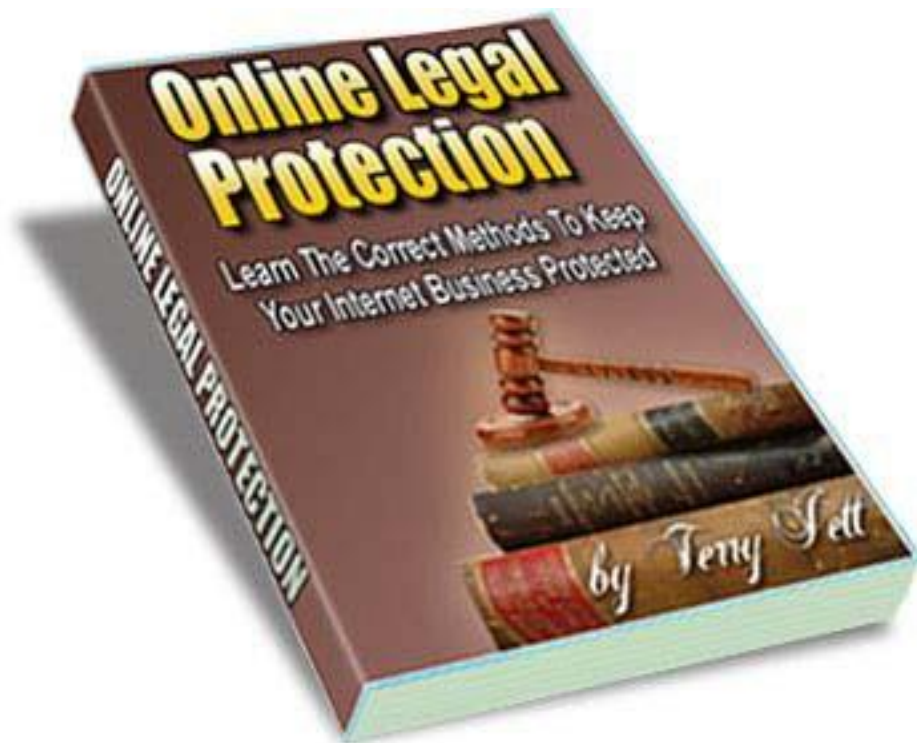


Online Legal Protection

Learn The Correct Methods To Keep Your Internet Business Protected



Brought To You By:

-8- Your Name -8-

<http://-8-yournameurl-8->

Table of Contents

Table Of Contents.....	- 2 -
Why Internet Marketers Need More Protection	- 3 -
You Can't Be Anonymous.....	- 5 -
Start With Basic Security Measures.....	- 6 -
Using Disclaimers.....	- 9 -
Proper Use Of Email.....	- 11 -
Protecting Product Rights	- 13 -
Protecting Your Website	- 15 -
Terms Of Use Or Service	- 18 -
Privacy Policy	- 20 -

Why Internet Marketers Need More Protection

From the moment you first connected to the Internet, you have probably been told that you need to use security measures to protect yourself. This is something that all Internet users face all of the time. There is a great deal more to protection for Internet Marketers however.

Internet Marketers need more protection than that average user simply because they have more to protect, and of course they have more at stake. The average user may use their personal computers to shop, play games, or to surf the Internet. As an Internet Marketer, you probably do all of those things, but you also operate an entire business online.

A hacker can easily break into the email that is associated with your website, read your mail, and use that account to send thousands of spam emails out – all in your name – between the time that you turn off your computer for the day and fire it up again in the morning. They could even do it while you are taking your lunch break – or while you are sitting in front of the screen working.

They may also manage to break into the databases on your website and obtain all sorts of private information concerning your customers. Either of these actions could literally put you out of business in a matter of hours – or minutes. This goes far beyond protecting your own personal credit card information or identity. This is basically about protecting everything you've worked so hard for.

The average user worries about computer viruses and protecting their identity. You have to worry about protecting yourself from computer viruses, protecting your website from malicious acts, protecting your customer's information, and protecting yourself legally. You would be surprised at the number of Internet Marketers who have failed to take these security measures.

The average user has the luxury of remaining totally anonymous on the Internet. The Internet Marketer does not have that option. There is a great deal of information regarding how to protect yourself from identity theft later, but this is another reason that Internet Marketers must use even greater security measures.

