

The Internet Marketing Chronicles

Powered By: [Internet Marketing Challenge](#)

January 24th, 2002 - "Protect Your Top Search Positions - Part 1"

IMC is published weekly and distributed to over 150,000 Internet marketers and webmasters who have asked to receive it.

1. [EDITORIAL](#): "Protect Your Top Search Positions - Part 1"
2. [TOOL OF THE WEEK](#): CoffeeCup Password Wizard v4.0
3. [SEARCH ENGINE BYTES](#): Q & A With Stephen Mahaney
4. [CONTACT THE CHRONICLES](#): Got questions? Get Answers!

1. [EDITORIAL](#): "Protect Your Top Search Positions - Part 1"

If you have had the chance to look through our full search engine series, issues #278 - #280 of The Chronicles... then you already have a good head start in the search engine optimization game.

But once you have all of your pages optimized, how are you going to protect the public from stealing the code that you worked so hard to create? It's actually easier than you think if you use the web based cloaking software that I've been running for the past 2 years.

I know many of you are already familiar with cloaking software and the issues regarding it's usage in the search engines. Will it get your site in trouble? Or will it help you to provide better content to both viewers and search spiders?

To better answer this question, Michael Campbell (a leading search engine specialist and author of best seller "*Nothin' But Net*"), was kind enough to allow us to reprint a recent article he wrote.

In this previously unreleased article, Michael takes an in- depth look at the risks, advantages and implementation of cloaking software from the view point of a developer of a popular cloaking product, an experienced search engine optimizer and a webmaster of a large ISP.

I hope you enjoy this weeks special editorial.

Finest Regards,

Boris Chow

Internet Marketing Challenge

P.S. If you haven't read issues #278 - #280 of the Chronicles, I encourage you to do so now by going to...

<http://www.marketingchallenge.com/backissues/>

Someone Stole Your Web Site.... Oh No! Not Again.... Sigh!

The question is, "*What can we do to protect ourselves from all this rampant stealing of intellectual property?*" Answer... protect ourselves with some very effective technology and good business sense.

You'll be happy to know that I purchased new software, just so I could test and review it for you. I've been testing it out as a content delivery system and search engine positioning tool. Not only does it **prevent anyone from seeing your optimized web pages**, no one will be able to steal anything from you ever again.

What I purchased is commonly referred to as Cloaking Software or IP Delivery Software. After much research, I decided on the Food Script from John Heard and Beyond Engineering.

I used to think that cloaking would be too expensive, too technical, or too hard to install, or hosting companies wouldn't allow it. But now I find out it's none of those things. I talked with three key people **before I made my decision** to buy the Food Script.

I interviewed John Heard, creator of the Food Script. Boris Chow - of Internet Marketing Challenge - who went through the process of buying and installing the script. And Paul Edwardson, for a webmaster's opinion on hosting a cloaked site.

How Does The FoodScript Work?

Every computer connected to the Internet **has a unique number** that identifies it from all the other computers connected to the Internet. It's known as an IP address.

It's similar to the address where you live, it's unique. It makes sure postal mail gets to you instead of someone else. The **search engines also have IP addresses** that they operate from, just like any machine with a dedicated Internet connection.

When a spider, crawler or browser requests an HTML page from a server, **It announces itself and makes a request**. The machine making the request states, "*I'm IP address 123.456.789.123 and I'm requesting your index.html page.*" On a normal web site the request is granted and the index page is served. **What happens on a cloaked site** is very different.

The cloaking software doesn't just serve up a page with no questions asked. It quickly looks into a list of IP addresses to find out if the IP address of the machine making the request is a known search engine spider or not.

If the requesting IP address does NOT appear in the list of known search engines, the request is considered to be a human just like you or me, sitting in front of our computer, innocently surfing the web with a normal browser.

If the IP address IS a known search engine, the **cloaking software quickly identifies** which one and serves it a custom designed web page. The spider gets fed a web page that was optimized specifically for it.

This means when a Hotbot IP address makes a request, it gets shown the Hotbot page. When an AltaVista spider makes a request, it gets shown the AltaVista page. When you or I, or anyone else makes a request, we get shown the "*common*" page.

This "common" page does not need to be optimized for the search engines. It is free from any design constraints and if someone steals the HTML code from your common page, they are getting what you have chosen to serve and show the public. They do not get the HTML code that got you to the top of the search engines.

My Conversation With Paul Edwardson

The first thing that I needed to do was to be sure that cloaking software would be ok with several hosting companies. I checked various hosting agreements and didn't see any reference to cloaking or IP delivery software.

