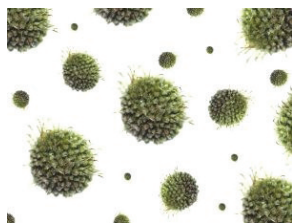


Ignorance Is *Not* Bliss: We Reveal 10 Web Application Security Myths

By Stefanie Hoffman

Even in the Web 2.0 day and age, there remain myriad Web application security myths. Some of the oldies but goodies persist (e.g., users will know when there's a virus or Trojan on their computer) to newer myths developed around Google search, social networking and Web browsers. With the preponderance of information about Web 2.0 security, it's easy to become overwhelmed. Here is our attempt to address some of the biggest lingering misconceptions about Web application security.

Myth No. 1: I Would Know If My Computer Got A Virus Or Malware



How do you know? Once upon a time, hackers wrote viruses to wreak as much havoc as possible—freezing computers, obliterating files and

delivering the fateful “blue screen of death.” Not so anymore. Nowadays, attacks are designed to quietly sit on a user's computer and stealthily steal sensitive data and passwords without a user's knowledge. Once infected, the computer becomes part of a malicious network of computers controlled by a remote command and control center. And more sophisticated attacks are designed to evade antivirus engines and spam filters. The only way to know that you're infected is to do a comprehensive scan of the computer. And you might be surprised by what you find.

Myth No. 2: A Web Page Is Safe If It's At The Top Of Google Search

Sadly, no. Google's algorithms rank the pages by key words and a variety of other factors, depending on the search topic. But Google has no way to determine if a site is malicious or has been compromised. Meanwhile, hackers are becoming more adept at search engine optimization techniques, which rocket malicious sites to the top of the search pages, banking on the fact that users will naturally gravitate toward the first few pages listed.

It might be a tad unsettling to know that not all Google searches can be trusted. However, there are a few signs that indicate if a search engine's page rankings are legiti-

mate. Pay close attention to the domain (if a site is registered to India or China, be wary). Also, pay attention to the URL, and treat unknown or unfamiliar sites with a healthy dose of skepticism. When in doubt, go directly to a known site.

Myth No. 3: Users Can't Get Around Company Web Policies

Wanna bet? More and more users are circumventing an organization's security policies by anonymizing proxies, which make it easy for employees to get around Web filtering.

Users often set up their own private proxies at home that enable them to surf the Web freely without fear of reprisal, while also making it easy for them to circumvent Web filtering policies and visit any site they like.

Meanwhile, hundreds of anonymizing proxies are being published daily in an attempt to keep ahead of Web security companies and corporate IT policies. All users have to do is simply Google “bypass Web filter” and take their pick from the more than 1.8 million ways to do this.

Meanwhile, unlike years past, many organizations can't simply crack down on social networking and other sites. More and more organizations are relying

upon social networking and other Web services as business-critical applications. In fact, many organizations view social networking as a business accelerator. While a few years ago, companies could easily pull the plug on the use of these sites to do so now could potentially mean forfeiting opportunities to competitors.

Unfortunately, this fact is not lost on hackers. And along with the benefits of social networking comes copious risk, as hackers are increasingly taking advantage of these sites to distribute spam and malicious links designed to infect users with malware. Subsequently, most organizations will likely have to make a choice regarding the level of access their users will have to social networking sites and the level of acceptable risk they are willing to swallow to placate social networking users.

Myth No. 4: Only Porn, Gambling And Other Sketchy Sites Distribute Malware

If only that were so. But it's not so easy anymore. Hackers are continuing to hijack trusted, legitimate sites and infect them with malware in what are known as “drive-by download” attacks. Users have only to visit the site to become infected.



Hackers take advantage of popular high-traffic sites to distribute malware to as many users as possible. Malware authors inject malicious code into popular sites and then take advantage of the high volumes of traffic to distribute malware and, not surprisingly, the majority of infected sites are ones that users trust and visit daily.

Predictably, attackers continue to take advantage of high-profile world events and other news, to entice users to click on a link or visit an infected site. And as usual, most users will have no idea that they have been infected.

Myth No. 5: Apple Apps Are Much Safer From Security Threats Than Others

Not so much. Apple App malware is on the rise as the use of iPhones, iPod and iPad devices increases. In addition, security experts predict that Apple attacks will increase in the next few years as consumer



devices, such as the iPhone 4, are more frequently used in the workplace.

