
Internet Traps, Rip-offs And Pitfalls

And How To Avoid Them

By Mike Alexander

If you haven't already done so, save this ebook to your computer by going to the *File* menu (top left), and choosing *Save a Copy* or *Save Page As*. Specify where on your computer to save it (such as your *My Documents* folder) or remember where you put it. If you get an error message saying " *This document does not allow you to save any changes...* " or something similar, just click OK.

Legal Notice

This is a free ebook. You may not sell it or in any other way offer it in exchange for monetary gain. You are however, permitted to give it away, or the link to it, provided it is not altered in any way. You are also permitted to include it, or the link to it, in any bundle or package of digital goods (i.e. electronic information or software) that you make available to the public (e.g. subscribers to a mailing list or members of a closed website) whether you charge for the package or not, provided the document is not altered in any way. You may not, under any circumstances, send it, or the link to it, to anyone by email without first establishing that you have their permission.

Contents

Chapter One	Introduction	Page	2
Chapter Two	The Internet For All	Page	5
Chapter Three	Good And Bad	Page	8
Chapter Four	A New Underworld	Page	10
Chapter Five	Primary Defenses	Page	14
Chapter Six	A New Gold Rush	Page	17
Chapter Seven	Cautionary Tales	Page	20
Chapter Eight	Opportunities For All?	Page	23
Chapter Nine	The Holy Grail	Page	27
Chapter Ten	Conclusion	Page	30
Appendix I	Glossary	Page	33
Appendix II	Recommendations	Page	38
Appendix III	Useful Tips And Links	Page	45

Chapter One

Introduction

1.1 Downloading This Ebook

If you *click* any *links* in this *ebook* whilst reading it in a *browser*, they will open in the same window, so you have to use your *browser's* **Back** button to return to the *ebook*. The drawback is that you then have to find where you were in the book because it will re-open at the beginning, **not** where you previously were. The best solution to this is to save the *ebook* to your own computer, then any *links* you *click* will open up in a **new window** in your *browser* and not affect your place in the *PDF file*. Also, the *ebook* will be to hand in the convenient form of a *PDF file* instead of you always having to find the *link*.

To do this, *click* the 'File' menu above and save it to your 'My Documents' folder or wherever you want to keep it. Over-write the file name that shows and call it **InternetTraps.pdf** (or something similar that you will recognize—but make sure the extension is .pdf).

You should then be able to go to the folder where you saved the *ebook* and double click it to open it as a *PDF file*.

1.2 Glossary

In case you are wondering why some words are in italics, it signifies the use of *Internet*, computer or marketing **jargon** and a short explanation of that word or phrase will be found in **Appendix I**. Also, wherever the name of this *ebook* is used in the **text**, it is usually substituted with the acronym *ITRAPS*.

1.3 Operating System

Unless otherwise stated, I am assuming that your computer is running on a version of Microsoft Windows. Where this is not the case, the assumption is that you are technologically advanced enough to translate any terminology used to apply to the *OS* you have.

1.4 Getting The Most Out Of This eBook

If you are new to the *Internet* and want to pick up some tips on how best to use it and how to guard against dangers, you may contemplate skipping those chapters that deal with *Internet* marketing. This is **not advisable** though, as there is much to learn that can be useful about **how marketers view you** and may approach **you** as a potential customer.

Besides, you might wish to try your hand. *Internet* marketing can be a thoroughly satisfying and extremely rewarding pastime or occupation or, admittedly, a real pain in the butt that can suck you dry **if you don't do it right**. It depends, among other things, on whether you have a proper understanding of how the *Internet* works, a strategy for getting past the obstacles, and knowing what to look for in a *bizopp*.

If you want to take the satisfying and rewarding path, and get **maximum benefit** from *ITRAPS*, be sure to read every word from beginning to the end, **no matter how tempted you might be** to start at the end and work back. And whatever

you do, don't miss **Chapter Ten** if you have an interest in earning money!

1.5 The Main Aims Of This eBook

1. To provide a short but structured **guide to the Internet**.
2. To help you with the **security issues** you need to deal with.
3. To outline the many **traps and pitfalls** you need to avoid.
4. To explain how to **recognize scams and rip-offs**.
5. To cover **working from home** and finding the **ideal opportunity**.