Internet Marketers have information that potential identity thieves want. You have customer names, billing addresses, phone number, and email addresses.

Online Legal Protection

You may also have credit card numbers, however, most payment processors are designed to encrypt that information, and there have been few instances where thieves have been able to obtain this information through a merchant's payment processing gateway. But the other information will give the thieves a head start regardless of this.

Aside from your own personal information, a thief or hacker is interested in the information that you have because of the customer information. Your customers trust you to protect that information with everything you have, and therefore, more security is required.

Then there is the legal aspect of your business. You need a disclaimer so that customers can't expect the impossible, or the not-so-average results, fail to get them, and then turn around and sue you because they didn't. There has always been a great deal of hype on the Internet, and now, there are laws to protect consumers from that hype. A disclaimer is necessary.

You also need a Terms of Service, or TOS. This serves to protect you and your other customers. It basically tells customers how they are to behave while using your site and this is typically more geared to sites that are community based – where customers interact with each other. Both the TOS and the disclaimer are covered in greater detail later.

You also have to protect your rights to any product that you create. This is especially difficult if you are dealing with information products, and it is a source of concern for most information product creators.

You also have to know how to use email properly, so that you not only protect your email account, but also because you need to ensure that you are following the law, and not putting your entire business – or your reputation – in jeopardy. Product rights and the proper use of email are also covered later.

It sounds like a great deal of work and worry, but the honest truth is that once you know what needs to be protected, and how to protect it, it isn't overwhelming or hard. It is just a matter of doing it. It is also a matter of keeping up with some basic technology advances, and also keeping up with what is going on in the dark world of hacking.

As an Internet Marketer, you have to think about protecting your computer, your website, and your information much like locking up your store at night and setting the alarm. Think for just a moment about a physical business. They have a good lock on the door. They have an alarm system. They probably have security cameras inside. They may even have a panic button that will quietly summon the police if there is a problem.

This is the kind of security that you need for your Internet Business – and without it, you are opening yourself, and your customers, up to a world of problems. So, now that you know you need the added protection, where do you start? You start with understanding how to protect your identity, in the Internet Marketing world where anonymity isn't really allowed.

You Can't Be Anonymous

Average users do more than protect their computers. They are also taught to protect their identity. This has a two-fold purpose. First, it protects them against identity theft, and second, it protects them in the physical sense. Unfortunately, Internet Marketers cannot be anonymous and expect to remain in business for long, even if they manage to get their business off the ground in an anonymous way.

This is another reason that Internet Marketers have to be even more cautious than average users – they can't be anonymous in most cases. Your name will be out there – hopefully in bright lights – but there is still a way that you can protect yourself from identity theft.

While your name must be out there for the whole world to see, this doesn't mean that other information must be made available. Most Internet Marketers are very open about where they are physically located in the world. They have to be, because the CAN-SPAM act requires that they include their business address in every single piece of commercial email that they send out.

Furthermore, you can't use a post office box. The law requires you to use your physical address. Most Internet Marketers work from home. What this means is that a potential identity thief not only has your name, but they also have your home address. An average user would never throw this information out there in the public – you are required to.

So, with your name and address out there for anyone in the world to find, how does an Internet Marketer protect their identity?

They do it the same way that everyone else does, but with a great deal more caution. Never store your credit card information or banking information online, for starters. Second, never give out your social security number, or any personal information that is not required from you during the course of business.

Online Legal Protection

Remember that you are already a target because your name and address are out there. If you keep that in mind, you will find that you are more cautious about sharing other personal information. In fact, you may be more cautious than the average user, as you should be, and therefore better protected from identity theft.

Finally, always look to see who is looking. While most people are urged to check their credit report annually, an Internet Marketer would do better to check their credit report every three months. This way, you will be better able to stop identity theft before it gets out of hand, and you find yourself in thousands of dollars worth of debt!

Start With Basic Security Measures

Just as average users use basic security measures, Internet Marketers must also use basic security measures. You should think of this as the foundation for all other security measures that you may employ for your online business.

You need anti-virus protection on your system. This virus protection must stay updated at all times. Don't take any chances with this. Make sure that you are running your virus protection at all times, and that you scan your system at least twice each week.

