

Stopping Snoopers

Protect Your Digital Files Against Thieves

This mini-report is taken from '[Squash Digital Thieves](#)'.

This Product Proudly Brought To You By

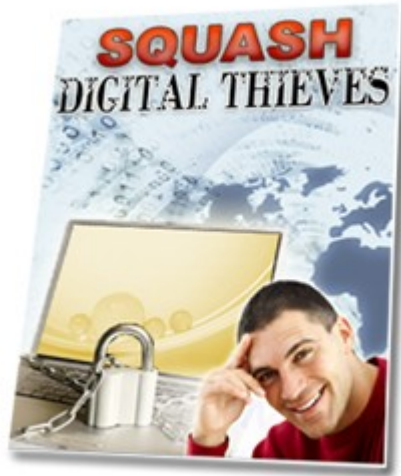
Mieke Janssens

<http://www.miekejanssens.com>

This Report-Extract Comes With Full Giveaway Rights

You may give away this extract as long as you don't make any changes to it. You may also include this product in a free membership site, or use it as a bonus.
You may NOT charge any money for it

Squash Digital Thieves



"Shocking Report Reveals Why Even The Most Experienced InfoProduct Seller Has Easily By-Passible Holes In Their Digital Delivery Security System --

And How YOU Can Take Steps To Squash Digital Thieves Before They Take A Bite Out Of Your Online Profits!"

The Squash Digital Thieves e-guide is designed to take you by the shoulders, shake you, and spoon-feed you some of the easiest digital infoproduct security tips you can, and should, use to safe-guard your files.

Strengthen your online security system in just a few simple steps and decrease the chances of online scoundrels from lifting your digital goods.

Get the full report today!

This e-guide will instruct you on the best course of action to take whether you are an everyday reseller of digital products, a creator/author of digital infoproducts, or just someone thinking about starting a digital product online business. Squash Digital Thieves is for YOU!

[Order Now](#)

So, you think your digital downloads are safe? You had better think again! No System Anywhere in the World can be considered 100% safe from thievery.

There are people out there that actually don't mean any harm by stealing, it is just a sad fact that maybe they cannot afford the prices for certain things they want, or need. But, there are others. . .

Others that really DO intend on harming the author, or reseller, by pilfering their goods. And to make matters even worse, they offer these stolen goods to others for a staggering price tag of, are you ready for this. . .

100% F-R-E-E!!

Think you're immune? Well, I'm here to tell you that you aren't. If big dog Marketers can be stolen from, what makes you think that an average "Joe" or "Jane" has a magical bag of "security" tricks? Look at it like this, if the guys(and gals) that are pulling in tens of thousands of dollars through massive product launches, they should be over-protective of their respective profits. So, if they can be stolen from, how hard do you think it would be to steal from YOU?! Not hard at all.

The most alarming thing about digital product theft is that it shows absolutely no signs of slowing down or stopping anytime soon. So long as there are ways to receive digital products, there will always be someone waiting in the wings to snatch it up and pass it around. However, we CAN slow this type of deceptive activity down from a flood to a trickle.

Now we come to the "good stuff". Letting you know how to try and reduce the amount of products stolen from YOU. There are a few things you can do to lessen this type of activity.

STOPPING "SNOOPERS"

Difficulty: Novice

Cost: Free

Time: 5-15 Minutes

There are some people that love to get online and snoop around your website to see what you have hidden inside your file folders. You know, the things that hold your content inside your web hosting space and give it a nice "shiny", uncluttered look? The little yellow folders!

The sad part is, if left unprotected it's as easy as going to eBay. Unlike going to eBay though, they won't have to pay one thin dime for anything they want that you've got.

There is a very simple technique to protecting your files from some of those "snoopers". By making use of **the correct CHMOD settings**. Okay, you may not know what this is. At first, I didn't either. But, through making associations with other like minded people, I was clued in to this little protective "gem" if you will.

While most file folders you create on your hosting space are automatically given the chmod status of 755, this is unsafe for anything you place inside there. Especially digital downloadable items you're attempting to sell.