1.6 Who Might Benefit From It

My studies into how much understanding the average person has about the issues covered in *ITRAPS* indicate that **most** readers are likely to find something here from which they can directly benefit.

If you are a *newbie*, it is highly likely that the majority of this information will come as a surprise, as well as the precautions you need to take. And even if you're a more seasoned *Internet* user, of perhaps three or four years experience, the chances are that you will learn something new. Some of the more invasive techniques being used by the 'bad guys' are only now coming into more general prominence.

If you are a parent with children who use the *Internet* at home, or at the library, or a friend's house, or anywhere where they might be unsupervised, maybe to do their homework or work on a school project, you **must** have **at least** the level of knowledge about the *Internet* that this little book provides. And, come to think of it, **so should they**.

Or, have you ever been tricked by a really slick sales letter? You buy a program or a piece of *software* that promises to solve a major problem, only to realize after hours (or weeks) of trying to get it to work, that it's not going to help at all. Or certainly not to the extent you expected. Then you find that you can't get your money back despite their "ironclad guarantee"? We are not necessarily talking about criminal behavior here. It's sometimes more a matter of deceptive advertising, exaggeration or over-enthusiasm. *ITRAPS* uncovers many criminal activities that you need to be aware of and also helps you recognize these rogues as well. They can strip you bare almost as efficiently and you need a strategy to deal with them too. This *ebook* can help with that strategy.

Perhaps you're an experienced marketer who, so far, has been unable to make a reasonable income *online*. If so, you are not alone. Despite all the promises of the so-called *gurus* of *Internet* marketing, the average marketer struggles for years before succeeding—and unfortunately many never do. *ITRAPS* will help you **understand why**.

As well as being a communications hub that can link you to a *virtual* treasure chest of knowledge, you will soon find that the *Internet* offers an absolute plethora of *WFH* opportunities that just weren't possible a few years ago. However, if you want to make money *online* by working from home, you need to take **extra special care**. There are many, many schemes available but even more **traps for the unwary**. *ITRAPS* spells them out and points you in the right direction. There is a very special opportunity too, that you definitely should **not** overlook, in **Chapter Ten**. It was put together as soon as I finished the first draft of this book and realized how few genuine opportunities there are which incorporate all, or even most, of the recommendations I make about what to look out for. **Don't miss it!**

1.7 Why Listen To Me?

I am not a *guru*; in fact I'm not too fond of them. I'm an ordinary guy who has tried just about every "sure thing" going, every "next big thing", every "answer to all your problems", all the "secrets they have been keeping from you", and more. In other words, you should listen to me because I have been scammed more times than I care to remember. I know

what it feels like, I know how they do it, but most of all, **I know what to look out for.**

Okay, so what do else do I have that might qualify me to help you?

Well, I started working *online* over 15 years ago, when CompuServe was big, the *Internet* was new, and was still mostly used by academics.

I have a successful *Internet* business. Not wildly successful; it doesn't bring in a million a year, but then again it was never expected to. If you know the 'newsletter content' business, then you know that it's an extremely competitive field. Nevertheless, enter that term (newsletter content) in a *Google* search form and you'll see my *site* on the first page. It was number five out of **40 million** entries the last time I looked. It's called ClipCopy Content Solutions. I also run '101 Internet Answers', where I **give away** my **FAT** (Fully Automatic Traffic) **System**. (For details of these and the rest of my sites, look under '101 Answers Sites' in Appendix II.)

I also run an *ezone* about newsletters called '101 Newsletter Answers', and a 'Free Ad Tips' mailing list. Full details are also available in Appendix II under '101 Answers Mailing Lists'.

I'm an 'oldie' too, with a wide experience of life and the world, having traveled extensively and actually have official citizenship of three different countries. I've been a salesman for practically all of my working life and one of my most recent positions in the corporate world was as sales manager of a publishing company where I was responsible for a team of twenty five salespeople.

Almost everything I've learned is solidly based on practical experience, both *online* and as a sales and marketing executive and trainer.