You need a firewall. Most systems today come with a firewall as a part of the operating system. Make sure that you set the security on your firewall to the highest possible setting.

You need spyware protection. This is not the same as anti-virus. They are two totally different things. Spyware protects you from malicious software that can gather information from your computer system, including keystrokes. Make sure that you keep this up to date, and that it is constantly running.

Your system should be password protected. If someone gains physical access to your system, they can easily install software to log keystrokes, and your spyware protection and anti-virus protection will not catch it. Use a strong password that contains uppercase and lowercase letters and numbers. Do not use common words.

Be extremely careful sharing sensitive information through email or instant messenger. These messages can be intercepted, and the information may prove valuable to a thief or hacker.

Online Legal Protection

Make sure that your operating system is always up-to-date. Often, software makers – and hackers – find holes in the operating system that would allow a hacker to gain access. When this happens, software patches are created that are designed to close those holes. You may have noticed that your operating system updates itself fairly regularly. If this is the case, make sure that you allow it to continue updating.

If this never happens, make sure that you have set your options for your operating system to automatically update. Without these updates, your system becomes vulnerable. Also make sure that any other software that you use on your system is regularly updated. The operating system isn't the only thing that can leave you vulnerable!

This brings us to how you use your computer. First, let's cover downloads. Never download anything from an un-trusted or unknown source. If you purchase a product, you can usually download it without a problem. It is the free downloads that you must concern yourself with.

Many free downloads contain viruses and/or spyware. If you don't read the license agreement that we all agree to, you really don't know what is being installed on your system. There may be third party software included that you weren't expecting. Take the time to read that license agreement!

Use caution when opening email attachments. Viruses are typically sent out this way. Once you open that attachment, if your virus protection does not catch the virus, you are infected. The only way to prevent this for sure is to not open attachments at all.

Of course, since you are doing business on the Internet you will have to open attachments from time to time. In this case, just make sure that you don't open anything that you don't expect or anything from people that you do not know and trust.

Use a pop-up blocker. Often warnings that you have a problem with your system may pop-up. These warnings almost look like a warning that your operating system is sending you – but they aren't. Often, they are malicious ads that will install software. Do not even click on the close button or the 'no' button on these pop-ups. Instead, just prevent them altogether with a pop-up blocker.

If your pop-up blocker does not prevent such messages from popping up, press the Ctrl key and the W key on your keyboard if you are running windows. If you are using a Mac computer, use Command and W.

Online Legal Protection

Beware of phishing scams. These are emails that claim that they are from a company that you most likely do business with, such as PayPal or eBay. They will tell you that you need to go to the site, and sign in for some security reason. If you click the link in that email, you are taken to a site that appears to be the site that you do business with, but it isn't.

The people who sent this email to you are attempting to gain access to your account with this email and fake website. Look for the signs. First, they won't address you by your first name, because they do not know your first name. The site that you do business with will always address you by your name.

Second, if you hold your mouse cursor over the link in the email, you will see that it actually goes to a different URL than the one in the email. This is a sure sign that this is a fishing email. Third, businesses such as these would never request you to sign in for security measures.

You may also receive emails warning you about viruses. These are usually hoaxes, and should not be believed. They will give you directions to either avoid the virus or to check for the virus. They may tell you to look and see if a certain file is on your computer, and in most cases, it will be – because it is an operating system file. Do not follow these directions. Instead, go to a reputable security site, such as Norton's site or McAfee's site and see if the virus is real first.

Make sure that you are using anti-spam features that come with your email client. These will keep you from being subjected to many virus hoaxes and phishing scams, as well as prevent you from letting potential spammers, or those who supply spammers with addresses, that you have a live address.

Often, spam is not a virus or a hoax. Instead, it has a small html graphic that you can't see included in it, and when you open the email, the sender is alerted that they have found a live address. By using spam filters, you will actually be cutting way down on the amount of spam that you receive.

If you have a network set up, where you connect multiple computers in your home together, you need the right router. Outsiders can take full advantage of your network if you aren't careful – especially if it is wireless. If you've opted to make files and such available to all computers on your network, those who are basically 'stealing' your Internet connection also have access to your files.

To prevent this, make sure that your router has a built in firewall, that each computer on your network is assigned a dynamic IP address, and that you use the security features that are included with your router and modem to keep outsiders locked out of the network.

