

Five tips to reduce risk from modern web threats

User education and awareness, preventive measures and a modern web security solution are all integral components of a comprehensive defense against today's web threats. This guide covers some essential preventive measures you should implement to reduce your risk and keep ahead of the threats as much as possible.

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

Five tips to reduce risk from modern web threats

User education and awareness, preventive measures and a modern web security solution are all integral components of a comprehensive defense against today's web threats.

This guide covers some essential preventive measures you should implement to reduce your risk and keep ahead of the threats as much as possible. In particular, it's important to:

- Keep your systems patched and up to date
- Standardize your web software.
- Secure your browsers.
- Enforce a strong password policy.
- Use an effective web security solution.

Each measure is discussed in more detail in the sections that follow.

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 tedious, annoying and time-consuming ongoing task. Unfortunately, hackers are counting on most people to fall far short of what's needed to keep their systems up to date.

Most web malware utilizes commercially available exploit packs that contain dozens of different vulnerability testers, redirectors and actual exploit code that attempt to test for and exploit any vulnerabilities they can find. These kits are designed specifically to prey on users who aren't diligent about keeping their software and operating system patches up to date.

The most common targets for these web-based exploit packs are not just web browsers such as Internet Explorer, Firefox, Safari, Chrome and Opera, but also common cross-browser plugins such as PDF readers, Flash players, QuickTime and Java Runtime Environment, as well as operating systems themselves.

The importance of applying system patches should be obvious. Although they are annoying and time consuming, they're also critical to the security and efficient operation of your IT infrastructure. Therefore, it's worth making an investment in system patches. One of the best ways to make patching easy is to keep auto-updating turned on for applications that support it and encourage users to apply all updates as soon as they are prompted to do so.

2. Standardize your web software.

If you've just read point number 1, you're probably still thinking that keeping systems fully patched and up to date is an onerous task. What makes this worse is if you don't know what software is running on your network or you have a variety of individuals using different browsers, plugins and media players.

As mentioned, modern web attacks often leverage commercial exploit kits that attempt to exploit dozens of different security vulnerabilities. The more varied your platforms and software are, the more opportunities you present to the hackers to exploit, and the more likely they are to find a vulnerability in an unpatched application.

Make your life easier and dramatically reduce your threat surface area by limiting users to—or better yet, standardizing on—a core set of minimal applications for interacting with the web. Enforce a policy that all users must access the internet with a common set of tools that meets the minimum requirements:

- **Browser:** Stick with a single mainstream browser. Popular browsers invite more exploits but also have more resources behind them to address vulnerabilities and provide patches more often.
- **PDF reader:** Again, stick with a single mainstream PDF reader. Keep it patched, ensure the auto-update feature is enabled, and ensure users are advised 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.
- **Plug-ins, add-ons and toolbars:** Avoid unnecessary browser plugins and toolbars. They only increase the potential surface area for attack.

In addition, configure your browsers to ensure they are not installing plugins, add-ons, ActiveX controls and toolbars without at least a prompt by using settings such as the one shown in Figure 1.

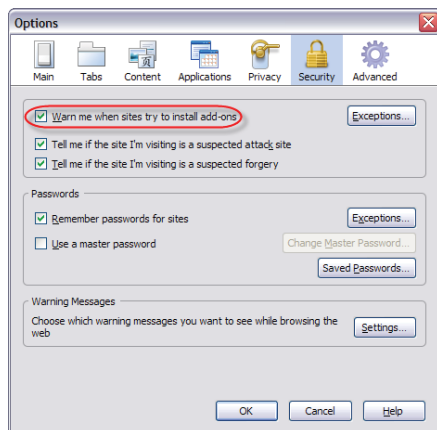


Figure 1: Use settings when configuring browsers

Simplify the task of minimizing security vulnerabilities and keeping your systems patched and up to date by reducing the variety of internet tools, applications and plugins used in your organization to the bare minimum, and standardizing and enforcing their use across your organization.

3. Secure your browsers.

You must familiarize yourself with the plethora of security, privacy and content settings that all browsers have in order to understand the trade-offs. Some security settings will merely increase the level of prompting—annoying users without adding any tangible security—while others can be important to limiting exploits and threats.

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

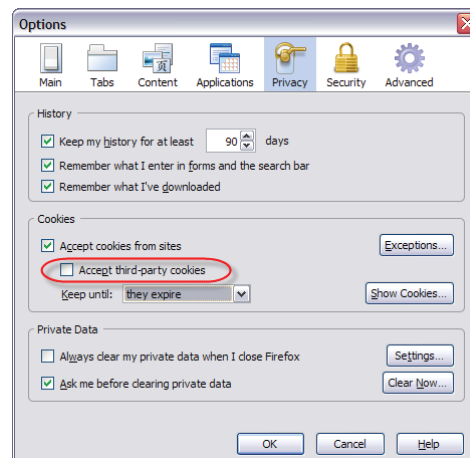


Figure 2: Block third-party cookies

Cookies: Although cookies can be exploited in some malicious ways, they are an important component of internet usability. Therefore, turning them off altogether is not a viable option. However, controlling third-party cookie activity is important. Check that your browser is blocking third-party cookies if at all possible by using settings such as the one shown in Figure 2.