Chapter Two

The Internet For All

2.1 The Developing Internet

Probably the most amazing thing about the *Internet* is the rate of technological development and the advances that spring from it. Nothing stands still; from its inception up to now is only a matter of a few decades yet the advances in that time are nothing short of phenomenal. And so it continues. *Broadband* access, for example, has given rise to video on the *net* and the growth of *sites* such as YouTube. Video editing, video news clips, user-generated video, video ads etc are some of the first things that come to mind now whenever the *Internet* is mentioned. Game playing is another; it's a huge industry on the *Internet* now. Portability has become a hot issue too, with the rise of wireless technology on the one hand and rapid proliferation of cellphone *networks* on the other. Peer-to-peer *file* sharing over the *Internet* has had a lot to do with the popularity and availability of music of all kinds, while the plummeting cost of optical and other electronic *file* storage systems, together with exponential growth in the volume of data that can be stored in very small physical areas, has helped foster the attraction of free 'social *networking*' *sites* such as MySpace.

2.2 The Wonder Of Email

The oldest, and still one of the most useful *protocols* on the *Internet* is *SMTP*, which governs the way *email* works. There is no doubt that it's beginning to creak a bit under the weight of its biggest problem, *spam*, but I don't believe it's about to curl up just yet. Nevertheless, *spam* now amounts to 90% of all *email* and is a major hindrance. Home users are the least affected if they just use *email* to keep in touch with friends and family. People who use it mainly for business contacts are likely to feel the effects of *spam* more but the biggest casualty is the business owner who sends out a regular *ezone*. Because of the prevalence of *spam*, many of their subscribers will use filtering *software* to reduce the amount of junk mail they have to deal with, or alternatively, they make use of a filtering service provided by their *ISP*. When it's their own *software*, they should know how to *whitelist email* addresses but when they use their *ISP's software*, there are often 2 problems:

1. Very aggressive settings, so practically all 'commercial' *emails* get blocked.
2. Reticence on the part of a lot of *ISPs* to *whitelist* addresses for them in a reasonable time.

Information about *whitelisting* is included in Appendix III.

2.3 Here Is The News

NNTP once ran a close second to *SMTP* as the most-used *protocol* of the *Internet* but has since been relegated to an also-ran position by the rise of the World Wide *Web*. It is sometimes called *Usenet* and is made up of '*newsgroups*', which has nothing to do with the news as you would normally think of it. *Newsgroups* are really text-based *forums*, each focused on a particular theme. *Usenet* is actually only one of many *NNTP networks*, although it is the biggest. Microsoft, for example, runs one of its own, and many *ISPs* and other organizations do too.

There are thousands of *newsgroups* on *Usenet* covering just about every human activity ever thought of, yet all the administration is managed by volunteers, (quite remarkable when you consider its scope). Its decline has more to do

with the fact that *newbies* seem to get mesmerized by the *WWW*, once they discover it, rather than there being anything inherently wrong with it—a great pity since it has so much to offer. Special *software* called a 'news reader' used to be necessary to access *newsgroups* but now most *email* applications, like Outlook Express or Thunderbird, can be used instead. (More about *newsgroups* appears in Appendix III.)

2.4 Transferring Files

FTP, which stands for *File Transfer Protocol*, is still very much in use on the *Internet*, though you might never have heard of it if you don't run a *website* of your own. This is because its main purpose nowadays is for *uploading files* to a *web server* for the creation or maintenance of *websites*. It can also be run on the *web* to *download files* but when you do this via a *browser* the *protocol* is hidden from your view so you are usually not aware of it at the time. *FTP* was the original *protocol* of the *Internet* and was designed so that academic institutions could transfer *files* seamlessly by computer.