Online Legal Protection

As you can see, there is a great deal to securing your personal computer. But once you are set up with the right tools, it becomes very painless and very fast. Just as you purchase the right tools for your online business; it is vital that you purchase the right tools for computer protection as well. This is a business expense that is vital.

Above all, just use caution and common sense, just as you do in your life. If something doesn't feel right or sound right, it probably isn't right. If your computer starts doing weird or unexpected things, don't assume it is just a glitch, or that your computer has a mind of its own.

It could be an indication that a virus, a Trojan, or some type of spyware has made its way to your system, despite your efforts to prevent this from happening. The best thing that you can do at that point is stop what you are doing. Open your task manager and see what processes are running. Make sure that your anti virus and anti spyware are up-to-date and let them scan your system. Find out what caused the weirdness and eliminate it.

Using Disclaimers

Disclaimers are a vital part of any business. A disclaimer serves to protect you in the legal sense, and depending on what you are marketing, they relate to the results that one should or could expect from the use of a service, product, or method.

Disclaimers can be used on websites, inside products, and in email. It is basically a 'use at your own risk' statement. Have you read an ebook lately? It probably had a disclaimer stating that the information was for informational purposes only, and that the author and/or publisher would not be held responsible for any results you may receive from your use of that information.

Failure to use disclaimers can result in lawsuits. Don't think that this won't happen to you – it has happened to many others, to the tune of millions of dollars.

A site disclaimer can entail many different things. First, you disclaim the information, stating that it is for informational purposes only, and that you claim not responsibility for the information, or for your visitor's use of the information. You then can disclaim any endorsements that you make of other people's

Online Legal Protection

products. Finally, you can disclaim any links that may appear on your website as well.

Many people do fail to use disclaimers, because they feel that they are essentially saying 'I don't know what I am talking about.' This isn't what you are saying. What you are saying is that this is what you know, but you are not going to be responsible for someone else's use of what you know.

Email disclaimers also have a variety of uses. They are typically used by corporations, and may cover topics such as negligent misstatements, entering into contracts, transmission of viruses, breach of confidentiality, or it may be a complete disclaimer.

A complete email disclaimer looks like this:

"This message may contain confidential information. It is intended only for the person named in the email. If you are not that person, you should not use, distribute, or copy this email. You should notify the sender that you have received the email by mistake, and delete it immediately. We cannot guarantee that this email is secure or error free. Information could be corrupted, destroyed, intercepted, lost, or contain viruses. We do not accept liability for any errors or omissions in this email message. For verification, please contact us at ABC Company, 123 Any Street, Any Town, Any State, 00000, Any Country, www.website.com. "

A sample website disclaimer looks like this:

"All information contained in this website is intended for general information purposes only. The information is provided by ABC Company. We try to keep the information up-to-date and ensure that it is correct, however, we make no warranties of any kind concerning the accuracy, completeness, suitability, reliability, or availability of the information contained in this website, or any products, services, links, or graphics that may be found on this website. Use this information at your own risk.

ABC Company will not be held liable for any loss or damage, or loss of data from your use of this website, or in connection with this website. This includes indirect or consequential loss or damage.

ABC Company has no control over websites that are linked to on this website. Those third party websites are under the control of their owners, and ABC Company will not be held liable for your use of those websites. By linking to these sites, we are not endorsing or recommending any information or views expressed in the content on those sites. "

Online Legal Protection

The above disclaimer can also be used for information products, as long as it is altered to reflect the product, instead of a website.

Finally, as an Internet Marketer, you may need income disclaimers as well. An income disclaimer generally states that any results advertised in your email or on your site are not to be considered typical, and that you have no control over how much one might earn from their use of your information.

Here is a sample of an earnings/income disclaimer:

"While every effort has been made to accurately represent the potential of this information/product, ABC Company cannot guarantee how much money you might earn, as we have no control over your efforts or your use of the information. Examples and testimonies used on this site are not to be interpreted as a promise or guarantee of your expected earnings. "

Disclaimers look fairly simple and straight to the point, and because they are straight to the point, you may be afraid to use them. Don't be – instead, you can soften them a bit, just as long as it is still clear that you are not going to be held liable for someone else's use of your information.