I asked Paul if his company supports cloaking and he maintains an attitude of ambivalence, neither liking or disliking the idea. Paul said, "*Cloaking software is no different in nature than bulk e-mailer software. You can either use it to spam people or send a monthly newsletter to your permission based opt-in subscribers. Cloaking and bulk mailers are both very powerful tools, **it all depends on how they are used.***"

Although Paul does not have an official policy posted on his site at the time of this writing, he says, "*So long as the software is being used in an ethical manner, delivering relevant content, he doesn't have a problem with people using IP Delivery software on his servers, neither should any webmaster. If it helps optimize your pages while protecting the HTML code that's fine. Just so long as the person is **not spamming or delivering unrelated content.***"

I uploaded the Food Script for Paul to look at, and he said **the software will work fine on his servers**. He said, "It would be easy to install, any '*tech head*' could do it."

On most servers, "*Any hosting account from a Basic Version on up will work, so long as you **have your own cgi area**. You should be able to get the software running on your own, if not, it looks like there's extensive help from Beyond Engineering.*"

- Paul Edwardson is a webmaster, self proclaimed CGI guru, and owns a privately held hosting company in San Francisco, California.

My Conversation With John Heard

My first mission with John was to find out **how easy the software would be to use** and what kind of help was available. After all, tech stuff and servers are not my forte.

John explained, "***There are detailed step by step instructions and screen snap shots to assist you in installing the software. If you try installing it and can't get it going, my people will go so far as to FTP into your server to see what you've done.***" They'll do everything they can to get you up and running.

Whether you need help or not, depends on your area of expertise. If you run the server and are comfortable installing scripts, you are the type of person that his tech support people usually deal with.

If you are a business owner, a designer or writer (like me), your web master - the person that looks after your servers - should be able to install the script for you.

(By the way, the documentation was good. I didn't mind reading it. **It was a very good experience.** It gave me a clear idea on how to name my files and where to store them on the server to make the Food Script work. But when it came time to install and edit the actual CGI code, I slipped my webmaster a few bucks and let him do it. :)

John strongly suggests that you **try and install the software yourself**, and only if you run into a stumbling block to ask for assistance. If they install it for you, you won't understand how the software works. If you install it yourself, even though you might run into a few snags, at least you'll fully understand it.

John will answer your support questions either over the phone or in the support forums. They deal with all sorts of people at various technical levels. At the very least you'll need to read the documentation so you'll know how to name your web pages and where to store them.

Once you have the software installed, that's when the real work begins. Think of cloaking as a multidimensional web site. You'll eventually have ten different versions of the same site. So where you once had a 5 page web site, you'll now have a 50 page site. 10 different versions of the same 5 page site. One cloaked site for each major search engine technology.

I asked John about public statements by companies like Google, that say cloaking is spamming. John said, "*It's the word 'cloaking' they are equating with the word 'spam'. Even though the pages that are being shown to the search engines and the pages that are being shown to the humans are NOT spam, they are still saying that the word 'cloaking' is synonymous with spam.*"

Sure enough, if you mention cloaking to a search engine technician, the hair on their neck stands up, they stomp their feet and fling dust into the air. If you say, "*I provide highly relevant content delivery specific to a particular browser's interest.*" Well alrighty, that's ok then. They'll nod their heads in agreement. They like it. It's not even an issue then.

What about my favorite shareware download site? It knows I'm on a Mac and only shows me Mac stuff. Windows users get a VERY different page. **Is this cloaking or spam?** Yes, according to their definition, any time two people - or human and spider - see the same page a different way, it's spam.

This brings up the issue of personalization software that remembers what you purchased on your last visit to a web site. It might say, "*Hi Michael, last month you bought these books, might we suggest these?*" This page - when spidered - **will look different to a search engine**, so technically it's spam.

Where are the lines drawn? It's a very hard to determine thing. Is it spam or not? The search engine company might think so. And its difficult to know where all this is going to lead.

John told me, "*There are so many things you can do that are spam free. For example, a lot of people use a left hand menu with images, which is great for people, but lousy for search engines. On the search engine page you can replace that imagemap with text links that contain keyword data. It's a little thing that can make a big difference in search engine positioning.*"

So you could **feed the search engines very basic HTML**, like nothing more than page title, headline tags and paragraphs of text. No graphics or font tags or style sheets, just real basic stuff, so they index every single word on the page. Every single word on the page has a specific purpose of building just the right theme and keyword density.

John says, "***The real issue or question for the search engine companies is, 'How far can we deviate from the human content versus the search engine content?' That's the big question. Google and Inktomi are discussing the issue right now. Exactly how much difference can there be between what their spider sees and what a human sees?***"

I agree with John that these things should be posted as a matter of policy. Surely a search engine company should be able to make an official post on their web site as to **what constitutes spam**.

