

Homemade Remedy for Download Theft

It's not for the geeks.

Many online sellers aren't bothered so much by copyright infringement as they are of losing money by theft of their online products. Most popular among these is the e-book. Guess we already know why those who are selling e-books are considered high risk merchants: the sole fact that the e-book they are selling can be easily downloaded for free (without being dubbed "freeware" or "shareware") makes them vulnerable to frauds and chargebacks in the long run.

Now, some first time e-book sellers are not savvy when it comes to protecting their products online. Of course it would be extremely helpful (and imperative) to learn how to do it before launching the e-book for paid download. It would be worth taking a look at my past article "What Every High Risk Merchant Should Know About Intellectual Property Rights" to find out more about what you can and cannot do on a legal basis when it comes to online product theft.

IT'S IN THE PACKAGING, SILLY!

Normally, a high risk merchant would find a way to counter hackers from getting access to the download page. But this takes a certain degree of skill. E-book sellers can find relief from download piracy by simply packaging the product into the Adobe Acrobat .pdf format. Amazon does it; all other online book sellers do it so only an image of the book page can be captured. The same goes for images. You would need to watermark it to prevent it from being stolen.

TREASURE YOUR SOURCE CODE

But a prepared online seller always knows how to attack a hacker even before he takes advantage of his download webpage's source code. Paypal has a way of helping high risk merchants to do this using a little bit of programming in the order button code. However, this method is quite faulty and you may still end up with a hacked page and not a dime of deposit from your customer's shopping cart. Encrypting pages that do not reveal source codes in the drop down menu is a good technique. Your best bet is to find providers who can sell you script to protect your source code so that hackers will not be able to bypass the payment page and download your e-book for zilch. The bottom line here is to never expose your source code for all the world to see.

DODGING SEARCH ENGINE SPIDERS

The homemade remedy is for you (or your programmer) to tinker with your webpage structure so that hackers will get confused. Make it difficult for anyone (even the search engines!) to access your download pages by using sub-directories (three levels down are best) or separate download pages. You will need to add redirect pages on your webpage while the sub-directories will make it harder for search engines to pick up the url and display it on the search results. As you replace water from your flower vase every week, so should you rename your download link every now and then.

Some high risk merchants would simply give customers access to the download page when they are able to make a deposit for the e-book they wish to download. I would say whatever technique that I have mentioned here works for you, suit yourself!

Source: <http://www.articlecircle.com>

About the Author

Gerri Bryce is a versatile technical writer specializing in general web content copywriting and development for finance and high-risk investment firms. She has contributed a massive number of articles for today's most popular technology, gadget, gaming, business, finance, and science news websites. She participates in a number of top webmaster / finance forums and focuses on new trends in high risk merchant account providers, one of which is <http://www.highriskexperts.com> Currently, Ms. Bryce lives in Marin County, California. She keeps herself abreast with Web 2.0 and cutting edge Internet trends by attending business workshops, online meet-ups, and conferences for web and business professionals. She also travels extensively throughout the United States and Asia. e-mail: gerri.bryce@gmail.com