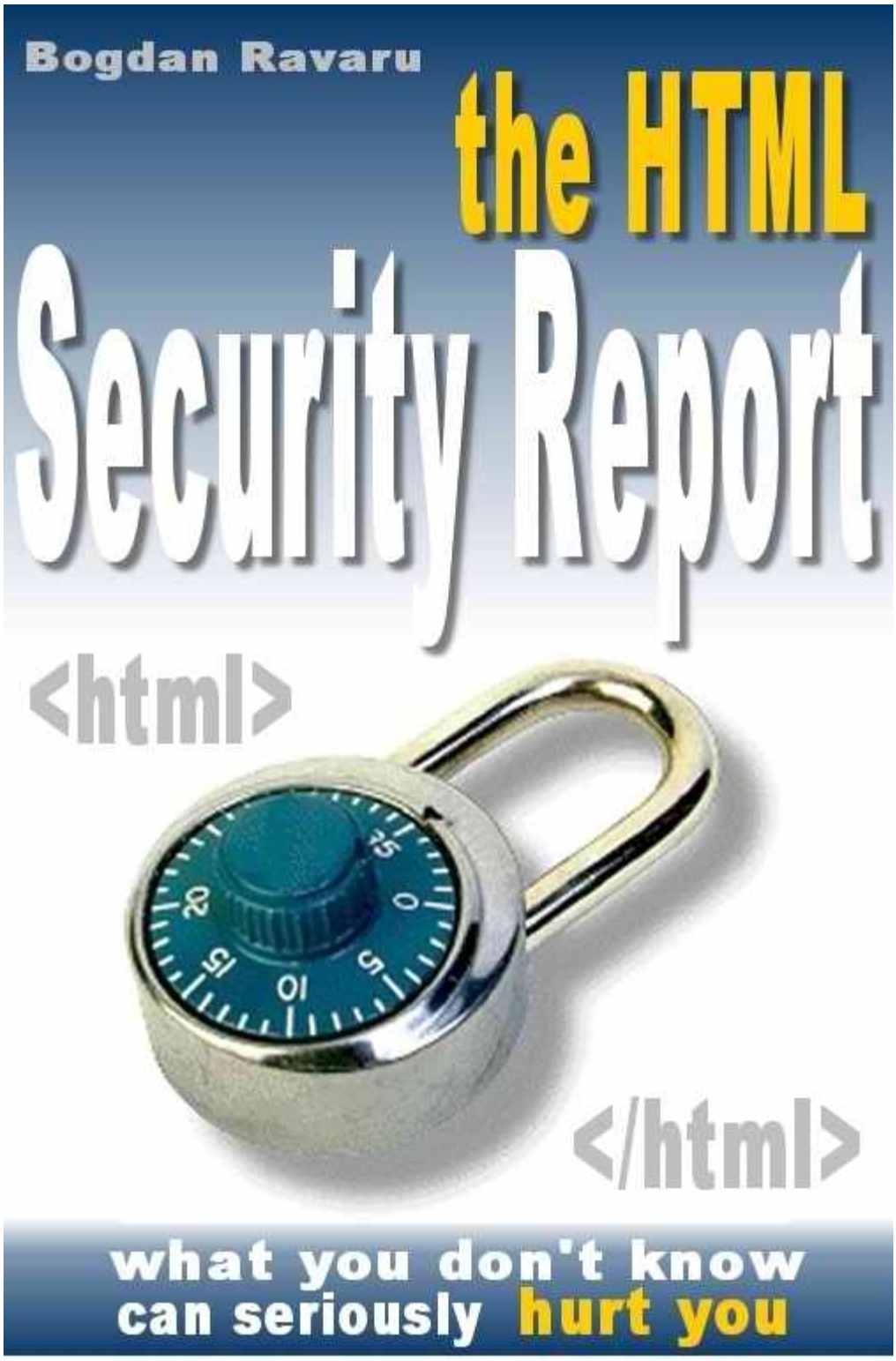
Bogdan Ravaru
the HTML
Security Report
<html>
</html>
what you don't know
can seriously hurt you

The **HTML Security**Report

Special Report from **Bogdan Ravaru**

“Are Your Visitors Stealing From You?”

Exposed At Last: The Dirty Methods Internet Thieves Use To Quietly Steal Up To 46% Of Your Profits And What You Can Do To Stop Them!

…what you don’t know can hurt you…

Legal Notice and Terms of Agreement

Before we begin, there are just a few "legal" things we need to cover (also known as *"my lawyer made me do it"* ☺)

While attempts have been made to verify information contained in this publication, neither the author nor the publisher assumes any responsibility for errors, omissions, interpretation or usage of the subject matter herein. This publication contains the opinions and ideas of its author and is intended for informational purposes only.

The author and publisher shall in no event be held liable for any loss or other damages incurred from the usage of this publication.

Published by:
Bogdan Ravaru
CEO & Founder of TheMarketingWizards.com

Warning: This is not a free report.

The suggested retail price for it is 17 US Dollars (17$)

Special Unadvertised Bonus

By purchasing this report you've qualified to receive Bogdan Ravaru's 5 days eClass completely free.

