PDF

6 WAYS

your e-books are stolen off your website

and

how to STOP it !!!

JHWhite aniota.com

6 Ways Your eBooks Are Stolen Off Your Website/Server

Imagine this horror story: You've had a website for several years. A couple hundred people visit your home page every day. And you're grateful for that. You're only selling one or two of your ebooks a month, but you think your traffic will eventually buy something. After all, you've read that the average buyer visits up to seven times before they buy. Still, you wonder what all those people are doing there, never buying anything.

And then, you find out. Your system operator gives you a report from your log files that shows hundreds of pdf downloads, downloads of your ebooks, all downloaded for free.

Talk about sick at heart.

*****

If you decide to go into information products, create ebooks and sell them from your own website, you need to know that protecting your product from thieves is a cat and mouse game. Once your eBook has been purchased or found in some other way, the information about where to get it for free will be posted to forums and even picked up by Google.

HOW CAN THIS HAPPEN?

Wherever you have your website hosted, you will have a root directory in which are listed one or more directories i.e. img/ (for your pictures), pdf/ for your eBooks and possibly more. Your html web pages will more than likely be in your root directory and, if you are not aware of your possible losses, your ebooks may be there, too.

1. Unless you have an index page in every directory, **ANYONE** with a browser can access anything in that directory. For instance, entered in your browser, http://www.yoursite.com/ will pull up http://www.yoursite.com/index.html and block a listing of everything in the root directory. The .com/ assumes an index page.

2. Unless you have a sitemap. A sitemap lists everything in your root directory. Clicking on the links in it will make everything in your directory accessible in your browser, including your ebooks. Downloadable. Free.

3. Even if you don't link to your sitemap from your webpages, anyone can "assume" that you do have one (you will be advised that search engines need one but they really don't) and enter http://www.yoursite.com/sitemap.xml or html into their browser and if you have such a file, it will appear and list everything you have in the directory.

4. Also, if you have your ebooks in a directory named /pdf or /ePub or something similar and have no index page in that directory, nothing can stop anyone with a browser from downloading everything in it. This is another easy one to assume.

5. Even if you do have an index page in your pdf directory, if your sales page gives the title of your ebook, anyone can type into their browser something like http://www.yoursite.com/pdf/My-eBook.pdf and the file will download immediately if the title is correct and it's in that directory.

6. If you are using a payment service such as Paypal, they will encrypt the script you will copy to your webpage so no one can see (view page source) the url of the return page that gives a buyer the download link to your ebook. However, this return page is **ALSO** listed in your directory so do not give it an easily identifiable name like rtnpg.html

What you can do:

If you intend to email your eBook to buyers, you CAN make it inaccesible to everyone but yourself in a directory made secure by setting the file attributes to 700. Otherwise **get your ebook completely OFF your server.** Pay a service to handle your sales and the delivery of your digital downloads.

Otherwise:

1. Either get rid of every version of sitemaps you may have (there are 5, .html, xml, xmlgz, ror and urllist) or go into each one and edit out links to your ebook files.

2. Create an index page for your "pdf" directory, change the directory name or create a new directory. In any case, make sure you create an index page for it.

3. Consider giving your ebook a file name different from the Title of the ebook. For example, the title could be "My-eBook" but the file name x374efymp.pdf. Keep a text file somewhere showing what file name refers to what ebook.

4. Give your return pages a hard to decipher file name. Either encode them so you know what they refer to or keep a list.

5. You could also send your ebook to the buyer by email after their purchase. Either automate this or say something like "delivery before 5:00 pm EST" to handle the time frame for them and remove you from 24/7 duty.

6. And lastly, consider requiring a password to open the pdf. You would need to email this to the buyer after their purchase. See #5 above.

7. **Ask your system operator for a daily copy of your log files (or a report from them) that shows what has been accessed from your website.**

*****

"**Embezzle" the fact-finding guide that will expose discrepancies in your accounting records and allow you to proceed on fact, not suspicion.**

EMBEZZLE
*How you are setting yourself up for embezzlement.
*How your Financial Statements hide embezzlement.
*19 Common embezzler tricks and how they work.
*If you're not seeing evidence of embezzlement, why bother to look for it?
*How to make sure you can access your records.
*What to do RIGHT NOW!
*What's so important about keeping your investigation secret?
*What to do now to recover money later.
*Exactly how to access bookkeeping accounts and find what you're looking for.
*How to massage bookkeeping data in excel to reveal vital clues.
*How to check the hard copy files for what IS and is NOT there.
*If your suspicions are confirmed, what to do next, absolutely NOT do?
*Other Risks.
*Prevention METHODS that make embezzlement almost impossible.
*How to Limit your exposure.

Most owners and managers are reluctant to accept embezzlement as a possibility because, if both their staff and their accounting is suspect, they believe there is no other solution than to hire their CPA to conduct an audit which will cost big bucks and may find nothing at all. That being the case reliable CPAs are reluctant to do an audit on the basis of suspicion alone. Owners and Managers then find themselves in a no-win situation, unable to go further,

"EMBEZZLE" is the solution! It's how you find the evidence, if there is any. EMBEZZLE" is not set up like an audit. It works from the inside, like a bookkeeper does. If there are discrepancies to be found, you'll have documentation: what it is, where it is. You'll be operating on fact, not suspicion.

With the instructions in "EMBEZZLE" you can easily do it yourself. If you need a little fine-tuning of your bookkeeping skills, consider **Bookkeeping Basics**. If you don't have the time or desire to follow "EMBEZZLE" yourself, hire someone to do it for you on a temporary/part-time basis. I suggest an outsider, a retired full-charge bookkeeper with years of experience, a high school education and a clean record

http://www.aniota.com/~jwhite/bookkeeping/embezzlement0.html $10.00