Special report from the e-desk of Bogdan Ravaru and George Katsoudas:

"How to stop Internet thieves from robbing you and actually make money from them!"

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

© Copyright December 2003 by Bogdan Ravaru & George Katsoudas

While attempts have been made to verify information contained in this publication, neither the authors, 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 authors 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.

The reader is encouraged to seek expert advice before engaging in any activity.

Published by:

Bogdan Ravaru CEO and Founder of
TheMarketingWizards.com

George Katsoudas CEO and Founder of
FrankensteinMarketing.com

NOTE: You now have <u>full</u> <u>redistribution</u> <u>rights</u> to this special report. You can give it away on your site as valuable content for your visitors or subscribers. The only "catch" is that you can't modify this report in any way... That's it ☺

Thanks ...

Thank you very much for downloading this special report and congratulations. We think that you will find it **enlightening** and **thought-provoking** to say the very least...

Over the last months, the problem of online theft has become **HUGE!** Internet entrepreneurs are at the mercy of unscrupulous individuals who have no problem at all getting their filthy hands on products and services <mark>**for free!**</mark>

This short report, will give you some ideas on how to stop them cold and even turn the tables on them and make a profit as well... <u>legally</u> and <u>ethically</u>!

And... we start with...

"The dirty trick my deceased grandfather used to rake in the moolah... and how to use it to <u>your</u> advantage!"

by George Katsoudas

Let me tell you a true story...

More than 20 years ago, when I was still a kid, my family and I visited my grandparents in Kalesmeno... It's a small village in Greece, you wouldn't know it... ☺

My grandma had a roost with about 25 chickens in there. And there was this thing that **caught my attention**... When the night would fall, my grandfather would go there and set up several small animal traps around the roost. I was very curious, so I asked my grandfather:

"Grandpa, what are those things for?"

...and my grandpa replied:

"They are there to catch foxes my dear. When the night falls, they come for our chickens."

"And what do you do when you catch them grandpa? Do you release them the next morning?"

For as long as I live, I will never forget what my grandfather replied:

"Heck no, Georgie boy! First I skin them, then I feed them to the dogs and then I sell their fur!"

And he went on:

*"You won't believe how much money I have made this way. Fox furs are very expensive. Plus, **I save a bunch on dog food!"***

Only decades later did I understand how much business sense my grandpa's words made. You see, your website is no different than that roost. It has many "chickens" in it. Digital products, sales-letters under construction, experimental software, unpublished articles and so on...

And the foxes? <mark>The foxes are present as well</mark>. People who try to gain access to these pages and files for free, **without** paying you for the blood, sweat and tears you've put in. Unfortunately, most online business owners will **never** take advantage of this fact in order to <mark>profit like crazy!</mark>

They either stand still and wait for the foxes to eat their chickens time and time again, or, at the very most, they just try to protect the chickens without making **any** profit from the foxes themselves. <mark>Too bad!</mark>

"That's interesting George, but how can I do this? How can I actually make money from online thieves?"

Beats me! Ok, ok I'm kidding. <grin>

Actually, it's **very** easy once you know how.

You don't believe me? Here's one of the **simplest** techniques that almost **nobody** is using!

When thieves try to 'attack' your site, several "error messages" are created by the web server software. Let's say for example that you have a digital product named: **"Secrets Of Chess"**. Do you know what many people will try to do?

They will try to type in the address bar:
http://www.yoursite.com/download

or maybe
http://www.nameofyoursite.com/sos.pdf (sos="Secrets Of Chess")

...and 100+ different combinations. Every time the address they type does not lead to a real file, a **"404 Error"** message is produced. I'm sure you have seen one. I'm talking about those ugly "Page Not Found" pages.

So, what can you do? Simple! You configure your site so that each time an "Error 404" is generated, the fox, errr... sorry, I mean "the visitor" will see a page of **YOUR** choice.

This can be done **ultra** easily since most hosts have an online panel that does that in a couple of minutes. But even if such a panel does not exist, you can email your webmaster and he can show you how to do this easily. Or just do a search on google.com for "create custom 404 pages" or "how to create 404 pages".

Now, the question is **what** to put there...

My suggestion?

NOT the same page that the visitor has just seen. If s/he decides that the only way s/he would have access to the product is for free, then maybe it's time to take "another route".

What is that route you ask? Simply, put a page for an **affiliate** product there. That way s/he will see a completely different offer and ==you stand a good chance of making some commissions.==

Of course, there are many ways that you can easily make **100 times the profit** from online pickpockets. As I said: It's easy once you know how... I will only say this much: You are ignoring a goldmine in your site if you are not incorporating similar techniques...

I guess my grandfather never knew how much money I would end up making because of that little chat we had so long ago.

God bless his soul...

If you thought that **this** technique was "cool" wait till you see what tricks await for you [here](#)!

"The search engine manipulation technique that can put you out of business by this time tomorrow!"

by Bogdan Ravaru

Listen up, because this is something many, **many** marketers are vulnerable to...