This special eClass **"The Confidential Diary Of A Marketing Wizard"** is guaranteed to help you increase your business with at least 77% in the next 5 days, with specific information like:

➔ Case Study: How I started my online business with absolutely 0$, made 70$ in my first month and increased this value 50 times in one year, ...and how you can do the same, only a lot faster

➔ How to take advantage of the one factor that can be used to predict your online success. **Warning:** This is the most important 'factor of success' on the internet!

➔ Analyzing one of the most common mistakes and the second most important factor of success. If you're not making enough sales & profits it might be because of this!

➔ Precisely what a 2 step marketing strategy is and why you should use one. Every affiliate should pay really close attention to what is revealed here.

➔ Exactly how to become a "Tiger Woods of Internet Marketing". How to stop your mind from unconsciously sabotaging your success and how to develop the money consciousness that magnetically attracts all the wealth you can desire!

To get your **free** copy of the course send any email to:

mwdiary@listwarrior.com

or visit the site below

http://www.TheMarketingWizards.com

Table of Contents

Internet Security Back In The Old Days

I have a confession to make. Listen closely.

I started marketing online in 2001. I already was an experienced computer 'techie': a programmer and a security expert.

I was pretty reluctant to marketing online because of one big issue:

Security

Protecting my product and my website seemed something pretty hard to achieve.

Allen Says, the man to whom I really have to thank for getting started with my online biz and making my first money online, was earning a massive 1,000 dollars a day from his websites at the time.

I figured I could do the same BUT there were some bugging questions:

"How could I protect my online products from theft?"

"How could I prevent illegal distribution of my images?"

"How could I stop *'wannabeez'* from copying my site?"

Even now, one year and a half later I still get emails from experienced marketers complaining that some of their competitors replicate their marketing efforts completely.

They have exactly the same websites, pay-per-click search-engine keywords, exactly the same autoresponder sequences and everything.

And this happens because a lot of webmasters and net-marketers overlook their website's security.

This is not recommended practice because people are not 'net dumb' anymore. They've been online for several years now. The Internet is old news.

Most people know HTML or can understand HTML code. Quite a few of them know basic web programming in Javascript, CGI, ASP or PHP.

They know about servers, protocols, sockets, proxies and the list could go on...

In fact, the latest Wordtracker report of the Top 200 most searched words positions the word 'cracks' on the 173rd position with 15108 searches on metacrawler search engines in the last 60 days.

As a term of comparison imagine that the word 'viagra' is on the 193rd position and 'free' is on 191st

Does this give you some hints about how bad some people want to hack & crack sites and software?

Here's a mental experiment for you

Imagine living in a bad neighborhood, going to work and leaving your house unlocked, with the windows wide open and nobody home…

What do you think will happen?

So… how can you be so careful with your physical property and completely ignore your online property?

I'm actually glad you bought this report. You should be too because I'm confident it will help you.

You will quickly learn how to solve many problems web site owners are facing today.

This report will cover the HTML security bugs your website might have.

But I will not stop here. I will keep writing about advanced techniques internet thieves use to illegally get your product or customer information and developing software that will help your website be more secure. (*I know I will make many enemies this way ☺)*

As a free bonus with the purchase of this report you have received my personal 'marketing diary' as a 5 day auto-responder course.

If you haven't done so already, sign up for the course and you will be automatically added to my newsletter.

You will also receive updates when new reports/software I've written are out.

Now that that's out of our way, let's start talking about the serious stuff…

Your Business and Your Website

Internet Security - The Jungle of Today

Two years ago a new type of software appeared on the market:

Software that offered HTML Code Protection.

In a very peculiar manner, this type of software brought a solution to the problem and made it worse in the same time.

This software increased the public awareness that HTML Code is very vulnerable (because it's a mark-up language and not a programming language it does not offer code encryption or compilation) and people started to become worried about the safety of their site, images and ebooks.

My guess is that it all started when the right click was first disabled!

Afterwards they kept adding lots of other tweaks to make the html code more secure (in this case the source code could have still be seen by clicking View->Source from the menu bar)

This is how a lot of 'hackers' learned that they could get products without paying for them…

And they told their friends about this… and other people found out… and others and others… and the methods have evolved and so on…

Software that could ensure web page protection in 2001 is not enough any more.

I'm not saying this software is useless. Not at all… My tests indicate that only 1 in 100 knows how to 'crack' the

protection this type of software offers and I'm teaching you in the bonus video.

1 in 100 means 1% and it sure beats leaving your page completely unencrypted and having 46% of the people (as you've already found out on the website) *stealing* your profits.

I've personally tested tens (about 15 to be more precise) of Page Guardians and HTML Encoders.

And from a security expert point of view I was not happy with the results. Not at all.

Your page is still pretty 'crackable'.

These programs might have been smashing hits one year ago but they are simply not enough to keep the jackals away.

I'm calling 'product stealers' jackals because they travel in packs (they gang up and trade products) and they usually are a source of infection (unauthorized distribution of your goods)

Keep on reading and I'll show you what they're doing to get your product free and how you can protect yourself.

Warning: The next chapters will be for informational purposes only. I do **not** encourage any of the actions below on sites other than your own.

