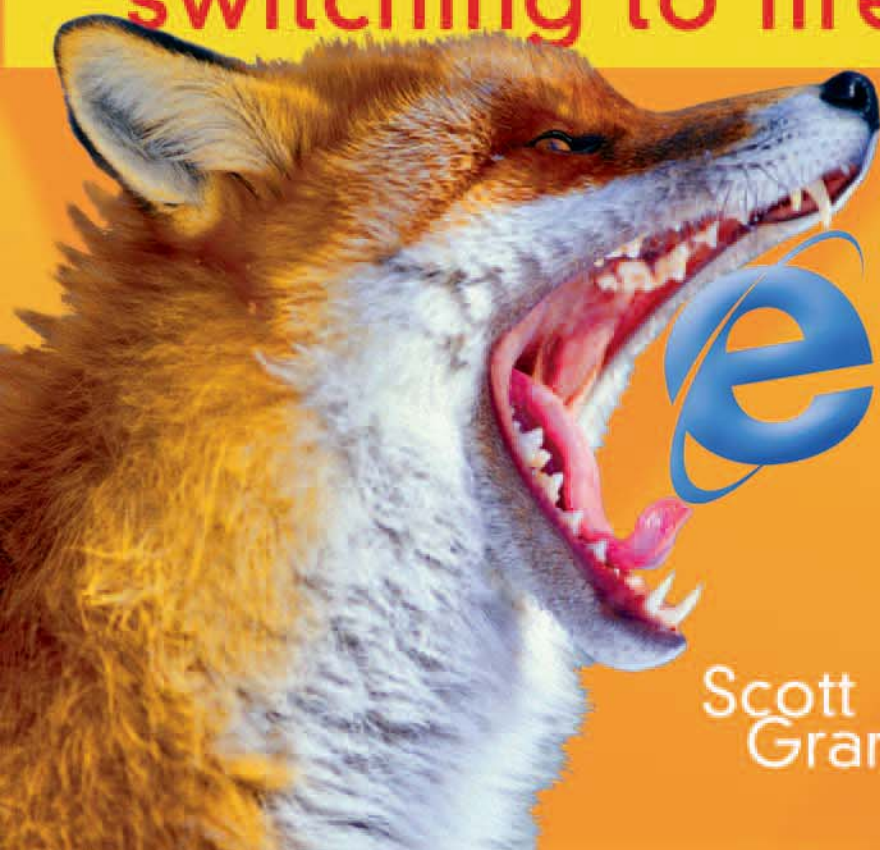


don't  
on the click  
blue e!

switching to firefox



Scott  
Granneman

## Safety and Security

Perhaps the main reason folks are quitting IE in droves is that the browser is plagued with security issues. I'll make this short and simple: Firefox is more secure than IE out of the box, Firefox implements security features more intelligently than IE, and Firefox fixes security issues faster than IE. I'm not saying Firefox is perfect; I'm saying it's better. A lot better.

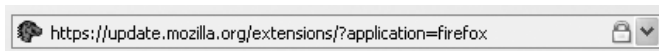
### Hey! You're on a Secure Page!

Every web browser warns users if they are entering or leaving a secure, SSL-encrypted web page. Firefox is no different, as Figure 5-14 shows.



**FIGURE 5-14.** Firefox tells you if you've requested an encrypted page.

Similar alert dialogs open if you're leaving an encrypted page, if a page has a mix of encrypted and unencrypted content, if you're submitting form content over an unprotected connection, and so on. That's good. You want that in a web browser, especially if you're the kind of person who doesn't pay attention to web addresses. However, Firefox goes beyond a simple alert box to let you know you're on a secure web page. Take a look at Figure 5-15—does it look a little different from your standard Location Bar?



**FIGURE 5-15.** Firefox makes it obvious that you're on a secure web site.

Most web users know that if they go to a secure site (such as Gmail or an online banking site) to enter or view sensitive information, the beginning of the URL changes from *http://* to *https://* and a little gold lock appears in the Status Bar at the bottom of the browser. These are nice indicators, but they're not exactly obvious to everyone—it's easy to over-

look the little lock, and you may not always scrutinize the URLs in the Location Bar. Firefox fixes that problem. If you hit a secure site, you still get a changed URL and you still get a little gold lock, but now you get something extra: the entire address bar turns gold, and a little gold lock appears to the right of the URL. This is flat-out brilliant. Now it's easy to see, and hard to ignore, that you're on a secure web site.

### **Chameleon**



Try it right now: head over to <http://update.mozilla.org>. Notice that you end up at <https://update.mozilla.org> and that the color of your Location Bar changes. Thank you, Firefox!

## **Anti-Phishing Measures**

“Phishing” is a growing problem on the Web. Basically, a bad guy sends you an email that appears to be from a bank, an ISP such as AOL, or an e-commerce site such as eBay or PayPal. The email informs you that there are problems with your account, that someone has been illegally accessing your funds, or that the company is performing a “security audit” (you get the drift). In any case, the email requests that you click on a URL and fill in the needed information on the company’s web site.