Autocomplete: Autocomplete or autofill is a feature in many browsers that stores information you recently typed, such as search terms, recently visited websites and your personal information (e.g., name, email, address, phone) in the interest of saving keystrokes. Although this data is obfuscated, some malware targets autocomplete data in order to steal passwords or other personally identifiable information. In addition, using autocomplete for login information can present a significant risk for lost or stolen laptops—allowing criminals to easily abuse account privileges. Ensure that you understand the trade-offs and risks involved and make the best decision for your particular organization with respect to usability versus security. Set up your browsers accordingly.

Add-ons: ActiveX controls, plugins, browser helper objects (BHOs) and toolbars are all examples of browser add-ons. As discussed in point number 2 above, it's imperative to restrict add-ons to an absolute minimum in order to reduce your threat surface area for exploits. However, if your security vendor supplies add-ons for your browser, make sure you don't disable them as they can be instrumental in bolstering the security of the browser—providing valuable pre-execution analysis of browser code. Make sure you understand how to view the active browser add-ons and force a prompt whenever a web page tries to install a new one.

Content filters: Although this is not a concern for users on a corporate network that implements a proper web security solution (see point number 5), users operating remotely, at home or at a Wi-Fi hotspot should ensure their browser content filters are enabled. Most popular browsers offer at least a basic phishing and/or malware site database that can help provide protection from the most ubiquitous threats (see Figure 3). Ensure that your users enable these filters on their browsers.

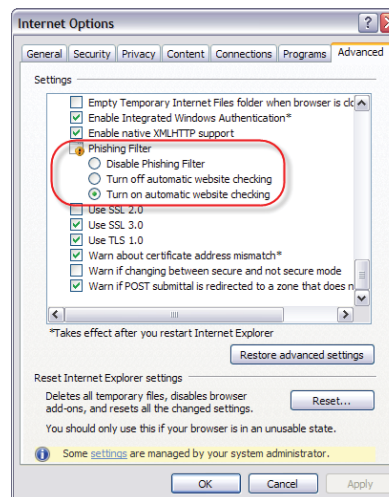


Figure 3: Enable filters on browsers to protect against malware and web threats

Popup blockers: Popups are not only annoying resource hogs, but they also can pose a security risk by either hosting embedded malware directly, or trying to lure users into clicking on something using a well known social engineering trick. 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 instigate a malware attack. Ensure 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.

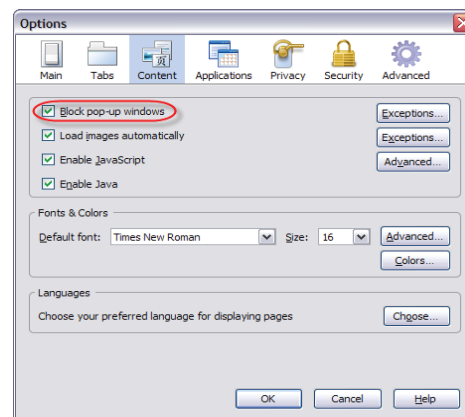


Figure 4: Ensure popup blocker is turned on

4. Enforce a strong password policy.

The purpose of a password policy should be obvious: If you don't want everyone to have access to something, you set up passwords to permit access only to authorized users. The purpose of an effective password policy is to keep passwords from being easily guessed or cracked by hackers. Despite this enormous vulnerability in every system, many organizations fail to take this threat seriously.

Here are some tips for creating an effective password:

- Use long passwords. The more characters they contain, the more secure they are.
- Include numbers, symbols, and upper- and lowercase characters.
- Do not use common dictionary terms. The first thing hackers will do is literally try every word in the dictionary to crack an account.
- Do not use personal information such as pet, romantic, family or other names, or birthdays.
- Change passwords frequently.
- Avoid passwords users can't remember, or equip them with a centralized password management tool to make password management simple and secure (such as LastPass and 1Password). The worst kind of password is one written on a sticky note next to the computer.
- Users should abide by simple and effective password policies both at work and at home. This will go a long way toward securing this major vulnerability in all systems.

5. Use an effective web security solution.

A proper web security solution is a vital component of an overall strategy for safeguarding your organization from modern web threats. It will reduce your threat exposure by limiting users' surfing activity to website categories relevant to their work, or at least help them avoid the dirty dozen categories (adult, gambling, etc.) that are a breeding ground for malware. It will also protect you from trusted sites that you visit daily that may become hijacked at any time to silently spread malware to unsuspecting visitors. Finally, it will also help protect your internet resources from abuse as a result of the exchange of illegal content or bandwidth-sapping streaming media.

The key components of a web security and control solution are:

- 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 in real time, as it's downloaded from hijacked trusted sites.
- HTTPS filtering secures this increasingly important vector that is completely blind to most web filtering solutions.
- Content-based filtering reduces the threat surface area from file types associated with malware and to control bandwidth consumption.

Review our Web Security and Control Buyers Guide for more insight into what constitutes an effective web security and control solution.

Summary

If you combine user awareness and education with suitable preventive measures as outlined here, along with an effective web security and control solution, you can rest assured you are doing everything possible to protect your organization from modern web threats that can infect your network, subvert systems into botnets or steal sensitive data. It's a daunting task, but it's very achievable—particularly if you have the right security partner by your side.

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