2.5 The Glory Of The Web

It was a brilliant Englishman, Tim Berners-Lee, who dreamed up and named, invented if you like, the *World Wide Web* during his time as a scientist at CERN, the European Particle Physics Laboratory. He did it by bringing together three main elements: *HTTP*—the *WWW protocol*; *HTML*—the 'language' of the *web*; and the *URL* system—for 'addressing' *websites* anywhere in the world. The use of these three elements transformed the *Internet* into what he called "a single, global information space". It allowed for the first time, transmission and retrieval of 'pages' that could each consist of many *files*. These might be *graphics files*, *text files*, *sound files*, or indeed any other type of *file*, since the only restriction is in the application that can interpret the language and present the results as viewable pages (what came to be known as a *browser*). Thus rich, interactive, multimedia documents, each capable of being *linked* to any other *files* on the *Internet*, suddenly became accessible to everyone. The *WWW* virtually took over the *net* and has been expanding at an exponential rate ever since. Tim Berners-Lee still serves on 'W3C', the *WWW* governing consortium.

2.6 Searching For Information

One of the most common complaints about the *net* right from the very beginning has been that finding things can be so problematic. People have previously been used to information being indexed in directories in the way that telephone numbers are, and are often frustrated to find that it isn't the way things are on the *Internet*. So why isn't it? Well, for one thing, it's impossible to index all human knowledge and that is virtually what the *net* now is—a repository for all knowledge. This is exacerbated though, by the problem of 'pseudo-knowledge'. You have to bear in mind that anyone in the world can put up a *website* or start a *newsgroup*, assign themselves 'expert' status, and then promulgate distorted facts and opinions. If challenged, such people often try to justify their view of things with even more distortions and falsehoods or eventually fall back on the argument that everyone is entitled to an opinion. To use the *Internet* effectively you have to be able to **differentiate between facts and opinions**.

One of the major reasons why the *Internet* seems to be so chaotic though, is that there is no owner. There is a governing body but their responsibility is to oversee the various *protocols*, approve developments in the interpretation of the languages of the *web* (*HTML*, *DHTML* etc), oversee the registration of owners of *domain names*, allocate *IP addresses* etc.

As a result, it was left to private enterprise to come up with solutions to help people find things. At first, most were fairly inefficient, mainly due to the fact that the *web* was growing faster than they were able to list things. There were, and still are, two main types of *web* indexing services:

1. Those that use *spiders* to find *sites* and list them in a searchable database
2. Those that accept submissions and list entries manually in a directory

Things have now settled down considerably to just a few major players and, of the two main ones, *Google* belongs in the first category and *Yahoo* in the second. Look in Appendix III for some advice and tips on searching for information.

2.7 Making Contact

There are many ways of making contact with other people on the *Internet* as well as the standard ways already mentioned. There is *web* telephony (*VOIP*, fax etc via the *Internet*) for instance, *IRC* (*chat rooms*), *web forums* and *blogs*, and probably most popular of all, by *Internet* messenger services such as those provided by Microsoft (*Windows Messenger*), *Yahoo* (*Yahoo Messenger*), *Skype* etc. One of the main advantages with these systems is the use of *webcams* which adds a video element. There are links to information about these and other ways of making contact in Appendix III.

2.8 Working The Net

The *Internet* has become so all-pervasive that it is now more common than not for businesses in the Western world to provide access to it for employees. The research possibilities and the convenience of interaction within the company, especially larger organizations with a national or international reach, are the main attractions. Of particular note is the adoption of *intranets*. These are privately or commercially owned *networks* of *websites* that are restricted to their own members. Another variation is 'extranets', which are generally understood to mean the same thing but oriented towards non-employees, most often customers, suppliers etc.

2.9 Surfing The Net

The term *surfing* arose because of the convenience of *hyperlinks*, the words, phrases or *graphics* that are '*clickable*' and can transport you to another place like a wave transports a *surfer*. Many people *surf sites* that interest them because most of the *links* on those *sites* are naturally centered around a common theme. It is far more convenient than searching out new *sites* or new information all the time, to simply *click links*, once you are in an area where the main theme covers the subject that interests you.

In the next chapter, we'll be looking at some of the philosophies that gave rise to the developing *Internet* and why there are so many problems to overcome.

Chapter Three

Good And Bad

3.1 The Online World

The *online* world (or worlds really, there are more than one) is made up of code that consists of billions of ones and zeros, so it is essentially an abstract concept. It is this fact that gave rise to the term *virtual* in relation to its place in the 'real' world. Hence it is sometimes known as a *virtual* world and similarly, *digital* products within it are *virtual* products, business organizations are *virtual* companies, individuals have *virtual* identities etc. Each *virtual* world can have more *virtual* worlds within it, even imaginary worlds with imaginary *virtual* inhabitants. In reality of course, each one is a computer *network*, or a part of one.

