

How to stop phishing

WE'VE ALL RECEIVED an e-mail that appears to be from a reputable bank or financial institution. Maybe it wasn't a bank—maybe it claimed to be your online stock trader of choice. A recently publicized IRS e-mail scam (just in time for April 15) is a relatively simple one. It grabs your attention by telling you that you are eligible to receive a tax refund and lists the amount. The e-mail then directs you to click a link to access a form for your tax refund. When you click on that link, you'll go to a bogus site that asks you for personal information, including your Social Security number. This is a timely, though unfortunate, example of a phishing attempt.



The new IRS phishing scam is just one of thousands out there. Regardless of the hook, the intent is the same. The perpetrators want access to

they provided appeared genuine and led to the correct eBay sign-in page, signin.ebay.com. If users clicked on this page, embedded parameters in

Whatever information these con artists are phishing for, wouldn't your users be a lot happier if you could prevent this from happening to them? If you own F5's BIG-IP Local Traffic Manager running v9, you already have the ability to make use of F5's custom, in-line scripting language, iRules. And now there's a new iRule that's been written for you that's designed to help stop phishing in its tracks.

Using this new iRule on a BIG-IP in front of your website allows you to deny the would-be phishing site access to content it needs to disguise itself. You can also supply your website with content that warns a user that the bogus site may be a phishing site not authorized by your company.

The following example demonstrates not only how to check for suspicious requests that originate from referrers that haven't been authorized to use your site's content, but also how to stop them

outright, or to inject code into the HTTP response that negates their ability to duplicate your site. This is done in three separate steps:

- 1** Define a list of valid referrers in the form of a class. This is a list of those sites that you expect to be linking to the content on your site.
- 2** Define another class of file types that should not be linked to except by the referrers in Step 1.
- 3** Check to see if an invalid referrer is trying to serve data from your site and what kind of content it's trying to serve. If it matches the file types in Step 2, block it. If not, insert some custom code to help prevent phishing attempts.

This is just a single solution that iRules can provide. The true power of iRules lies in its flexibility, which enables you to craft custom solutions to meet your specific needs.

Phishing scams have become a sad fact of life—but developers can stop them, with a little help.

your account, and all they need you to do is provide some small piece of personal identity information. Sometimes it's your Social Security number; other times, it's your account number or your username and password. They'll ask for this by saying there's been some major change or that you need to update your account information.

Many of the scams are growing more creative, if such a word is appropriate. For example, in July of last year, a different type of phishing scam started with fraudsters sending emails asking eBay users to update their accounts. Disarmingly, the link

the normal character stream redirected users away from the page after the sign-in page to a fake phishing page via an open relay hosted at servlet.ebay.com.

The anti-phishing iRule is free, easy to set up, and available now for all F5 BIG-IP Local Traffic Manager v9 customers. Visit F5's DevCentral developer community website at <http://devcentral.f5.com>.

VISIT DEVCENTRAL

F5's online developer community

DEVCENTRAL IS A GREAT WAY TO get more out of your F5 products with free iRules, tech tips, and tutorials. Join DevCentral for tools, techniques, and collaboration to help you build solutions with F5's iControl and iRules, which enable the network to truly serve as an extension of the applications you're delivering.

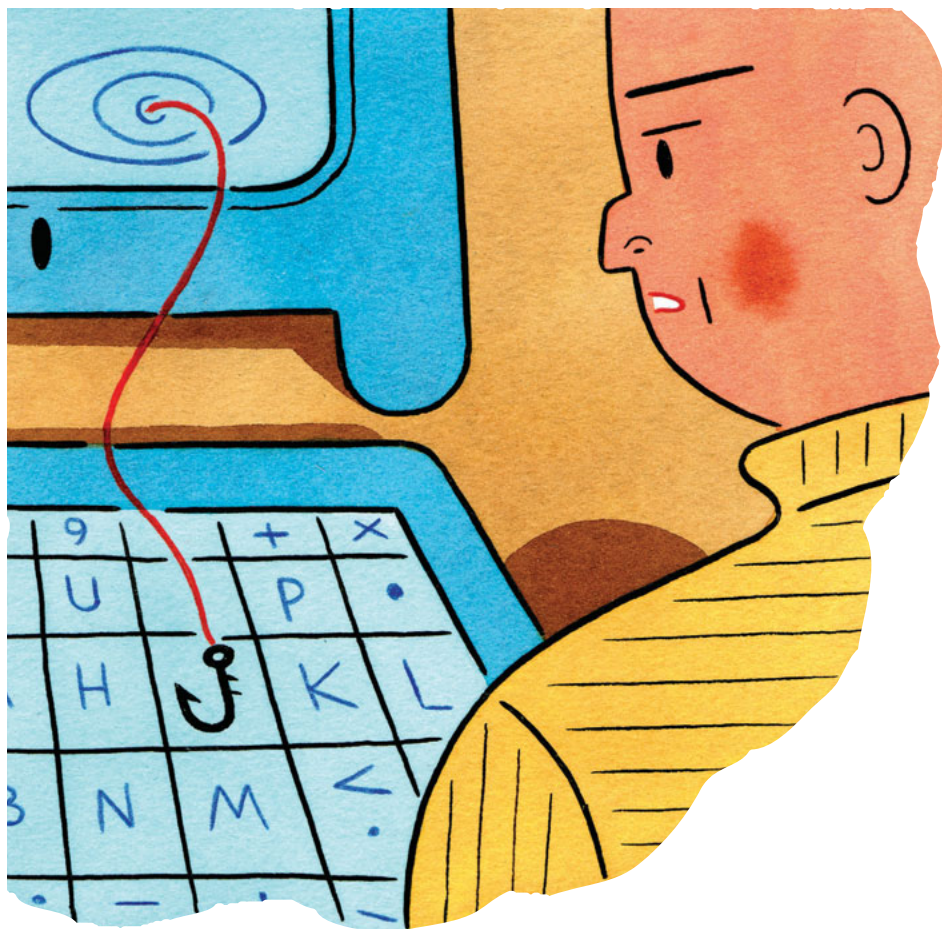
It's easy to get started. Check out the **iControl Quickstart Guides** for Java, Perl, or .NET and review the **Docs and Tips** section. **Code-share** is a great place to download and post application samples. Be sure to visit **Downloads** for SDKs from F5. If you have questions about iControl or iRules, **Forums** are your source for answers and ideas.

Visit <http://devcentral.f5.com> for more information.

About F5's iRules and iControl API

F5's iRules represent a unique approach to how application traffic can be intercepted, parsed, modified, and routed based upon customizable logical policies. iRules, exclusive to F5 Networks BIG-IP v9, utilizes a standard scripting language—Tool Command Language (Tcl)—to construct these policies that can apply to any IP

application. The iRules approach makes it possible for you to use many of the standard Tcl commands, not to mention a robust set of extensions that BIG-IP provides to help you optimize and secure application traffic to meet your specific requirements, expand upon an application's functionality, or even help offload some of the work to the network layer. For more information, visit F5's online developer community, DevCentral, at <http://devcentral.f5.com>.



NEW ONLINE VIDEO:

Anti-phishing, step-by-step

Want to see the anti-phishing iRule in action? F5 has created a new video that shows you, step-by-step, how to implement the anti-phishing iRule with your BIG-IP v9 product. Visit the following to learn more:

<http://devcentral.f5.com/weblogs/dctv/archive/2006/01/16/iRulesNoPhishing.aspx>.



See the iRule anti-phishing solution in action in a short video from F5.