You see, many Gurus and newsletters (and I'm talking about really high circulation ezines like 100,000+) have conditioned them to watch out from the search-engines

spidering their private content (images, downloadable files etc)

They will all teach you to create a **robots.txt** file on the root of your server and write a couple of "disallow" lines for the images and download directories.

This is to prevent the listing of download links for your products from forums, from blogs, articles in the SERPs - haha, I'm teaching you some new 'slang' SERPs Search Engines Results Pages

Note: Contrary to popular belief - search engines **cannot** see your **entire** site as it is hosted on your server. They will see it **exactly** like any regular visitor. So, the search engines cannot index pages and files that are not linked from public pages normally accessible by an average visitor.

But "things are not always as they appear to be" as Rayden said in Mortal Kombat. ☺ While this "robots.txt" trick might seem smart, what does the smarter hacker do in this case?

S/he goes to http://www.yoursite.com/robots.txt and sees your download directories completely unprotected...

And being a nice fellow, s/he leaves your site without downloading any of your products and God knows what other confidential data you were keeping there!

Yeah right... and if my grandma had wheels, she would be a **skateboard**!

You can **solve this problem** either by password protecting your directories (and we will teach you how to it **quickly, easily and free** in the full version) or by using special software that offers dynamic download links to your products.

This way, even if your thank-you links are traded, distributed or posted on forums to get picked up by the search engines, people won't be able to download from your site...

> You can find out about password protecting your directories **quickly** and **easily** from the Project Mouse Trap site. The site also has a very special software that can create dynamic download links for your downloadable files.

>>> And now, our, all time favorite **horror story** that has crippled many internet businesses for good….

"How Nicolas lost $9,062 in potential profits and how to avoid making the same mistake yourself..."

by Bogdan Ravaru

Here's a **very interesting** story I'd like to share with you...

A few months ago, a good friend of mine named Nicolas was working on what he hoped to be his biggest moolah maker - EVER! He had been working on it for (drum roll please...) OVER 8 MONTHS!

No, that is not a typo. He had been putting blood, sweat and tears in this very special package for 8 freaking months.

It was some awesome, **awesome** stuff - text, audio, video, student workshops etc...

Now, that is not the unbelievable part. Read on and you will see...

He was going to sell the package for $197... and... he expected it to do **really well** because the info was top notch in his industry…

Plus, he had a list of 25,000+ responsive subscribers!

After he finished the product, he uploaded it on his site so that a few of his business partners and beta testers could download it and give him their opinions.(The product was more than 95% ready at that point.)

Now, **get this!**

One day, we were talking on MSN messenger and he says:

"Bogdan, something went wrong."

"Like what?", I reply.

"Look, only ten trusted individuals know the location of the package on my site. Yet, my web logs indicate that it has been downloaded 56 times!"

"Ha, ha! You little bugger. Had me going there for a second!", I reply.

"I'm not kidding, man! The package has been downloaded 56 bloody times from my site!"

"Hmmm... that's strange. Are you sure that your ebook is in a directory with a name that's difficult to predict?"

"Yes Bogdan, the name of the directory is "bigfoot". There's no way that someone could guess it. And on top of that, my subscribers don't even know that this product even exists!

Plus, I have named the file itself "Josephine.zip". Who could guess THAT? [**NOTE:** My friend had a buddy whose name was Paul. Josephine was Paul's girlfriend. Long story, don't ask. You won't believe what I hear on MSN ☺]

Anyway.

The same day, I decided to subscribe to my friend Nicolas' newsletter. I wanted to see what my friend's subscribers saw.

When I received the first message, it said:

"Bogdan, thank you for subscribing:

Here's a free gift as a token of my appreciation for you.

http://wwww.my_friend's_site.com/bigfoot/gift.pdf"

(Notice the name of the directory!)

What the... somebody pinch me!

I typed on my address bar http://my_friend's_site.com/bigfoot

...and to my amazement, I saw a list of about **fifteen** files in there with different names and extensions as well as a **very interesting** file named: "Josephine.zip"

Not only had he put his paid product in the **same** directory with his freebies, he had also **forgotten** to put an index page in that directory!

Can you believe that?

Always, always, **always** put a file named "index.html" (even if blank) in every directory of your site. Otherwise, the visitors will be able to see a list with all the files you

have in each directory. Plus, **all the links** to download them for free!

This mistake is so usual that it's not even funny anymore. But in all fairness, people who don't have a "techie" background may not know it.

And of course, for the name of Spiderman, **never** put your paid products in the same directory with your freebies. It's <mark>bad karma!</mark>

The same night I logged in MSN to talk to Nicolas again. I didn't have the chance to tell him what had gone wrong with his product when he said:

"Bogdan, Bogdan! Big news man!"

"What?" I replied.

<mark>**"Paul and Josephine broke up! ☺"**</mark>

<sigh>

This is **just one** of the many mistakes well-meaning webmasters make that cost them dearly. Are you **sure** you are not making them as well? You can discover the whole truth once you download this shocking report – **Project Mouse Trap**

"How to track down thieves and spammers to put them out of business for good!"

by Bogdan Ravaru

Allow me to state a principle here: <mark>**"Most thieves and spammers are very lazy!"**</mark>

Because of this, they get sloppy and it can get **very** costly for them. You see, normally, a thief/spammer should change the email address and IP address (using a proxy or an anonimizer service) every time s/he steals, spams etc...

