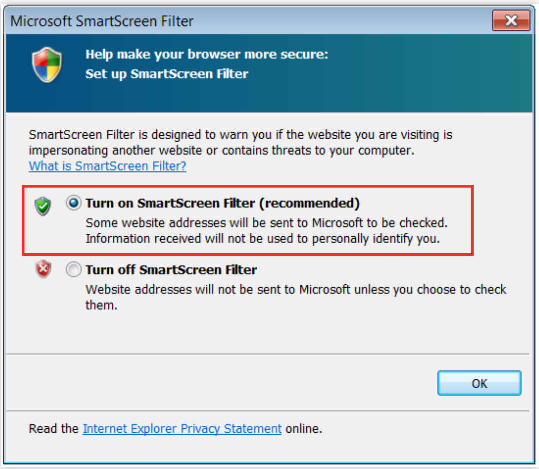
When using the location bar, suggest: History and Bookmarks

Figure 2: Block third-party cookies

Add-ons: Configure your browsers to prevent them from installing add-ons such as plugins, ActiveX controls, toolbars and browser helper objects without a prompt. Remember to restrict add-ons to an absolute minimum in order to reduce the attack surface area for exploits. However, if your security vendor supplies add-ons for your browser, make sure you don't disable them. They can provide valuable pre-execution analysis of browser code.

Content filters: Your users are well protected when they're on a corporate network with a proper web security solution (see point number 5). But you should filter content for users operating remotely, such as at home or at a Wi-Fi hotspot. Most popular browsers employ a database of phishing and/or malware sites to provide protection from the most ubiquitous threats. Make sure that your users enable content filters on their browsers (see Figure 3).

Popup blockers: Popups are not only annoying resource hogs, but they also can host embedded malware directly or lure users into clicking on something using social engineering tricks. For example, some popups can be ingeniously crafted to look like Windows dialog boxes, and the mere act of clicking the "X" to close the box can unleash a malware attack. Be sure that your selected browser has popup blocking enabled (see Figure 4) and make users aware of the dangers of interacting with any kind of popup.



Microsoft SmartScreen Filter

Help make your browser more secure:
Set up SmartScreen Filter

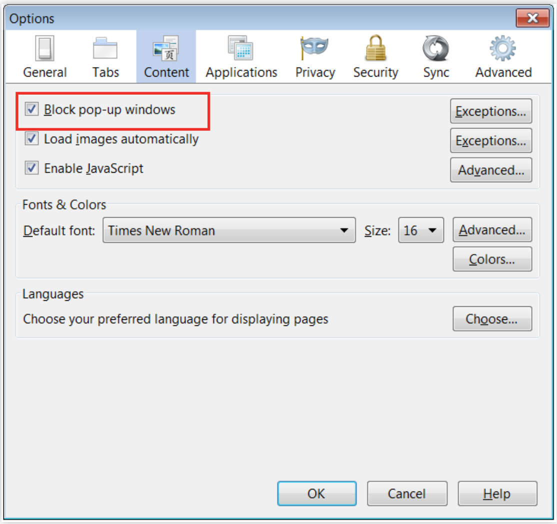
SmartScreen Filter is designed to warn you if the website you are visiting is impersonating another website or contains threats to your computer.
What is SmartScreen Filter?

● **Turn on SmartScreen Filter (recommended)**
Some website addresses will be sent to Microsoft to be checked. Information received will not be used to personally identify you.

○ **Turn off SmartScreen Filter**
Website addresses will not be sent to Microsoft unless you choose to check them.

Read the Internet Explorer Privacy Statement online.

Figure 3: Enable filters on browsers to protect against malware and web threats



Options

☑ Block pop-up windows
☑ Load images automatically
☑ Enable JavaScript

Fonts & Colors
Default font: Times New Roman Size: 16

Languages
Choose your preferred language for displaying pages

Figure 4: Make sure popup blocker is turned on

4. Enforce a strong password policy

The purpose of a password policy should be obvious: to permit access only to authorized users. Weak passwords make it easy for hackers to guess or crack them. Despite this enormous vulnerability in every system, many organizations fail to take this threat seriously.

You should enforce policies for creating an effective password, following these guidelines:

- Use long passwords. The more characters they contain, the more secure they are.
- Include numbers, symbols, and upper- and lowercase characters.
- Don't use common dictionary terms. The first thing hackers do to crack an account is try every word in the dictionary.
- Don't use personal information such as pet, romantic, family or other names, or birthdays.
- Change passwords frequently.
- Avoid passwords you can't remember, or use a centralized password management tool such as LastPass and 1Password. The worst kind of password is one written on a sticky note next to the computer.
- Abide by simple and effective password policies both at work and at home.

5. Use an effective web security solution

A proper web security solution reduces your threat exposure by limiting users' surfing activity to website categories relevant to their work, or at least restricting access to the categories (adult, gambling, etc.) that are a breeding ground for malware. It also protects you from trusted sites that may become hijacked at any time to silently spread malware to unsuspecting visitors.

Finally, it protects your Internet resources from abuse as a result of the exchange of illegal content or bandwidth-sapping streaming media.

Your web protection solution should offer these capabilities:

- **Productivity and reputation filtering** establishes acceptable user policy, limits threat exposure from notoriously malicious site categories, and filters out sites with bad reputations regardless of category.
- **Proxy filtering** prevents users from bypassing web filtering and putting themselves and the organization at serious risk.
- **Real-time malware filtering** catches malware as it's downloaded from hijacked trusted sites.
- **HTTPS filtering** secures an increasingly important vector that evades most web filtering solutions.
- **Content-based filtering** reduces the threat surface area from file types associated with malware and controls bandwidth consumption.
- **Protection everywhere** so that even users outside the corporate network are fully protected, wherever they go.

Try it now for free

Register for a free 30-day evaluation
at sophos.com/web.

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

Boston, USA | Oxford, UK

SOPHOS