“What Can They Hack And How Can They Hack Me?”

There’s one thing we need to get straight from the beginning.

You can never have too much protection on your site.

A well known internet security source published that in the year 2002 the average website receives 200 hack attempts a month.

And we all know that many big sites like Microsoft.com and NetworkSolutions.com have been hacked multiple times.

I don’t even want to talk about hackers who like to break into government sites or educational ones.

Well… I’m sure you’re thinking:

“Yeah Bogdan, you might be right but what does this have to do with me? I don’t have a big site; I’m just an average marketer earning a living by selling my products on the Internet…”

Well yes, you might not be in real danger of a hacker attack but let me tell you something.

There are many people, (and when I say many I mean many), especially from Bulgaria, India, Romania, Russia, China that don’t have the money to pay for your products… and your copy being so persuasive (hopefully) they are looking for a way to grab your stuff free.

There are 2 possible scenarios here.

1. They go hunting for stolen but valid credit-cards on the Internet to ‘card’ your products.

2. They try to hack your site to get the products

Most merchants today have a way to 'screen' the purchase to minimize the risk of fraudulent transactions which are very likely to result into charge-backs.

Trying to locate the 'carder' by tracking the IP of his computer is almost a futile endeavor because most of them use high-security proxy servers or *anonymizer* software.

However, there are many credit-card processing companies on the Internet that have very good fraud screening control and can really protect your products from being stolen (more on this in the next chapters) or carded.

The ones I personally use and really recommend are

1. www.ClickBank.com – they are very popular because they also have a built-in affiliate program.
2. www.ReveCom.com – the same as PaySystems.com, another popular service that is very secure with low fees.

If you have a merchant account and don't use a credit card processing company there are many tricks you could learn to protect yourself from 'carders'.

If you want to learn more about how to protect yourself from carding please go to http://www.911mechant.org and join the group.

I am in no way associated with the group but I they are recommended because you might find them useful.

Okay, this wraps up the ‘carding’ part.

“What about the ones trying to hack the website?”

There are two possibilities here (again…)

Either they try to bypass the payment screen (this is trying to hack the credit card processing company) or they try to exploit your site for common vulnerabilities.

From my own experience they almost always try both of the options.

I’m responsible for a few hacks myself. I’ve been hired by many companies to try and hack their website and I’ve discovered many vulnerabilities this way.

If you’re interested in renting a security expert to hack your website drop me an email at

webmaster@themarketingwizards.com

and we’ll talk about it.

Let’s get back to where we were, should we?

I was saying that they might try to hack your credit card processing company to get your products free.

Again ClickBank.com and Revecom.com are very safe options for credit card processing but there are some other services that are highly popular.

For instance Authorize, Paypal and quite a few other big names in ecommerce have

really weak HTML code and you could easily get **almost** any product sold through them by analyzing the code.

Heck, Paypal and Authorize are infamous for this.

However, there are fixes to these problems that will ensure your downloads are safer. A program I've developed, called HTML Code Guard 2003 is one of them.

There are other services like Verisign and Verio that don't have such a weak HTML code but the information posted to the processing script is pretty obvious and most products can still be stolen by understanding how their script works.

Of course if you're selling through them, don't think that your average web site visitor will be able to crack the protection. They need to have some experience in web programming and know some things about system sockets as well.

Okay, the second scenario was that some of them will try to exploit your site by viewing your HTML code and also 'scanning' your site for known vulnerabilities.

My opinion is that the HTML page should definitely be encrypted on your order page (yes, this includes affiliate links!) and on every page where the user can sign-up for your membership site, newsletter etc.

More on this will be revealed in the next chapters.

Hackers scanning your website for known vulnerabilities are also very dangerous because this way they might be able to

find many other extra things like:

- your webhost(and scan the webhost afterwards for vulnerabilities and get complete control over their machine)

- your customer information (names, emails and sometimes even address and credit card number)

- copies of your receipts, auto-responder messages

- content that is not yet published or that is being beta-tested

- etc…

“Can My Text And Images Be Secure Enough?”

The really interesting stuff begins with this chapter.

Sadly, the answer to the question in the title is **NO**

BUT, they CAN be safer than printed information in the offline world.

In the past, if anybody wanted to copy the information, they had to copy it by hand.

Now they can scan it and use OCR conversion software to get the text and images but this is also painful because they need a top-notch computer and a lot of time.

Let’s exactly see how a no-good-doer could extract and reuse the text and images from your website.

1. They could select the text, copy it and save it in a file.
2. They could save the whole page and open it with Microsoft Word, Macromedia Dreamweaver or their favorite HTML editor.
3. They could push the print-screen button to make a snapshot of your site and use any graphics processing program like PhotoShop or Paint Shop Pro (even Microsoft Paint) to paste the printed screen and save it.
4. They could print your website, scan the sheets of paper and then use OCR conversion.
5. They could push the right click button on your images and click save-as
6. They could position the mouse on your images, wait for the image toolbar to appear and click to

save the image.

If you have the time and energy to do some searching you will be able to find some free scripts on the internet that will disable the selecting/copying of text on the website, the right click and some other little things.