Before you write your own disclaimer, take the time to read those used by other companies. This will give you more ideas for your own disclaimers, and help you to write one that covers you from all directions.

Proper Use Of Email

The chances are very good that you know how to use email. Email, after all, is becoming the most popular and most widely used form of communication worldwide. As an Internet Marketer, knowing how to use email is as important, if not more important than knowing how to use the telephone. But do you know how to use email properly?

Rule number one is to never, ever send out any spam, or anything that might be construed as spam. Rule number two is to not use your email client to send out mass email. Instead, use an autoresponder. This way, you won't bog down your ISP, who might actually shut you down because you are bogging the system down.

Every commercial email must contain your business name and physical address. It must, by law, have instructions for people to remove themselves from your

Online Legal Protection

email list. You have the option of including a disclaimer. If you have employees who use business email, you most likely need an email policy as well. This policy basically lays out the rules for the usage of the company email system, which employees are to follow to the letter.

Do not send attachments in email unless they are expected by the recipient. Also, run your email – especially emails sent out to an opt-in list – through a spam checker to make sure that your message won't hit the spam folders. Make sure that your virus scanner is set to scan all incoming email.

Finally, use these twenty rules of email etiquette when sending email. These don't relate to protection, but they will be good for your business!

1. People are in a hurry, get to the point. Emails are not like letters – they are usually short.
2. Answer all emails in a timely manner. Make sure that you've answered all of the questions asked.
3. Check your spelling and grammar. Most email clients include spelling and grammar checkers. Use them.
4. To avoid dry emails, make your email personal. Address the person by name.
5. Do not attach files, unless they are expected.
6. Do not write in all capital letters.
7. Do not use the high priority option, unless it really is a high priority.
8. When mailing to multiple people with your email client, use the BCC field instead of the CC field. It is rude to share other people's email addresses with others.
9. Do not overuse emoticons, and take care when using abbreviations.
10. Do not request read and delivery receipts. People feel that this is an invasion of their privacy.
11. Do not forward chain letters, unless you are forwarding it to people that you know are enjoying them. Be sure to ask first. Never forward virus hoaxes.

Online Legal Protection

12. Never reply to spam messages.
13. Never discuss confidential information in email. It could be intercepted. Instead, let the recipient know that you have something confidential to discuss, and either ask for a good time to call, or include your phone number and state when you will be available for a telephone call.
14. Always use a subject line that relates to the email message. Don't try to fool the recipient.
15. Make sure that your email is formatted properly, so that it does not break up in your recipient's email client. The general rule is 45 to 50 characters per line, including spaces and punctuation.
16. When replying, make sure that you leave the message that the person sent you in the email message you are sending back, for easy reference.
17. Use caution when sending rich text or HTML messages. Not all people want to receive these.
18. Make sure that you are replying to the right person. If the email was sent to multiple people, you may or may not want to use the reply to all features, depending on the nature of the email, and your response.
19. Avoid using words like URGENT or IMPORTANT unless it really is. Don't use hype.
20. Read the email before you send it. Correct any mistakes, and make sure that it is indeed the message that you want to send. Once it is sent, you can't take it back.

Protecting Product Rights

The rights to a product are something that most product creators these days – especially creators of information products – worry about. The Internet offers us the ability to find any information that we want – that is what it is all about – the sharing of information. This doesn't mean that you want to share the rights to your product.

The first thing you need is a copyright. Copyrights are used on websites and in products – and may even be used in emails. Many people mistakenly think that copyrighting information requires filling out forms and paying fees. This isn't

Online Legal Protection

true. The fact is that as soon as you write something down or create something, it is copyrighted.

You don't ever have to fill out a form, or pay a copyright fee, although in some instances, you may want to. This is typically done for hard copy books, music, and other creatives – but not usually done for digital products. This doesn't mean that it cannot be done for digital products.

The fastest way to copyright something, however, is to add this statement:

Copyright © 2007 by Your Company Name
All Rights Reserved.

That alone takes care of it, although because the person who first writes or creates something owns the copyright, it is important that you have some documentation that indicates the exact date that the product was created, in case someone tries to infringe on your copyright. Microsoft Word does this.

You won't find the copyright symbol on your keyboard. It is created by holding down the CTRL key and pushing the numbers 0169. Give it a try. It can also be found in the character map, which you will find under your start button > all programs > accessories.

