

Advertisement: The Orange Savings Account 3.00% APY No Fees. No Minimums. ING DIRECT Save your money® Member FDIC

washingtonpost.com > Technology

Subscribe to The Post

RECENT POSTS

- Zone Alarm Update Fixes Microsoft Patch Problem
A Baker's Dozen of Security Updates for iPhone 2.0
Speeding In Maryland Could Be Hazardous to Your Identity
Ghosts of Java Haunt Users
U.S. Supreme Court Judge Data Exposed Via P2P

- Stories by Category: Cyber Justice, Fraud, From the Bunker, Latest Warnings, Misc., New Patches, Piracy, Safety Tips, U.S. Government
Stories By Date: Full Story Archive

RELATED LINKS

- The Archives
Security Fix Live: Web Chats
About This Blog
Password Primer
7 Security Tips
Technology Section

SYNDICATE

- XML RSS Feed
Google
MY YAHOO!
NEWSBURST
Pluck
newsator
Bloglines
netvibes
MY MSN
MY AOL
ROJO



Brian Krebs on Computer Security

About This Blog | Archives | XML RSS Feed (What's RSS?)

Study: Site Redirects Abundant, Aid Phishers

An examination of nearly 2.5 million Web pages at some of the Internet's most popular and trusted sites turned up at least 128,000 links that could be manipulated by fraudsters and virus writers to make online scams more believable, a study released this month found.

Scammers and phishers are taking advantage of commonly used coding used in "redirects" to divert traffic from reputable Web site to sites that could harbor malicious software or phishing schemes.

Redirects aren't all bad. In essence, they are Web links that are used to forward traffic from one site to another. They can be useful when Web site owners want to move content around and don't want old links leading to dead pages. Redirects can help selectively re-route traffic: For instance, www.example.com may want to forward any requests for a specific Web page to a third-party site. In addition, well-known companies use redirects to forward traffic from site names they own that include common misspellings of their brand name.

But redirects can be abused when Web sites that employ them leave them "open," or permit them to forward traffic to any site on the Internet. Phishers and virus writers constantly seek out these kinds of security vulnerabilities in trusted Web sites, because the bad guys know people are more likely to click on a link if they believe it will take them to a site they know and trust.

Understanding how redirects can be abused is often easier shown than explained. For example, I altered this link -- found at About.com and originally used to help site visitors locate content that had moved to another portion of About.com -- so that it instead brings you right back here to Security Fix. As does this redirect at Web ad giant ATDMT, this page at MacDailyNews, and this link from the National Sex Offender registry.

(By hovering over a link -- or by right-clicking on one of these links, selecting "Copy Shortcut," and pasting the URL into another Web browser -- you can see how it was formatted to take you from one Web site to where I wanted it to go.)

Researchers at Indiana University sought to find out just how many open redirects are now out there by building a computer program that crawled tens of thousands of the most-visited sites, using sophisticated formulas to automatically discover when sites were running open redirects.

Advertisement: 3G LaptopConnect Card WORKS IN MORE PLACES WORLDWIDE THAN ANYONE ELSE CONNECT NOW FREE after mail-in rebate ROLL OVER FOR DETAILS at&t

Ads by Google

- The Real Barack Obama The truth behind the candidate - "Barack Obama Exposed" - Free! www.HumanEvents.com
Jesse Jackson News Full Story on Jesse Jackson's Crude Remark About Obama w/ News Toolbar News.alottoolbars.com
10 Rules of Flat Stomach Drop 9 lbs of Stomach Fat every 11 Days by Obeying these 10 Rules. FatLoss4idiots.com

Indiana Ph.D student [Craig Shue](#) said he and his fellow researchers were surprised by the number of high-profile Web sites with open redirects, particularly since they are not difficult to identify or fix.

"When someone else can manipulate your redirect and craft a link however they want, that can really hurt your brand. If you're **eBay** and you have an open redirect in your site, that makes it really easy for a phisher to incorporate the actual eBay site," in a link that ultimately forwards people to a counterfeit eBay page, Shue said.