But these scripts can easily be found by your visitors (when they click to view source) and they will be able to save your page, remove the script (and get your script too, for free) and use the page as if it was unprotected.

And you are back where you were in the beginning.

You could also disable printing and the PrintScreen button. I agree that this is not something you would like done for all your pages but there are times when you should do so and there aren't many scripts out there showing you how to do this… (It's a secret of the trade ☺)

But they could still remove any javascripts from the page and have your whole content as if unprotected.

A more interesting option is HTML Code Guard 3, the latest security software I've developed.

If you're looking for a complete solution to protect your pages, your site and all the above (yes, even protecting your existing javascripts) please take a look at

http://www.htmlcodeguard.com

I've tried pretty hard to offer unsurpassed value for a small price and I think I've succeed.

Using HTML Code Guard 3 reduces the risk of site (text/images) theft to 1 in 500. That means you will be protected from **99.98%** (minimum) of these no-good-doers.

Note: If you have already heard about "HTML Code Guard" or you even own a copy then it's very likely you have HTML Code Guard 2.2 which is the previous version I released some time with master resale rights.

The new HTML Code Guard 3.0 is simply amazing…

I've worked for some time completely rewriting the code and now the 3.0 version offers superb security while being compatible with almost any browser.

Eh… I've blown my own horn enough.

Let's get back to business.

There's another thing you could do to your images to make sure people will not be using them.

This method applies to large images usually and it's called watermarking.

So, what is a watermarked image you ask?

A watermarked image is simply an image with a distinguishing small text/image embedded over it (usually in the lower right corner)

For instance, if you're launching your book "Titanic – Sensational Discoveries" on your site www.titanicdiscoveries.com and you don't people to reuse your pictures you could superimpose on the image your website address in the lower right corner.

This is called ‘watermarking’.

You can watermark your images in any graphics processing software – even the well known “Paint” that comes with Windows.

You could also use a more professional program.

The one I usually use to create my graphics is Paint Shop Pro from www.jasc.com

It has a better learning curve than Adobe Photoshop, but you could also try this one from www.adobe.com if you’re interested in really professional graphics software.

Exactly Why Forms Are The Weakest Link In Your Web Page

Not too many people are going to tell you the truth about this…

But encrypting the forms on your website is of critical importance.

You are very vulnerable to 'form' exploits if:

1. You run a traffic-exchange (start page, exit page or banner display) program
2. You run a pay-per-sign-up or pay-per-lead site
3. You run a site with a Top
4. You have a newsletter/mailing list
5. You have hidden tags on your form: An hidden tag can be for instance the **price** of your product, like a **really big** network of sites that I know of has. I don't want to name them here because you will then easily be able to change the price you pay for their products and this could cost them tens of thousands of dollars. Another example is the **thank-you link,** and almost everybody associates Paypal and Authorize with this.
6. You run tell-a-friend scripts
7. You run special offers like those "help me achieve Amazon best-seller status" where you give a lot of bonuses if the people order today
8. You do surveys/polls on your site
9. and the list could go on and on… if you use forms for any important function of your website like most websites do ☺

Ok, there's no need to be really alarmed now because I'm going to detail a little bit on each of these problems.

Let’s say you are a traffic-exchange site owner. You probably know that a lot of people are interested in cheating traffic-exchange programs.

There are scripts on the internet (in PHP, ASP or CGI) that emulate a real web-browser. These scripts can submit forms, see the text the page returns, use proxies and so on.

If your form is unencrypted these cheaters can easily see your posting location and configure such a script to keep POSTing the information needed to credit their account to your tracker.

They will know all the values your script needs to credit their account from the form and the link in the address bar.

And I assure you that if they are smart enough they cannot be untrackable because I’ve tested (not really used ☺) the method myself on several traffic-exchange sites.

Okay… let us now assume that you run a pay-per-lead service on your site - you pay people to bring you new leads or sign-ups.

If user John knows a little bit about HTML and your form is unencrypted he can easily see where you post the new lead information and how you credit the referrer.

He can then easily use scripts such as the above mentioned to post 1,000 new bogus (generated) leads to your service and collect thousands of dollars. Not a pretty thing to do right?

What if you run a Top, you ask?

Let’s see, Webmaster X joins your top and he gets the link that will credit his account. Every click on this link will bring Webmaster X one point and Webmaster X’s site is ranked in your top according to the number of points he has.

Well, let suppose Webmaster X is a skilled webmaster and uses a script (like the above mentioned one) to keep posting votes to his link.

He will be able to do this from different IP’s because he is a smart webmaster and he uses proxies.

And he will be able to cheat your system and get #1 ranking in the top without deserving it. Pha!

I bet that you start to see the picture now.

Let’s detail some more on this POSTing war.

What if you use a form to post the name and email address of your new subscribers to a script like formmail.pl or any other script that will add their names to a database and send them an instant response.

Someone with bad intentions can use your site to spam others (especially if you’re using formmail.pl)

Heck, your competitors could easily add a lot of fake subscribers to your list (which are real people, from their database for instance) and you could be accused of SPAM and permanently shut down.