But that's the major issue, **most search engines don't have a policy**. It's being determined by the search engineers on a case by case basis, whenever they have a need to review a site. It's vigilante vengeance at its finest.

John has been trying to get definitions from them, since instances of what the human sees and what the spider sees are all over the place. "*What about sites that have*

dynamically generated news and weather information. If a spider comes and indexes the page, then comes back 10 minutes later, the page will be different." How true indeed.

So if the search engines do make a filter that compares content, there will be all sorts of legitimate pages getting caught in it and filtered out. A narrow filter would catch any site with active content, a broad filter would catch heavy spammers only. It all depends on how they are going to approach the issue of what is spam and what isn't.

Bottom line, **should you cloak or not?** IP Delivery is a controversial and very powerful tool. You have to be very careful how you use it. My personal opinion regarding cloaking? Be fair, honest and ethical. Do not spam. Do not steal pages from other web sites. Cloaking can be a good or evil. **It all depends on how you use it.**

Like I said in one of my earlier rants, one of my so called friends noticed I was high in the search engines for a particular product. Being too lazy to write his own ad copy, he **copy and pasted my web page** into his and is now competing with me to sell the same product, using my very own words! But what's surprising is how **many people are taking it a step further.**

Not only do **they steal your page**, they then cloak it, so you don't know they've stolen it. Then they compete against you in the search engines using your very own page. When you click on their link in the search engine, you're directed to the thief's "common" page. But in reality the search engine - through cloaking - is being fed what **used to be your top scoring page.** Yes, be concerned... this is happening every day!

Now what if they subscribe to one of those services where the search engine will come and re-spider their page every 48 hours? They steal your page, cloak it, tweak it slightly **and come out ahead of you in the search engine**, within 48 hours. Pretty sickening I agree, but that's just a sampler of what's going on out there.

John tells me the number one reason people are calling him is that they are **tired of people ripping off their code.** There's a lot of page theft going on. There's even reports of search engine optimization firms and pay per click companies engaging in this stealing and cloaking of pages.

So is it safe to use cloaking software? John says, *"I've used the Food Script Software as a webmaster since 1995 and have never had a single one of my domains banned."* John further suggests you can stay out of trouble by following these **two simple rules:**

1) *"If you go down the wrong end of IP Delivery and **try to mislead somebody**, or get irrelevant, or if you use content that is not your own, then **you're just asking for trouble.** If you use cloaking software to protect stolen pages, it's not going to help you either. Sooner or later you will get caught."*

2) "If you use your own original content, that is totally relevant to the search phrase, and you're giving the user of the search engine exactly what they're looking for, **without misleading them or taking them down the wrong path in any way, then you're helping the search engine, the user of the search engine, and your company."**

-- John Heard is the president of Beyond Engineering, creator and maintainer of the Food Script IP delivery software.

Here's what Food Script can do for you....

Protect your html code from theft

Stop competitors from using your code against you

Serve keyword pages optimized to each search engine technology

Serve graphically rich "common" pages to the public

Update information on your pages without affecting positioning

Increase your conversion ratios through better communication

Increase your sell through ratios through better human experience

Break yourself free from search engine design limitations

To get your very own copy of the Food Script click here....

<http://www.cdzn.com/jhf/>

If you are still not convinced that you need the protection of the Food Script, I encourage you to read the second part of this article in next week's Chronicles.

I will be interviewing Boris Chow, a search engine optimization specialist that has used this script successfully on over 14 sites. You'll get his expert opinion on how this product fairs for the consumer.

May you have a safe, prosperous and theft free future.

Michael Campbell

About the Editor

Michael is the author of "*Nothing but Net*" and the Internet Marketing Secrets Newsletter.

Sign up free at: <http://www.InternetMarketingSecrets.com>

This article is Copyright 2002 Dynamic Media Corporation. All rights reserved worldwide. Reprinted here with permission from the author.

[Table Of Contents](#)

2. **TOOL OF THE WEEK: CoffeeCup Password Wizard v4.0**

This week's Challenge Tool was submitted by IMC.

"CoffeeCup Password Wizard allows you to create usernames and passwords to protect your Web pages without knowing Flash, Java, or HTML. You can create an unlimited number of username/password entries. This ability allows you to secure sensitive content on your Web site. You can set up the applet to send users to another URL of your choice should they fail to supply a proper username and password. You can also set the URL to which the user is sent depending on the username.