In fact, the screen shot to the right of a **Phishtank.com** writeup shows a portion of a link leading to a live eBay phishing site that uses an open redirect on the auction giant's site.

Interestingly, this phishing site has been live nearly six weeks now: Note the Jun. 5th submission date (I took that screenshot of the phishing site last night). Another recent Phishtank submission shows [an open redirect on AOL.com](#).



A redirect link at eBay.com that a Phishtank user spotted in an e-mail (above) leads to a fake eBay site (below)

Redirects are nothing new. Indeed, some of the Internet's biggest Web sites -- particularly Google -- used to host large numbers of open redirects. But as the Indiana study shows, open redirects remain very easy to find and exploit.

It's important to note that the researchers' bots found 128,000 open redirects just using regular HTML code. They didn't bother trying to craft links that used sneakier or more advanced methods -- such as Javascript or [URL encoding](#) -- which would have no doubt drastically expanded the number of open redirects uncovered.

Shue will present the Indiana University study at the [USENIX Workshop on Offensive Technologies \(WOOT\)](#) later this month in San Jose, Calif. The paper is available from [this link here](#) (PDF).

By Brian Krebs | July 16, 2008; 4:35 PM ET [Fraud](#) , [From the Bunker](#) , [Latest Warnings](#) , [Misc.](#) , [Safety Tips](#)  
Previous: [Zone Alarm Update Fixes Microsoft Patch Problem](#) |

**Comments** Please [email us](#) to report offensive comments.

**Post a Comment**

We encourage users to analyze, comment on and even challenge washingtonpost.com's articles, blogs, reviews and multimedia features.

User reviews and comments that include profanity or personal attacks or other inappropriate comments or material will be removed from the site. Additionally, entries that are unsigned or contain "signatures" by someone other than the actual author will be removed. Finally, we will take steps to block users who violate any of our posting standards, terms of use or privacy policies or any other policies governing this site. Please review the [full rules](#) governing commentaries and discussions.

Name:

Comments:



Preview

Submit

### [Blog Archives](#)

[XML](#) [RSS Feed](#) [Subscribe to The Post](#)

© 2008 The Washington Post Company

#### Ads by Google

##### [Barack Obama Soda](#)

Show Off Your Thirst For Obama! Great Gift, Fun. From Jones Soda.  
[www.CampaignCola.com](http://www.CampaignCola.com)

##### [Barack Obama Posters](#)

Decorate your walls, or cubicle with these Obama posters.  
[www.DemocraticStuff.com](http://www.DemocraticStuff.com)

##### [Barack Obama in 2008](#)

Show Your Support! Buy Obama Tees, Stickers, Buttons, Yard Signs  
[www.CafePress.com](http://www.CafePress.com)

SEARCH:



washingtonpost.com



Web: Results by Google™

[Search Archives](#)

[NEWS](#) | [POLITICS](#) | [OPINIONS](#) | [LOCAL](#) | [SPORTS](#) | [ARTS & LIVING](#) | [CITY GUIDE](#)

[JOBS](#) | [CARS](#) | [REAL ESTATE](#) | [RENTALS](#) | [SHOPPING](#)

**washingtonpost.com:** [About Us](#) | [Work for Us](#) | [Advertisers](#) | [Site Map](#) | [Search Terms](#) | [Topics Index](#) | [Make Us Your Home Page](#) | [mywashingtonpost.com](#) | [Mobile](#) | [RSS](#) | [Widgets](#)  
**The Washington Post:** [Subscribe](#) | [Subscriber Services](#) | [Advertisers](#) | [Electronic Edition](#) | [Online Photo Store](#) | [The Washington Post Store](#) | [National Weekly](#)  
**The Washington Post Company:** [Information and Other Post Co. Websites](#)

© Copyright 1996-2008 The Washington Post Company | [User Agreement and Privacy Policy](#) | [Rights and Permissions](#)