Something even more serious happens when

you have an unencrypted form where you (or your merchant) keep the hidden tags like price, return links or any other sensible information.

Paypal.com (which was bought by eBay.com) is infamous for the poor security it offers to the merchants. At the time of writing this report, you can see the thank-you “return” link as clear as daylight when you click to view the HTML source.

Not to mention that some webmasters use the GET method when posting the form instead of using the POST one. The disadvantage of doing so is that everybody can see the information that was sent in the address bar!

Even Verisign (Verio?) is very vulnerable to form attacks. When I was younger I discovered that I can get almost any e-product sold through them without paying ☺

They are pretty easy to bypass if you have decent HTML / web programming knowledge but I’ve already told you about this.

I think that you got the general idea and I don’t need to keep pumping your head with the importance of encrypting your form.

If you run a tell-a-friend script the visitor can easily see your form and get to the ‘thank-you-for-recommending-us’ page without submitting any contacts or he can use your script to spam.

If you have special ‘Amazon Bestseller’-like offers then the visitor can see the posting location and get your bonuses without purchasing the book you’re selling.

If you run a poll/survey your competitors can easily see the posting location and submit thousands of random answers and really mislead you!

Okay. I hope my point is now clear.

And now for a shameless plug.

I should remind you that I've written the HTML Code Guard 3 software from a "security expert who also runs an internet business" point of view and I assure you that HTML Code Guard 3 will protect your forms and hidden information from anybody trying to hack your site.

HTML Code Guard 3 can encrypt whole pages or just critical parts of your website and I guarantee that 99.98% of your visitors will be unable to crack the protection.

…And I'm sure that your piece of mind only is worth a lot more than what I'm asking for the program.

The One Thing Every Affiliate Not Earning Enough Should Do!

I'm going to tell this one thing to you bluntly and then I'm going to detail on it and stress its importance.

Every affiliate, and I mean EVERY AFFILIATE should use encrypted redirect pages!

Some good months ago I heard some rumors about 'commission hijackers'.

Of course I was sure that this was no rumor and that it was indeed a fact but I wanted to find out the real importance of hiding my affiliate links.

I wanted numbers not speculations.
So I conducted a little experiment.

I was then selling the first version of HTML Code Guard and I was my only affiliate at the time (HTML Code Guard 1 had just been released)

The next step was as clear as daylight.

I was going to run a paid solo ad to 1,700 people with an affiliate link - my affiliate link to my own program ☺

And the results were astonishing.

13 sales came in but only 7 of them were actually from my affiliate link.

6 orders came from different affiliates.

Imagine that: 46% of the buyers replaced my affiliate link with their own, practically stealing money from me.

I think that Tom Hua, a really well-known marketing authority and owner of the very successful reprint-rights site eBookWholeSaler.com has conducted

similar tests before me and he reported a 30% for commission theft ratio.

And my guess is that the percentage is on the rise.

I honestly think that by the time you are reading this report more and more people are stealing commissions from affiliates.

Everybody wants to save a buck today. Some people even sell ebooks that teach you how to steal commissions and make money (I honestly cannot call these people marketers!)

But wait… There are other people that do not steal the commission but still lose you money.

They just hate you making money off them or they simply don't have the same security when buying from an affiliate so they remove the affiliate id/number.

I mean, how many times have you seen a link that looks like

http://www.htmlcodeguard.com/?john

And you just went to

http://www.htmlcodeguard.com

without giving 'john' proper credit?

I hope this makes you wondering.

Luckily, I have discovered a way to keep those pesky internet pickpockets away.

In the past redirect pages used to be a solution for cloaking your link.

You could simply create an HTML page on your site with the sole purpose of

redirecting the visitors to your affiliate link.

You would then link to this page.

The code to create a redirect page is this:

--------- JavaScript Redirection -------

```
<script>
this.location.href ="affilpage.html";
</script>
```

------ End JavaScript Redirection ------

But a redirect-page is simply not enough today.

After visiting your page your users will still be able to see the real affiliate link in the address bar and steal from you.

I've actually found a solution to this problem also.

I use a framed & encrypted redirect page that is 100% browser compatible and it even works without having Javascript enabled.

--- small side bar ---------------------

These days, the only browsers that do not properly support JavaScript are really old Internet Explorers (1 and 2) and Netscape Navigators and the WebTV browser – which is for the TV

If at any time you run a script on your page and someone who has disabled JavaScript visits your site you can add the following lines after your closing </script>

<noscript>JavaScript needs to be enabled to properly view the page!</noscript>

This alerts the visitor to turn Javascript on

--- end side bar ----------

The software is so nice that it even allows you to submit your affiliate links to search engines and get a decent ranking.

I know somebody who got Top10 ranking on Google, Yahoo and Excite for his affiliate links (he didn't submit the pages the software created but he linked to them on his main page and the search engines found this way) and chosen keywords for several *days*!

This massive traffic these engines brought was a really impressive side-effect taking into account that it was **free traffic.**

For a limited time I'm giving the software away as a **free bonus** with every order of HTML Code Guard 3 – the nightmare of all online criminals.

Click here to see the details for HTML Code Guard.