Essentially, any malware exploiting a browser-based vulnerability on the iPhone or iPod Touch will work equally as well on the iPad, given that all three devices share a practically identical OS. And as with the iPhone, one of the most vulnerable attack vectors in the new iPad will be browser-based, which will likely subject the device to numerous Web kit vulnerabilities. In addition, security experts contend that they have seen malicious apps make their way into Apple's App Store.



Meanwhile, Apple prohibits any third-party software, including security software, from being installed on its mobile devices, which doesn't bode well for the iPad, considering its anticipated mass consumer appeal, security experts say.

Myth No. 6: Users Can Only Become Infected If They Download Files

Remember that thing we talked about—a “drive-by download?” These days, users only have to visit a malicious site to become infected. During the attack, hackers inject malicious code into the Web page content, which is automatically downloaded and executed within the browser once a user opens the page. Drive-by attacks are becoming more common in light of the fact that hackers have increasing



access to exploit kits that leverage known exploits in the browser, operating system or plug-ins, designed to infect the computer and download more malware.

Attackers routinely lure users to these sites via social engineering schemes delivered via e-mail. Then they entice users to click on infected links. There are an unlimited number of ways users can become infected, without any intervention except viewing a Web page.

Myth No. 7: Firefox Is More Secure Than Internet Explorer

Well, not quite. Surprise, but all browsers are equally at risk of attack. Why? Because all browsers provide a wide-open playing field for JavaScript execution, the programming language of the Web. Subsequently, all Web browsers are susceptible to malware attacks exploiting JavaScript vulnerabilities. In addition, many exploits leverage third-party

browser plug-ins such as Adobe Acrobat Reader software, which is applied to all browsers. As the more popular Web browser, IE is likely a bigger target by hackers wanting to get the biggest bang for their buck and is also subject to more publicity about security vulnerabilities.

However, it's the unpublicized exploits users should be most concerned about, primarily because they're more likely to fly under the radar and less likely to be addressed or repaired in a timely manner. The fact is, there is no safe browser. And according to security research firm Secunia, Firefox was actually significantly less secure when compared to other browsers, receiving the highest number of browser exploits in 2008.

Myth No. 8: A Web App Is Secure If It Has That Lock Icon In The Corner

The lock icon indicates there is an SSL encrypted connection between the browser and the server to protect the interception of personal sensitive information from external threats. The lock icon is often used by sites transmitting sensitive financial or personal information to verify that it is legitimate. However, that little symbol does not necessarily indicate the absence of information-stealing malware.

Meanwhile, some malware can exploit vulnerabilities to spoof SSL certificates, impersonate legitimate sites and trick the user into submitting sensitive information to a malicious site. Hackers spoof the SSL symbol in elaborate phishing schemes that replicate bank, credit card or PayPal sites, which are challenging, if not impossible, for the average user to identify as fraudulent. As such, the infamous padlock icon could potentially provide a false sense of security, representing one more way for hackers to take advantage of users.



Myth No. 9: Links Sent From Facebook 'Friends' Are Safe

Did that message from your best Facebook friend seem a little weird the other day? It read something

like, “Hey, I caught you in a video. Check it out,” along with an embedded link. It was impossible to resist, so of course you clicked.



But when you did, it linked to you to a weird landing page where nothing happened.

Chances are your real Facebook friend had nothing to do with this. These kinds of attacks—called spoofing attacks—are becoming more common on popular social networking sites. Hackers will hijack a user's social networking account and then gain entry to their contact list to distribute spam or malware. Which means that sometimes, you can't even trust that your friends are your friends.

In general, view all links delivered on social networking sites with skepticism, and avoid clicking if there's even a shadow of doubt it wasn't sent by your friends.

Myth No. 10: Social Networking Sites Are Safe Because Only 'Friends' Are Included

In recent years, social networking sites such as Facebook and Twitter have exploded in popularity. But security levels have failed to keep pace with their rocketlike success. All you have to do is read the news to find out about the latest worm or security threat on Facebook.

True to form, hackers are capitalizing on the explosion of social networking use, leveraging the trust that users have on the network to launch malicious attacks. In fact, hackers are routinely launching spoofing attacks— impersonating a user's profile—to entice other users to click on malicious links and download malware onto their computers. And while users might have developed a healthy amount of skepticism when opening attachments and links delivered via e-mail, that same skepticism has yet to translate to social networking sites.



As such, Facebook and other social networking users should exercise caution when clicking on links, opening videos on these sites—even if they're sent from someone the user knows and trusts on their network.

No. 1 rule of thumb—don't put anything on social networking sites that you wouldn't want exposed to the world, because chances are one day it will be.