But, if you change this setting to 751, then the contents of the file folder remain hidden from prying eyes. Or at least for the most part they do.

Now, using this alone will not completely protect your file folders however. **You should always, and I mean ALWAYS remember to put a file with the name of "index.html" or "index.htm" inside every single folder that resides on your web hosting space.** The purpose of this is most inquisitive folks looking for a "free ride" so to speak will put in your URL path leading simply to your folder. Like this:

<http://www.yoursitename.com/yourfolder/yourgoodstuff/>

And then, if you don't have the above two securities in place, it's Thanksgiving! They've hit the jackpot. You being none the wiser, unless you constantly check your web statistics. Which most of us are a little too busy to do with running several businesses and such.

But, if you have the file folder chmod'ed to 751, they won't see anything inside of it. Add to that a blank, or whatever you want to put on it, index.htm page, that's all they'll see. No goodie gathering from you! They're blocked. Or at least to a point.

You would not believe how many digital resellers DON'T do this. It's mind boggling. Obviously, the CHMOD 751 trick won't work for every folder inside your web hosting space. Especially those that run specific scripts that need to be set at something different in order for the scripts to work.

If that's the case, then put your digital products inside their own file folder system. And we'll discuss how to do this in the next step.

One other note about "snoopers".

The term "snooper" isn't reserved for only people. Nope. **Because search engines like Google excel at the act of snooping.** They do this so they can index your pages throughout their own system. But, because they are merely machines, for lack of a better term, doing their jobs. Basically, they don't know the difference between your product download page and your blog. What I mean is, they see them all as content references they can index into their system.

So, what do you do? You add this line of code to all the .html or .htm pages you DON'T want included for indexing inside the search engines:

```
<meta name="robots" content="no index, no follow">
```

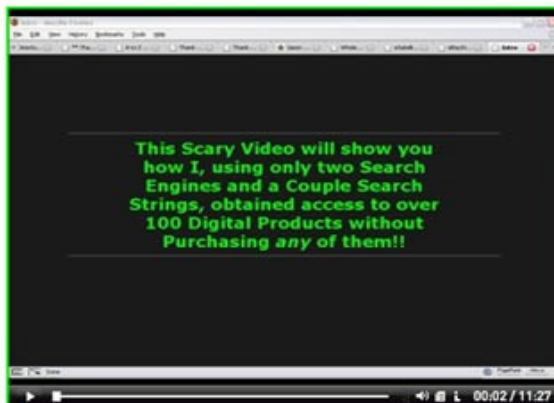
Where to put it? In between your <head></head> tags within your html code.

Also, it's important to understand that **you should NOT be putting links to other websites inside your download pages.** The reason for this should be obvious. If not, then here's the gist of it. . .If you place links to other websites, like www.WinZip.com or www.Adobe.com onto your download pages, the higher risk you run of your download page being found via online searches. So, just provide the link, don't make it "live", or clickable, if you must include them for your customers benefit.

**WANT TO GET MORE TIPS ON HOW TO PROTECT YOUR DIGITAL FILES
AGAINST THIEVES?**

[ORDER THE FULL REPORT TODAY](#)

STOP giving away your Digital Products!! Watch [this Stunning Video](#) to see why you need to protect your Download Page (click the image to watch the video)



Quickly and Easily Secure your Download/Thank-you Page without using any complicated IPN or Talk-Back scripts communicating with your Payment Processor's Web Site!

Compatible with all Popular Payment Systems: PayPal, ClickBank, 2Checkout, PayDotCom and many more...



I have just created The **E-Z Download Page Protector** for those of you that are looking for a **quick, easy, and very effective solution to securing your Product's Download/Thank-you page.**

The *E-Z* Download Page Protector allows you to **quickly secure your Download or Thank-you page** without the need for your site to communicate with your Payment Processors site, (ie: PayPal's IPN system or ClickBank's Secure Key variable).

[Read More Here](#)