But they don't, and this is good news for you!

Now, when you receive a spam email, take a good look at the **header information.** In Outlook you can do this by right clicking the email and selecting "Options". Now check the bottom box called "Internet Headers".

The headers will look like this (I'm using an older email from George as an example):

➔ Received: by mail01.powweb.com (mbox mwmaster)
 (with Cubic Circle's cucipop (v1.31 1998/05/13) Wed Sep 3
13:31:01 2003)
X-From_: george@frankensteinmarketing.com Wed Sep 3 09:35:11
2003
Return-Path: <george@frankensteinmarketing.com>
X-Original-To: webmaster@themarketingwizards.com
Delivered-To: mwmaster@mail01.powweb.com
Received: from server146.teknonservers.com (unknown
[66.246.86.48])
     by mail01.powweb.com (Postfix) with ESMTP id 11DB3368BF
     for <webmaster@themarketingwizards.com>; Wed, 3 Sep 2003
09:35:10 -0700 (PDT)
Received: from lami364-b004.otenet.gr ([62.103.228.100]
helojnvn13kum2oxitx)
by server146.teknonservers.com with asmtp (Exim 4.22)
id 19uab5-000588-Td
for webmaster@themarketingwizards.com; Wed, 03 Sep 2003
18:35:08 +0200
Message-ID: <000001c37239$5c4f9e90$64e4673e@jnvn13kum2oxitx>
Reply-To: "George Katsoudas"
<george@frankensteinmarketing.com>
From: "George Katsoudas" <george@frankensteinmarketing.com>
To: "Bogdan Ravaru" <webmaster@themarketingwizards.com>
References: <000601c37233$d3602d20$020ba8c0@rexnet>
Subject: Re: an idea...
Date: Wed, 3 Sep 2003 19:35:01 +0300
MIME-Version: 1.0
Content-Type: text/plain;
charset"Windows-1252"
Content-Transfer-Encoding: 8bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
Disposition-Notification-To: "George Katsoudas"
<george@frankensteinmarketing.com>
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
X-AntiAbuse: This header was added to track abuse, please
include it with any abuse report
X-AntiAbuse: Primary Hostname - server146.teknonservers.com
X-AntiAbuse: Original Domain - themarketingwizards.com
X-AntiAbuse: Originator/Caller UID/GID - [0 0] / [47 12]
X-AntiAbuse: Sender Address Domain - frankensteinmarketing.com
⬅

From this email I can find out a whole lot of nitty-
gritty stuff like:

Stupid George sent this text email (Content-Type: text/plain;) using the following SMTP server of his host – server146.teknonservers.com (So, George is hosting with teknonservers.com)

I also found out that his virtual host name is "lami364-b004.otenet.gr", with the IP address of 62.103.228.100.

Now, even if I didn't know his IP address I could easily go to http://www.dns411.com

and type his hostname and get his IP address.... Dns411 is a great, **free** service and can give you a whole lot of very accurate information: what IP corresponds to a certain hostname, what hostname corresponds to a certain IP, what company was the registrar for a certain domain name, what company is hosting that domain, who bought the domain etc...

Ok, so now I know that George's IP address is 62.103.228.100... Let's assume that George is a thief or a spammer (although he is actually a really nice guy) and let's do some further research on him...

Note: For this type of research you need to know the IP address. You can get the IP address from the email like I showed you above or directly from your website's/shopping cart's logs if no email has been exchanged.

Now, let's go to http://visualroute.visualware.com

Another great service... In the past this service was totally free but now they require you apply for a **free account** with them. It only takes 30 seconds.

So, we go to the site and enter "62.103.228.100" (without the quotes) in the box that says "Enter Host/URL" and we hit Enter. A real time graphical report that shows me the network path from Dulles (East Coast) to Greece....

Tada! I just found out that George is from Greece.

Note: Well, I'm not that stupid... I could tell that .gr means Greece, but many times, if you only have the IP address or a .com/.net/.org host name, you can't tell where that machine is located.

If you continue the investigation, you can **e-a-s-i-l-y** locate how and where to report this offender (thief or spammer) and make sure that he never messes with you... **ever again!**

> Now, if you want to discover the no-holds-barred, entire process of locating a thief/spammer and reporting him/her please download this confidential report:
> Project Mouse Trap From Eastern Europe

"Departing thoughts"

As you see, there's a lot more to what meets the eye. The out and out truth is that you can protect your site and increase your profits substantially IF you know how.

Heck, even **Rosalind Gardner** (Yes, **the** Rosalind Gardner of the **Super Affiliate Handbook** fame) managed to increase her profits by receiving this info.

As a matter of fact, you can go here and **listen** to her story (Yes, it's a short audio ☺). And then, while you are at it, download the full report that will show you many more tricks like the above (only better <grin>)

Thanks for reading, and best of success with your business endeavors! ☺

Your friends,

Bogdan and George