You click on the URL, and the web page really does appear to be that of Citibank, or AOL, or Paypal. You fill in the asked-for information, including your username and password, your account number, and your credit card details, and then you hit Submit. Guess what? You just sent your most valuable information to a criminal in Russia.

Phishing works because the bad guys know how to obfuscate the URL of the web site you’re on to make it appear that you’re on Citibank’s web site when in fact you’re somewhere else. Here’s a sample URL that illustrates the issue:

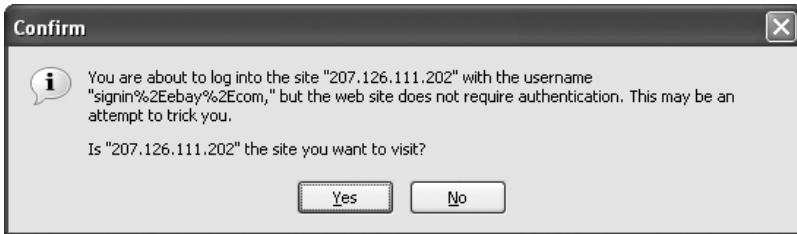
<http://www.mozilla.org&item%20blah:4356abdc@evilhackerdude.com/gotcha.htm>

Many users would see the *www.mozilla.org* part of the address and assume that they are on the Mozilla.org web site. The problem occurs because of the way browsers allow users to log into password-protected web sites. The usual method involves a URL of this form:

http://username:password@www.website.com

Take a look back at the phishing URL. See now how the username is *www.mozilla.org&item%20blah*, the password is *4356abdc*, and the real web site is *evilhackerdude.com*?

Phishing is a big problem, and it's getting worse. Fortunately, Firefox is smart enough to recognize if something fishy (phishy?) is going on. If you go to a site that has the *username:password* combination in the web address, Firefox opens up a dialog box similar to that seen in Figure 5-16.



**FIGURE 5-16.** Firefox won't let web pages lie about who they are.

That's smart—very smart. Firefox still allows you to use the *username:password* method for sites that are legitimate, but it warns you in a way that makes phishing sites obvious.

### **Crude, but effective**

IE's solution? Just remove support for URLs in the form *username:password@www.address.com* completely. If you have a flat tire, abandoning the car will solve the problem.

## **Smart Update**

I have to give credit where credit is due: Microsoft's Windows Update, introduced first in Windows 98, is a great thing. After all, if your operating system is that buggy and vulnerable to constant security problems, you should make it as easy as possible for your users to keep up to date

with your never-ending stream of patches, fixes, and updates. To this day, Windows Update is a great first step to keeping your OS (relatively) safe and secure.

Other programs since then have realized the value of using the Internet to provide users with software updates, and Firefox is no exception. At any time, a user can go to Tools → Options → Advanced and press the Check Now button in the Software Update section to see if any Firefox updates are available. As nice as that is, though, most users will never remember to perform that action, so Firefox helps everyone out by automatically checking for updates, not only for the browser itself, but also for any browser extensions and themes that you have installed. If an update is available, Firefox displays a notifier in the upper-right corner of the browser, just like in Figure 5-17.



**FIGURE 5-17.** Firefox lets you know if updates are available.

Different colors tell the user about the types of updates that are available:

*Green*

Extension or theme updates are available, but they're not vitally important.

*Blue*

Extension or theme updates are available, and they're important.

*Red*

An update is available for Firefox itself.

If you hold your mouse over the notifier, a small tool tip appears stating that new software is available. Clicking on the notifier opens the Firefox Update window and immediately begins downloading information about any available updates. At that point, you can choose which updates, if any, you wish to download and install. What could be simpler?

Again, I have to give Microsoft credit for bringing the idea of simple online updates to a mass audience. And again, I have to give Firefox credit for, as it has in so many ways, taking Microsoft's ideas and improving them!

## No More Killer Scripts

A programming language called JavaScript is widely used on the Web today, and it provides lots of useful functionality. Occasionally, however, a web developer will code his JavaScript poorly, or will only code it for IE and fail to test it in browsers like Firefox. This can be problematic. In the past, running these bad scripts might have caused browsers to crash, or to lock up and stop responding. Firefox takes care of that problem, as you can see in Figure 5-18.



**FIGURE 5-18.** If a script could potentially cause problems, Firefox will warn you.

If a killer script threatens Firefox, the warning dialog helps alleviate the problem. Feel like taking a chance? Press Cancel and see what happens. Things may be fine. I've tried Cancel before on certain sites, and after a moment, I was able to continue on my merry way. I've also seen Firefox crash, but that's not the browser's fault: after all, it warned me. If you want to preserve your browsing session, choose OK and drive a stake into that killer script. Follow that up with a polite email to the site's webmaster, asking him to test that page in Firefox. You may be helping a lot of fellow Firefoxers.