How To Stop Search Engines From Spidering Your Private Content

Contrary to what some webmasters tend to believe, search engines do not ‘see’ all the pages of your website and index them all.

The search engine spiders only visit the pages that can be reached through valid links – either from your website, or from other websites.

So, if no page of yours (or anybody else’s) links to your thank you page and you (or anybody else again) do not submit the thank-you page directly to the search engines then your page will not be indexed.

However, with highly successful products the ‘thank-you’ link tends to be spread and usually this happens on forums.

I’ve seen some cases where Google.com for instance had spidered some forum posts and some thank you links together with them.

So, if you’re in need to protect your thank you page from being spidered just add the following piece of code between the <head> and </head> on your thank you page.

<META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW">

If you have been using software that encrypts the whole webpage like HTML Code Guard 3 then your thank-you page will automatically get such small ranking that it can be neglected and the users will not be able to find it.

This happens because the search engine fails to find relevant and valid

keywords in the page and only encrypted javascript text (search engine spiders/bots are not able to interpret javascript anyway)

I hope that everything is clear now and you know what to do to stop Search Engines from spidering your thank-you pages.

How To Properly Use Javascript Redirection To Your Advantage!

In one of the previous ‘chapters’ I’ve told you a little bit about redirect-pages.

Redirect pages are a great way for affiliates to track clicks among other things.

But, there are 2 common problems with redirect links:

1. after redirection the address bar will show the real link the user is currently visiting
2. after redirection, if the user clicks the back button he/she will be taken to your redirect page instead of the previous location. The redirect page will re-redirect him to the current location if the user doesn’t click again the Back button fast. Also, some people might only click Back once and then immediately click to View Source and see why and where exactly you are redirecting them.

If you’re already using redirect-links you might already know about these problems.

Here’s a script that you might find useful that fixes the second one.

Instead of the common javascript redirection I gave you in the previous chapter you can use the following

---

```
<script language=JavaScript>
window.location.replace('affilink.html')
</script>
```

---

or if you prefer plain HTML just create a blank html page with the following

text

<meta http-equiv="REFRESH"
content="0;url='affilink.html'">

There is also a piece of software I already told you about, called Affiliate Redirector (comes as a free bonus with HTML Code Guard 3) that will solve both problems, will actually encrypt your affiliate link and will work on any browser.

Your users will never suspect that you've redirected them and they will think they are on your site the whole time because they will see your actual URL in the address bar and not the affiliate link.

Click here to find out more.

The Truth About Password Protecting Your Site

There are times when you might really be in need to password protect a certain page on your website.

…and you usually desire for the password protection to be very difficult to crack.

It is also known that if the password is kept somewhere in the document itself then the password will be fairly easy to be located and decrypted.

Again, it is only common sense that the stronger your encryption algorithm is, the more persistent the trouble makers will be.

They will double their efforts to crack your site because they will have a higher satisfaction afterwards.

And that would not be all – they will brag to their friends about their newest ‘hack’ and ‘dare’ them to crack your site too.

And so on…

And I’m pretty sure you don’t want that.

(Okay I admit. The childish ones will dare their friends but even the not-so-childish ones will still want to share their ‘results’)

This is one of the reasons major file-protection software (like Winace, WinRar, WinZip) does not keep the actual password in the file.

The trouble is that there are a lot of people selling software on the net and guess what:

They’re all trying to sell you software that stores the password inside the HTML file.

Yes, they encrypt the password and they store it in the HTML file… and their justification for selling the software is: ‘you get to pick the password you want’.

Well, what good is password protection if the password is easy to crack?

What would you say if I would give you a complete solution for your password protection needs right now?

(yes, I know I am a good guy ☺)

Okay, the solution is to create a doorway page that asks for the password and afterwards redirects the user to the **enteredpassword.html** file.

Let me give you an example to make this even clearer for you.

Visitor comes to yoursite.com/protected.html

(this is the actual password protected page)

The page asks the visitor for the password.

Visitor enters ‘**bond007**’ as password

Page automatically redirects visitor to yoursite.com/**bond007**.html

Do you see how this works?

The method is **almost** impossible to be cracked.

Here’s the javascript code you need to implement such a doorway page (protected.html in our example)

```
<html>
<head></head>
<body>
<SCRIPT LANGUAGE="JavaScript">
var password = ''
password=prompt('Please enter your
password:','');
if (password != null) {
location.href= password + ".html";}
</SCRIPT>
</body>
</html>
```

(please note that you can change the ".html" to suit your ".php", ".asp" or ".whatever" page on your site)

I bet you already love this method.

What You Can Really Do About Paypal.com Authorize.net And Other Card Processors With Poor Security

Well there are about three things you could do.

1. change your credit card processing company but there's no need to do so.
2. manually check all the orders but this could be very time consuming
3. do a *referrer* check for the thank you page.

What the heck is a referrer check you ask?

Well… a page referrer is a value that your browser sets (99% of browsers do) and represents 'from what page the visitor clicked a link to reach the current page'.

Okay, so let's see how and when you can actually use such a page referrer.

Let's analyze the following scenario.

John Doe gets to your page. He sees your product and he also sees a way to get it free.