There are several such *networks* in existence, for example *AOL* is one, but the number is diminishing rapidly due to the tremendous popularity of the all-encompassing and collectively-owned *Internet*.

3.2 The Communication Revolution

The most revolutionary development brought about by the *Internet* is that all forms of communication are now instantaneous. If we look back in the history of mankind, speech evolved first, then drawing and writing. These were followed by technological inventions like printing, then film, the telegraph, telephone, radio and television. There were many other developments that can be said to come under the same umbrella but these are the major milestones on the road of human communications. Now, with *email* and the *WWW*, another huge step forward has been made. At last all these things, and much more, are brought together in a series of interlinked *protocols* that are collectively known as the *Internet*—and can be instantly transmitted anywhere on earth.

3.3 The Information Superhighway

This concept was popularized in the early 1990s by Al Gore, then Vice President of the U.S.A., to describe (what became) the *Internet*. Even though most people had never heard of it at the time, the term quickly caught on as a vision of the future. Now that it has come into being, it's surprising how many people have forgotten the significance of the term. It recognizes that most people who *surf* or search the *net* do so to **find information**. Anyone who ignores this point, particularly if they have something to sell, does themselves a disservice. Wise *webmasters* ensure that they always offer valuable information to their visitors, above all else.

3.4 New Opportunities

The number of people accessing the new world of the *Internet* regularly is now absolutely mind-boggling—tens of millions a day. The potential number of new markets opening up as a result is also staggering. Every conceivable facet of life is covered and, with few exceptions, national boundaries count for very little. And it is still expanding at an unprecedented rate. There truly has never been a phenomenon like it before in the entire history of mankind. Opportunity is knocking for thousands of entrepreneurs around the world and very, very loudly. But it is still a communications and information hub—**not a bazaar!**

3.5 Web 2.0

There are always people speculating about the next 'big thing' in information and communication technology and this has led to the adoption of the catchphrase 'Web 2.0'. There is no such thing really. However, the term has come into general acceptance as meaning the new 'interactiveness' of the *Internet* as illustrated by the growth of 'user generated content' such as video and the phenomenal growth of 'social networking' *sites* such as MySpace and Squidoo. Look in Appendix III for more information about social networking and video sites.

3.6 Plug-In Security

Apart from its two main features (communication and information), everything else that can be done on the *Internet* is done by means of a plug-in; a script or program for which the *Internet* was not originally designed. That is not to say that they don't work. Most such plug-ins (e.g. money transfer scripts, password protected *sites*, etc.) work just fine, but if you want to understand the *Internet* properly you have to concede that they are afterthoughts and therein lie problems, particularly in regard to security.

3.7 The Bad News

Unfortunately, there are some very large potholes on this 'road' and no traffic police or road rules. The *online* world has come to be known as *cyberspace*, as if it's a sort of parallel universe. In a way it is, but it's a universe without law enforcement most of the time, or even any laws of any kind a lot of the time. As a result, there are more crooks and con-men *online* than have ever previously gathered in one place. In fact, so many scams and rip-offs operate completely openly that the Wild West would be a poor comparison. Aside from the guns, it was tame next to the *Internet*.

Couple the two things together (i.e. the lawlessness and the security weaknesses) and you have what the timid might call a potential disaster. No wonder there are so many rip-offs and so much deceit—the crooks have taken over!

“Why is this?”, you might wonder. Well for a start, all laws operate within the jurisdiction of individual nation-states. What is law in one country is not necessarily law in another. More pertinent is that some countries don't have the means to enforce their own laws, or corruption is so rampant that they don't even try. This wouldn't matter except that the *Internet* doesn't recognize geographic boundaries, so anything that can be done **somewhere** can instantly be made available **everywhere**. Another factor is that, with the right *software*, it is possible to almost completely eradicate any tracks on the *Internet* that would expose someone's identity. In other words, it is really easy to hide, if you know how, and continue with your illicit activities. There is also the little matter of encryption. It is now possible to scramble any data, whatever it may be, so that it's impossible to view without a secret key. Lastly, there's the speed (or rather, the lack of it) at which the law operates. Even in the most sophisticated societies, justice crawls along and no-one has yet worked out how to make it effective in an *Internet* environment where everything is instantaneous.