If you have work created for you, it is called 'work for hire.' Usually, the law requires that the copyright is automatically transferred to the person paying for the work, when the creator is paid for that work. However, depending on whom you are dealing with, you may want to create an agreement that states exactly when and how the copyright is transferred to you.

Of course, copyrighting work doesn't necessarily prevent others from stealing your hard work. There are many out there who are not above plagiarism – and this is a problem.

You can use a fabulous website called Copy Scape at <http://www.copyscape.com> to see if others are using your work. This is a free service. If you find someone else using your work, the first step is to send them an email asking them to remove the plagiarized work. If this fails, send them a registered letter, via postal mail. If that fails, you will most likely need a lawyer to intervene, and you may have to take them to court.

There are two other ways that you can protect your product rights. The first is a non-disclosure agreement, and the second is a non-compete agreement. These are useful when you have other people doing work on your product. They know

Online Legal Protection

all of your secrets, and without a non-disclosure agreement, they are free to tell your competitors whatever they want to tell them.

You can find many samples of non-disclosure agreements on the Internet, for free. It is a good idea to have anyone who works for you sign an NDA, and have it notarized as well. While this may not stop them from sharing your secrets, it certainly gives you more of a legal leg to stand on in the event that they do.

A non-compete agreement is a little different from an NDA. A non-compete agreement essentially states that the person working for you is not allowed to compete with you or work for your competitors for a certain number of years after leaving your employ.

These are typically meant for full-time employees. They are not usually meant for people who do contract work, because it would prevent them from making a living after their work with you is finished. For these people, an NDA should be used instead. Like NDAs, non-compete agreements can also easily be found on the Internet, and you will find links to both in the resources section of this ebook.

Other than using technology that prevents people from printing or copying your work, or prevents them from seeing programming code, this is really all that you can do to protect your work. Remember the steps for dealing with someone who has used your work:

1. Contact them via email. Request that they remove the plagiarized work.
2. Contact them via postal mail, using registered mail that they have to sign for, so you can prove that they received it.
3. Hire a lawyer, and have them contact the violator.
4. Take them to court.

Be prepared. Court action is not cheap, and neither is hiring a lawyer. If possible, work it out without either of these things, and only sue as a last resort.

Protecting Your Website

Protecting your website from hackers is crucial – not only for the security of your business, but also for the security of your customer's personal information.

Online Legal Protection

Hackers know how to break into a website, so to speak, and literally take control of it, and you have to know how to protect yourself, and your customers, from such actions.

Aside from really messing up your site, the most dangerous thing is that hackers can implement viruses that your customers are infected by when they visit your site, and they can take control of your email to send out viruses and spam. Both of these actions can make you liable, if you aren't careful.

Start by removing any unnecessary files from your server. Even if the files are not viewable on your website, search engines can still find them and index them. That leaves these unused files open to exploitation. Make sure that you are not removing any needed files, and make backups of those files before you delete them.

Keep your other files up to date. This is especially important for script or program files. Just like operating systems, the creators of these programs and scripts often update them to work out bugs and close security holes. Failing to keep your copy up to date is an invitation to be hacked.

Use a robots.txt file on your server. This file can be used to tell search engines not to index certain files, and also not to index images. Images can be searched for, specifically, and this makes it easy for someone else to steal your images.

If you have databases, scripts, or any other sensitive file, it can and should be password protected. Make sure that you are using passwords that are not easy to crack. Files such as these are the ones that hackers really like, so make sure that yours are protected with a strong password.

Don't think that using the script that prevents right clicking on your page will protect your content. It won't. People are getting smarter, and they can just as easily go to their browser window, select edit > select all and then edit > copy and capture everything on your page. Instead, use a script that hides your source code completely. Even better than that, use style sheets for your HTML.

If you left click on each file on your server, you will be presented with the CHMOD option. This enables you to set permissions on each file, and it is important that you do so. You can check with your web host or web developer to find out how the permissions should be set. The options are read, write, and read – write. This allows some people to only read the file, while others have the option of reading and writing to the file. Note that changing these permissions may have an adverse affect on some scripts or programs.