Suppose he decodes your super-strong JavaScript protection (he probably couldn't be able to do this if you encrypted your page with HTML Code Guard 2003) or maybe your code is unencrypted.

There are a lot of merchants out there that do not encrypt the link the buyer will be directed to if the purchase was successful (like the paypal.com and authorize.net mentioned in the title)

The typical code for Paypal.com is this

<INPUT TYPE="hidden" NAME="return" VALUE="http://www.YourDomain.com/thankyou.html">

---

and the one for Authorize.net is

<INPUT TYPE=HIDDEN NAME="x_Receipt_Link_URL" VALUE="http://www.YourDomain.com/thankyou.html">

…And I bet that it's as clear as daylight, even for someone who doesn't have a clue about HTML where to go to get your product free.

So if John Doe goes to /thankyou.html he will probably get your product free unless you have a way to check if he arrived from the link Paypal/Authorize provides after successful payment.

This is called a referrer check.

When you implement a referrer check you allow a certain page to be accessed only from another specific page that you specify.

You could place the referrer-check directly as Javascript code on the page or you could implement it as an PHP/CGI/ASP script,

I repeat, the referrer represents the exact page where the link for your thank-you was located.

This link is found on the order confirmation (after successful billing) page on both Paypal and Authorize at the current time of writing.

You can find out the referrer of the page by using this script

(source code on the next page)

```
<html><head>
<script>
rx1=document.referrer.toLowerCase();
document.write(rx1);
</script>
</head><body></body></html>
```

When you access this page the script will write on the screen the name of the page where the link that brought you here was located.

The referrer is considered to be **null** if you access the page directly, without clicking on any link.

You can use this script to test and find out the exact referrer, so you can properly allow access to your thank-you page only from a specific link.

HTML Code Guard 3 is a great software that has built-in encrypted referrer check in javascript.

It can easily and securely protect your thank you pages if you are selling through authorize.net or paypal.com.

See HTML Code Guard 3 for yourself here.

What You Can Do When Your WebHost Is Stealing From You…

We are going to have a very serious 'talk' in this chapter.

At first, I almost couldn't believe it when my friend, Stephan Ducharme emailed me.

Here's the thing.

Stephan is a **really big** name in Internet Marketing. He is the owner of the very successful site and ebook "How To Get 1 Million Visitors To Your Web Site Without Spending A Dime In Advertisement"!

I once had a chance to look at his traffic stats and I was totally blown away by the impressive number of free visitors he receives.

(This is a sure sign that the methods he presents in the ebook work ☺)

Stephan also writes very compelling copy and successfully manages to convert his traffic into a lot of money.

I got his book about 2 months ago and I increased my traffic about four times since then!

If you haven't seen his site you don't know what you're missing – click here now to visit his site.

Okay, so like I said, Stephan Ducharme emailed me and told me that (guess what)

His own web-host was stealing from him!

He had lost $20,000 (☹) without knowing it and some people even said that he was lucky…

Let's take the following scenario:

If you currently imagine that your online business is at home then you are only partially right.

Because you probably don't have a high-speed T1 connection in your house or apartment you pay a host, right?

And this is *crucial* because this is where the heart of your business is: Your store is your website and it's located at their place!

Now, you probably choose your host on some criteria like: affordability, reliability, allowed bandwidth, speed, interface etc…

…My friend, you just forgot a little detail that had cost Stephan more than $20,000…

Are you sure the host is safe?

Imagine this: You are working really hard to create your own website (don't we all?), the money finally pours in after months of work, and first thing you know, your own host sees the success you have and starts STEALING from you from the inside!

You think it's impossible? Gee, they have all the passwords, so why not? You would be surprised to see how much often it happens. Thousands of fraud cases are reported every day!

This is totally unacceptable and how do I know?

Because it happened to Stephan!

Yes, he just found out that for weeks HIS OWN HOST was STEALING him…

Outrageous and unbelievable in the same time!

At first he thought that a #/$%?&* (his exact ‘words’) hacker was stealing orders directly from his website itself.

Several times a day, the ‘hacker’ was changing Stephan’s links and hi-jacking his commissions.

Stephan would change the passwords about every 6 hours, but nothing could solve the problem.

At first he thought the hacker had a new tool to breach the security so he increased the security to a maximum limit. He invested thousands of dollars…

But it didn’t stop ‘the hacker’.

So, to make a long story short, after a few days, he knocked the hackers in the corner. No more places to go, they were tracked and caught.

That's when he found out that the first man involved, the first-row stealer was **the technical supervisor** to whom he would speak to OVER THE PHONE to change his passwords!

Luckily again, Stephan had the enormous amount of money required to hire a very good lawyer who specializes in copyright laws to sue his web-host.

He did win the case and to tell it all in several words: “almost 2 years in jail and 1 million dollars”, because the webhost was hosting another 6,000 sites.

Whew… wasn’t this an interesting little story?