CoffeeCup Password Wizard works in frames and tables, and it allows you to control border styles, widths, and background colors. The previewer displays your work as you create. You can also view the HTML code as you go. A shortcut helps you browser-test your work while you create."

To get more information on this tool, visit: <http://www.CoffeeCup.com>

Have a Challenge Tool that worked for you? Want to share it? Send us the URL and a brief review of the resource (up to 7 lines) to:

Tool@MarketingChallenge.com

3. **SEARCH ENGINE BYTES: Q & A Sessions -- With Stephen Mahaney**

TOPIC: Will redirects get you blacklisted?...is there a better way to set up multiple entryways into a site?

QUESTION: I am doing some optimization analysis for a client who has purchased about 25 keyword specific URLs that are redirecting to their home page. They seem to be ranking pretty well on most of the search engines. I have always read that redirects are a sure way to get black listed from the SEs but maybe what I've read isn't accurate. Can you give me some info about this?

ANSWER: In general search engines don't like redirects. Normally, unless there is a real good reason for the redirect (like flash site content), it's better to build stand-alone pages or sites that emphasize each of those 25 keywords vs simply redirecting them to the home page.

Besides, that way you can use these so-called keyword specific information sites to build link popularity by cross-linking them with each other as well as with the main site. As noted in the se-byte answer above, this works best if the keyword sites are spread out over a variety of web hosting services to take advantage of the "*expert site*" factor gained by having incoming links from various Class C blocks.

Will they ban a site for redirects? Not normally unless there are quite a few of them or someone starts complaining about them. We doubt that a mere 25 redirect pages would cause much of a problem but we still recommend not using redirects if you can help it.

About This Contributor

Stephen Mahaney is one of the Industry's leading experts on top search engine placement. Stephen is the President of Planet Ocean Communications Inc. (Publisher of best selling ebook, "*The UnFair Advantage Book on Winning the Search Engine Wars*"), and Senior Editor for Search Engine News (a monthly look at the latest search engine changes and strategies). To maximize your search engine placements, pick up "*The Unfair Advantage Book*" today at:

<http://www.MarketingChallenge.com/senews/>

Are you curious, confused, or completely frustrated about search engines? Send your search engine question to:

<mailto:sebytes@MarketingChallenge.com> and include your name and website URL. If selected, your question will appear in a future installment of the Chronicles.

4. **CONTACT THE CHRONICLES: Got questions? Get Answers!**

Do you have Internet marketing questions? Do you want to share your thoughts? If so, send your lemons or your laurels at: Share@MarketingChallenge.com

Are you a successful cybermarketer? Do you want to contribute an article in exchange for some free exposure? If so, send your contribution, with your brief, promotional byline, to: Article@MarketingChallenge.com

Your FREE subscription to The Internet Marketing Chronicles ezine is brought to you by the Internet Marketing Challenge website. If you enjoy this ezine, chances are you will love the IMC Private Site where we and other highly-successful online marketers SPILL THE BEANS and share EVERYTHING we have learned the expensive way.

Click here NOW for INSTANT access:

<http://www.MarketingChallenge.com>

New to the list? Backissues can be found on the web at:

<http://www.MarketingChallenge.com/Backissues/>

Don't hesitate to forward a copy of this newsletter to friends and associates, but

please ask for permission before reproducing the content in any form -- we would like to know who you are.

To update your subscription information we have on file, enter your email address at:

<http://www.MarketingChallenge.com/Chronicles/>

To unsubscribe, enter your email address at:

<http://www.MarketingChallenge.com/Unsubscribe.html>

To subscribe to this newsletter, simply visit the URL below:

<http://www.MarketingChallenge.com/Signup.html>

Copyright 1998-2001 Internet Marketing Challenge 2000 LLC. All rights reserved. No part of this publication may be reproduced in whole, or in part, without the express written consent of the publisher. Registered with the Library of Congress. ISSN: 1525-8424

Internet Marketing Challenge

1664 Harbor Seal Drive, Point Roberts, WA, 98281

Phone: 800-505-8232 or 604-730-6979

Fax: 800-505-0507

Put your Newsletter on Autopilot. Increase Customer Loyalty With One Software Package:

The Internet Marketing Chronicles are sent to *over 150,000 subscribers* each week using the revolutionary "**Mailloop - E-mail Automation Software**".

Click here now to learn how Mailloop can **automate your daily email chores** in as little as the next sixty minutes... so that you can *spend your time promoting your business and exploding your profits* on the Internet.

| [TOP OF PAGE](#) |

| [EDITORIAL](#) | [TOOL OF THE WEEK](#) |

| [S.E. BYTES](#) | | [CONTACT](#) |