Online Legal Protection

Protecting your sites email is extremely important. As a business owner, you probably have opt-in forms and feedback forms on your website. If you ever receive a strange message from your feedback form, be on the lookout for spammers. It is best to use a script that hides your email address, or to use an image for email, instead of an actual linked email address. These two methods will help to prevent spam software from collecting the email address.

As netizens, we put our email addresses out there in a lot of ways – and many times, we don't even realize that we are doing so. We sign guest books, participate in forums and newsgroups, and of course we advertise. First, start using a throw away email account, such as a Yahoo account. Failing that, don't put your email address as you@yourdomain.com. Instead, use you at your domain.com.

Make sure that you change the password to your control panel often – at least once every thirty days is recommended. You should also password any folder that contains set up files, if possible. Some applications won't work if the setup files are in a password protected folder, but since most applications no longer use the setup files, once the application is set up, this can work – and it does protect your website.

Is Telnet available for your site? If so, turn it off. Most hackers use Telnet to connect to what they want to connect to, and to do their dirty deeds – and by leaving Telnet turned on, you are inviting them to do so. Be sure to ask your web host whether or not you have Telnet, and if so, how to turn it off.

Make sure that your scripts are running from the right directory. You will find that most CGI scripts, Perl Scripts, and PHP scripts are meant to run from the CGI-Bin. This is because the CGI-Bin offers protection from hacks.

Failure to protect your website from spammers and hackers can have incredibly bad results for you. Your site could be shut down. It could be blacklisted. The entire server could get blacklisted as well. Hackers may steal valuable information from your site. Repairing damage will cost you in terms of time, and possibly in money.

Spammers can use your website to send mail bombs from your domain, to send spam from your domain, and to steal passwords and other private or sensitive information. Always make sure that you are doing everything that you can to protect your website.

Terms Of Use Or Service

You have probably become a member or used websites that actually have a Terms of Use or Terms of Service in place. A TOS, or Terms of Service, is quite different from a disclaimer. While a disclaimer disclaims, a TOS basically states the rules of using your site or service.

There are three main objectives you should have when creating your TOS. The first is that it must be understandable by the average person. A TOS that is full of legal jargon probably won't do you much good. Use everyday language. The second objective should be to make sure that your TOS is easily found on your site.

Many website owners include the TOS when a person registers for the website. After they have filled out the registration form, they are presented with the TOS, and it includes a checkbox that says that they have read and understand the TOS. If the site does not have any type of registration, the TOS may just be present, but may not require that a visitor gives any indication that they have read or understood the TOS.

In the second case, the words used in the TOS become more important. You must state that just by using your site that the visitor has automatically agreed to the TOS. Ideally, however, you will require your visitors to give some type of indication that they have read and do understand the TOS.

The third objective is to make sure that the TOS covers everything. Remember that this is a document designed to protect you from lawsuits down the road. The TOS should state what could go wrong, and what you will not be held liable for. It should also state how your visitors are expected to behave on your website. This is crucial for community websites, where customers interact with each other.

A Terms of Service agreement is typically used when the website offers some type of service, other than information. A Terms of Use agreement is typically used for information only type websites.

Here is a sample TOS/TOU:

"By using our website you are agreeing to comply with and be bound by the following terms of use. Review the terms carefully, and if you do not agree with them, do not use this website. The terms us, we, or our refers to YourCompany, while the term you refers to the user or viewer of the site.

Online Legal Protection

You agree to the terms and conditions as outlined in this Terms of Use Agreement with respect to our site. This agreement is the entire and only agreement between us and you, and it replaces any prior agreements you may have had with us, with respect to our site, products, services, and content. We reserve the right to change this agreement from time to time, without notification. The latest agreement will be posted on our website, and it is your responsibility to review the latest agreement.

This site is copyrighted by us. This copyright covers all content, organization, design, graphics, compilations, digital conversion, and magnetic translation that relates to this site. Copying this website, unless otherwise allowed, is a violation of our copyrights, and is strictly prohibited. You do not own any rights to any content on this website, unless it is your own work, such as messages you have written in our forum.

Ourcompany.com and others are our service marks or registered service marks or trademarks. Other product and company names mentioned on this site belong to their respective owners.

You are granted a non-exclusive, non-transferable, revocable license to:

- a. Use the site strictly in accordance with this agreement.
- b. Use the site solely for internal, personal, non-commercial purposes
- c. To print out information from the site solely for internal, personal, non-commercial purposes, ensuring that you adhere to all copyright laws and other policies in your usage of that information.

