To Protect Your Ebooks And Software From Being Stolen!

There are many systems that can lock your software or document, allowing you to control access to that file. But the problem arises with assuming that this will stop all theft. A well thought out, thorough protection system can deter theft, but it cannot stop it 100%.

There are many systems that can lock your software or document, allowing you to control access to that file. But the problem arises with assuming that this will stop all theft. A well thought out, thorough protection system can deter theft, but it cannot stop it 100%.

An "unbreakable" protection system simply does not, and will never exist. If someone really wants your information, they can get it, even if it takes years of work.

SO WHAT'S THE POINT? WHY USE ANY PROTECTION AT ALL?

There is no 100% security guarantee in anything, but that's no reason to totally ignore protecting your intellectual property -- A thief can easily kick in your front door and rob your house, but you still lock the door. Locking the door is not 100% effective security, but we still do it. Why? Because it deters most potential theft and those who are more determined will have to work a bit to get in.

WHO SHOULD USE PROTECTION?

The big question here is, HOW VALUABLE IS YOUR INFORMATION TO YOU? Sensitive, proprietary or private information demands some sort of protection, otherwise transmitting over the net is not an option.

If your information is not free, then it's obviously of some importance. So, how much damage would it do to you if it were made freely available? What type of impact would it has on your sales and could you (or would you) absorb that without thinking twice?

Is a $14 Ebook worth paying for another service to protect it? Probably not, but it depends on the situation and target market. What about a $2,000 report? Does the price change the perspective?

Businesses protect their property. If you believe your information or software to be of a unique or proprietary nature, you should protect that information using some means, no matter how small.

Companies like Microsoft lose hundreds of millions of dollars due to software theft and fraud, yet they continue to implement protection measures in their software. I would guess that without any protection whatsoever the losses would be in the billions.

WHAT SHOULD YOU EXPECT?

Like I said, there is no 100% way to prevent every possible incident, but you can make it very difficult and less likely to happen. At best what you should hope is to provide just enough security to close obvious security flaws and discourage would-be thieves. But not so much security that it discourages honest users and customers.

PROTECTION OPTIONS

Here are some common protection schemes:

No Protection: Just distribute your information and hope for the best.

- Pros: No special process to access files which means less support issues.

- Cons: File can be passed around, copied, distributed and/or sold without authorization from the owner. Can't prevent access after chargeback or refund.

General Password Protection: Simply requiring a predetermined password to install or register the file.

- Pros: Simple for customer or end user.

- Cons: File and password can be passed around, copied, distributed and/or sold without authorization from the owner. Can't prevent access after chargeback or refund.

PC-Unique Password Protection: Generates a unique password based on the user's computer.

- Pros: Can't pass around the file since it is basically locked to one machine.

- Cons: Requires an extra step for registration; Customer cannot move file to another PC; If their PC crashes they will need another unique password; Can't prevent access after chargeback or refund.

Delayed Registration: This requires a user to enter a second registration number a specific number of days after they first register the file. For example, after 90 days of use, they must enter a new registration number that they receive from you.

- Pros: It allows control over chargeback and refunds. The file will be disabled after the second registration period because you will not provide the second key to reactivate the file.

- Cons: Requires an extra step for registration; A user can request refund or chargeback AFTER the second registration period.

Post-Purchase Activation: Requires activation by online server. After user purchases they are entered into an online customer database. They then install and register the file by entering their name/email or some data. The server confirms the purchase and then activates the software. This method is become more and more common with big name software.

- Pros: Can prevent unauthorized distribution of file since the file must be activated by the online server.

- Cons: User must be online to register file; Can't move file to a different PC; Can't prevent access after chargeback or refund.

Active Password Protection: Each time user attempts to access file it checks an online server to confirm the usage rights and permissions for the user.

- Pros: Prevents distribution or copying of file; File Owner can revoke access to file after chargeback or refund; Access permissions can be changed and applied in real-time.

- Cons: must be connected to the net to register and/or access file; User may not be able to move file to another PC; User registration can be somewhat cumbersome and difficult for some customers.

EVALUATING PROTECTION SERVICES

When looking to protect your digital information any protection system or service that you consider should have a few basic security bases covered.

For software and executables:

1. When opening the file, a protection system must not save or copy an unprotected version of the file to the windows TEMP directory or anywhere on your PC for that matter.

2. The system should automatically prevent password sharing and access by unauthorized parties. This will prevent the document from being passed around or distributed illegally since it can't be opened unless you are authorized.

3. It should have some method to revoke or cancel access for refunded or fraudulent users.

For PDF documents, providing adequate protection requires a bit more security as there are many more ways to obtain a protection free copy of the document.

Any PDF protection system must cover the three bases above, as well as:

* It must prevent emailing of file and exporting or extracting pages from file.

* It must prevent copying file and text to the clipboard

* It must prevent redistilling of the file and printing to PDF

* It must prevent unlimited, uncontrolled printing of file

* It must watermark all printed pages

* If using Adobe Reader, the company providing the protection service must be an authorized Adobe DRM provider.

WHAT ABOUT COST? IS IT WORTH IT?

Is $300 a year too much to protect your copyrights? Definitely not. Protection costs money, but if your business is making money then it's a cost of doing business.

Is it for you? I don't know. Selling a few low priced applications a month probably won't warrant any sort of protection, but if you generate a substantial income from your software or the information distributed is of a critical nature to your business, then you need to protect your intellectual "capital" at some level.

FINAL THOUGHTS

Personally, I believe that some level of protection should be implemented on any piece of software or document that is of any value to you. You should never mass distribute a file in an unprotected format. Otherwise you will be scrambling when you find someone misusing it... if you find them!

It's easy to listen to those that say "don't worry about it" (a common reply to the document protection topic) until someone is actually stealing from you. Then all you can do is worry about it, but it's too late really. The damage is done. You can't take something back once it's out there unprotected. No amount of legal threatening is going to phase someone in Prague who just doesn't care about your copyrights.

Author: fusfus