So, to make sure that what happened to

Stephan will never happen to you (because you might belong to the 'unlucky' group) there are 2 changes you might want to make:

1. Get a **very** trustworthy web-host. Personally, I'm using Allen Says' (already told you about him) WarriorPro. This is a great (affordable and reliable) hosting offer and it comes with some other killer bonuses like:

- unlimited follow-up autoresponders
- unlimited ad-tracking links
- a free subscription to his radical ezine "Guru Killer"
- free access to the "Warrior Group" members area with hundreds of ebooks and reports on internet marketing
- a free membership on the Warrior Forum, one of the best forums when it comes to Internet Marketing

Click here now to take a look at the Warrior Pro offer.

2. The other solution is to get "HTML Code Guard 3.0"

This software will ensure that your site remains the same: your host will not be able to steal from you because they will not be able to modify your page or substitute your links with their own.

Click here now to take a look at "HTML Code Guard 3.0"

The End…

Having said these things my report comes to an end.

I hope that it has been of great help to you.

I also hope that you will decide to take advantage of the unadvertised bonus and enroll in the free course offered by The Marketing Wizards.

If you already run an Internet business and you would like to learn how to make it even more successful by becoming your own 'marketing wizard' then this course is for you.

After completing the course you will be automatically added to my newsletter and we will be able to keep in touch.

I congratulate you for reading this report in its entirety.

I wish you unlimited peace and prosperity.

Best Regards,

Bogdan Ravaru

PS: Remember to take a look at HTML Code Guard from htmlcodeguard.com, one of the most advanced website protection software.

One of the nice site effects of using HTML Code Guard is that it will give you instant credibility because protected pages will make you look more professional.

And we all know that credibility is what you need for your online success.

For a limited time I’m even throwing in some amazing free bonuses that you cannot get anywhere else…

One of the bonuses even protects you from spam.

Click here to find out more.

Bonus : Imaginary Long Transcript Of The Wordless Video

Hello,

my name is Bogdan Ravaru from http://www.htmlsecurityreport.com and this is your bonus video.

I'm here to teach you how to crack 90% of existing Javascript protections in 55 seconds flat with your bare hands without knowing a thing about web-programming.

I'm sure you are already excited so let's just begin and see how this really works.

In this example the right click is disabled on the page.

The blue circle shows that I am right clicking.

Because right clicking is disabled I will use the universal solution to view the source code of a page.

Click View -> Source.

As you can now see the code is encrypted by a 'common' HTML encrypter specially developed by me for the purpose of this video only.

Let's see how you can crack it.

Carefully examining every line we come to the following code

document.write(ccj)

Even if you don't know a lot of programming you can safely assume that all lines that are in the format of

document.write and something between

brackets

will write something on the HTML document.

So let's see what exactly this something is, should we?

Let's modify the "document.write" to "alert" and reload the page.

Whoa, surprise... it's the actual HTML code.

You've broken the page and I'm sure it took you way less than 1 minute.

Because you still have **plenty of seconds** left let's do something a little more elaborate.

Here's what you'll be doing.

Insert an HTML text box here like this

```
<form name=pad>
<textarea name=text
style="width=330;height=300”>
</textarea>
<form>
```

and modify the alert to

```
document.pad.text.value+=
```

This means that the script will add the decrypted text to the text the text area already holds.

As a small side note (I won't get into the specifics and give you the exact reason why) "+=" is always better than plain "=" when cracking javascript protections

Let's reload the page and see what happened.

Amazing isn't it?

The decrypted code lies in a text box ready for you to copy it and use it in any other way.

I hope you are now convinced that most HTML encrypters on the market are pretty worthless.

I have to admit that some of them use a method called 'escaping'. They will 'escape' the javascript part where the document.write is, to make the code harder to crack.

However, this is not real protection because you can find javascript unencrypters everywhere for free on the net and a lot a people already know about them.

In fact I was emailed a couple of days ago by a photographer that had no security knowledge and he was wondering how can some people call 'escaping' protection because he was able to decode it with his eyes closed.

I've not included an HTML unescaper in the package because that would mean using a tool and I promised that I will teach you how to crack the protection using your bare hands.

The other reason is that I don't want to actually TEACH you how to 'hack' these protections. That would simply be unfair.

I've explained the principle to you and the principle stays the same. You will basically unescape the code using a free program or script and you will apply the same method.

But this is a terrible thing to do right?

And I'm sure you don't want people doing the same to your site.

This is why I know you are smart enough to invest in the software I've personally developed called HTML Code Guard 3.

It is available from http://www.htmlcodeguard.com

I will meet you on the site.

Peace and prosperity
This is Bogdan Ravaru signing off.

Allow me to tempt you with a **customized** version of the report…

I want to personally customize the report with **your name, your site** and **your affiliate link to HTML Code Guard 3** (I'm using ClickBank.com for my affiliate program…)

The master resale rights will allow you to sell the report and transfer these rights to your customers.

The report will then work as your 24 hours round-the-clock salesman promoting your link, making you profits and bringing extra visitors!

Just **imagine** that you'll be selling the report on your website or to your list and your customers will also sell it but with **your** links in it!

Can you see how **easy** it will then be to make serious profits earning a solid 50% commission on all your sales for HTML Code Guard 3?

To find out more about the Gold Resale Rights for this report click here

http://www.themarketingwizards.com/report/rights.html