You are not granted permission to use any information printed from our site in any type of litigation or arbitration, under any circumstances.

Your right and license to access and use this site, including any information or materials on this site, are subject to the following restrictions and prohibitions of use:

- a. You may not copy, print (except as expressed above), republish, distribute, display, sell, rent, lease, loan, transmit, or otherwise make available in any form, or by any means, all or any portion of this site or any content and materials retrieved from this site.
- b. You may not use the site or any materials on the site to develop any information, storage or retrieval system, database, information base, or any other similar type of resource that we offer for commercial distribution of any kind, including through license, sale, lease, rental, subscription, or any other type of distribution. "

As you can see, a TOS can get very long. This sample gives you the basics of a TOS, and your TOS should be designed to protect you and your site, specifically.

From here, it may go on to state rules for communicating on the site, and it should also go on to state how you intend to pursue those who violate the terms of service.

Privacy Policy

While a TOS may be very long and drawn out and very detailed, a Privacy Policy is typically more cut and dried. You absolutely must have a privacy policy, and many other sites that you do business with will actually require you to do so in order to use their service – such as a payment processing company for your website.

Here is a sample privacy policy:

"Thank you for visiting our website. This privacy policy is designed to inform you how information is collected from our site, and how that information is used. Please read this privacy policy, in its entirety, before using our website, or submitting any personal information through our website.

By using our website, you are accepting the practices described in this privacy policy. These practices may be changed, and those changes will be posted on the website. All changes apply to practices moving forward, and do not affect the policies used in the past.

The privacy policy displayed here only pertains to this site. We link to other websites, and those websites have their own privacy policies. Our privacy policies do not pertain to their website, and their privacy policies do not pertain to our website.

We collect personally identifiable information, including names, postal addresses, email addresses, etc. That information, however, is only obtained by us, when it is voluntarily submitted by you and our other visitors. If that information is provided to us, it is done so to help us fulfill your request. The information is only used to fulfill that request, unless you give us specific permission to use it in some other manner.

This site may use cookie and tracking technology, depending on the features offered. The use of cookies and tracking technology are needed for gathering information that includes the type of browser you are using, the type of operating system you are using, and in tracking the number of visitors to our

Online Legal Protection

site. This enables us to understand how visitors use our site, and how we can make changes that benefit our visitors.

Personal information cannot be collected with the use of cookies and tracking technology. The information gathered from the use of cookies and tracking technology on this website is used for internal information only, and not shared with others in anyway that could personally identify our visitors.

We may share information with governmental agencies or other companies if they are assisting us in fraud prevention or investigation. We do this when it is permitted by law for us to do so, or when we are trying to protect against or prevent fraud or unauthorized transactions, or when we are investigating fraud that has already taken place. The information is not provided to any company for marketing purposes.

Your personally identifiable information that you provide is kept secure. Only authorized agents, contractors, and employees, who have also agreed to keep information shared with them confidential, can access this information. Any email or newsletters sent to you through our website are those that you requested, and each one will allow you the option of opting out of further mailings.

If you have problems, questions, concerns, or comments related to this privacy policy or our website, you may contact us at:

Our Company
Street Address
City, Town, Zip Code
Phone Number
Email Address

We reserve the right to change this policy, if we find that changes are needed or warranted. All changes to this policy will be posted on our website. "

Again, you can adopt the privacy policy example to suit your own purposes.

Overall, as an Internet Marketer, you must view everything from different angles. You must consider how information can be compromised, and also consider how your own content and services can be used against you from a legal standpoint. When you see problems that may occur, it is up to you to implement legal policy for your site that is designed to protect you – or to implement security measures designed to protect you and your customers or visitors.

Online business owners simply must see a bigger, wider picture than an average computer user sees. While you won't always catch every potential problem, if

Online Legal Protection

you follow the information in this guide, the chances are very good that you won't find yourself in the middle of a legal battle that pertains to your website or online business.

Your two main objectives should be to protect yourself, and to protect your customers!

This is a "guide" to protecting your business and yourself. The author takes no responsibility and will not be held liable for any losses. You should always consult a lawyer for professional legal help/advice.