3.8 The Good News

The good news is that human nature is many-faceted and good does tend to prevail over evil, at least in the long term. In the meantime you need to know how to protect yourself, your family and your business. Knowing your enemy is half the battle. In the next Chapter you'll see what you're up against.

Chapter Four

A New Underworld

4.1 You Are Being Watched

The average person, and that probably includes you, doesn't have a clue how the bad guys operate, how pervasive they are, or how hard it can be to catch them. Criminals, many of them very sophisticated but at the same time very bad guys who would strip you bare without a second thought, already have you in their sights and are just waiting for the opportunity to strike. You can't possibly defend yourself unless you know what it is you're defending yourself against. At least now, you are reading this little book and will soon come to realize why it's vital to be aware of the dangers and what to do about them.

4.2 Criminal Behavior

First of all, let me stress that any and every scam that ever successfully operated in the 'real' world, is being operated right now on the *Internet* (assuming it's transferable to the medium). How do I know that? Just because it's obvious. Why wouldn't it be? If the crooks made easy money from it in an environment where, if they were caught they would be convicted and jailed, do you seriously think that it isn't being done now when they know they're highly unlikely to be caught and, even if they were, practically nothing could be done about it? That wouldn't make sense.

There are also many brand-new rip-offs, a lot of of which are possible for the first time because of the advancement of technology. *Diallers* are a good example, though there are many variations and many other equally effective but vicious schemes. A *dialler* is a program that can automatically call a phone number using your phone line and one is usually installed with your *OS*. It's a great thing in that it also allows you to send faxes as well. However, if it's a *malware dialler*, it can be used to call an overseas pay call number without you even knowing about it. You can imagine what the international rate might be for such a call, but when you get the bill, which invariably includes a cost-per-minute charge, you find you are facing a bill of hundreds or even thousands of dollars (and often it will purport to be for a 'phone sex service' or something equally embarrassing). What's worse, you didn't even know about it—but try telling the phone company that.

That kind of theft, however distasteful, is nevertheless easy to understand. Some people however just want to hurt you, even though they don't know you and will never meet you. Don't ask me to explain their behavior. There's probably a word for it, somewhere in the annals of advanced psychiatry. The important point is that **they're out there**. They use *bots* or *spiders* to look for any and all computers connected to the *Internet*, test them, and when they find security holes, target them for attack. They really don't care if your livelihood is involved, or your medical records, or those irreplaceable photographs, or even your child's innocence. **Every** computer is vulnerable and, unless adequate defenses are set up, **will be attacked** eventually.

4.3 Malicious Software

Since all *malware* has to gain access to your computer somehow, just how do they do it? Well believe it or not, they usually get you to do it! They might con you into opening an infected *email* attachment, reading an infected *HTML email*, or persuade you to visit a *site* that looks normal but is actually loaded with *malware*. In the case of the latter, they might invite you to unwittingly *download* an infected *file* or *files* or even just view an infected *graphic*. Not surprisingly,

porn *sites* are a favorite vehicle for tricking the unwary. The pornography is just a way of disguising the real purpose, which is to infect your computer. But remember, it might be about almost anything—so long as it can be used to trick you. For example, it is not uncommon for crooks to *spoof* a legitimate and fairly well-known *site*. There are a number of other ways they can infect your computer by using a *website* and, if all else fails, they can trick your computer into allowing them to access it directly without your knowledge.

4.4 Viruses, Trojans, Worms, Rootkits And Backdoors

Attacks are commonly made nowadays using various forms of *malware* transmitted over the *Internet*. Just so you know the difference between them, a *virus* is a piece of computer code that infects legitimate applications or other programs on your computer and, when activated (innocently) by you, spreads to other executable *software* on your computer. More often than not, they contain within them malicious code that performs other unwanted actions, like deleting vital *files*. A *worm*, on the other hand, is a program which actively transmits itself (without your involvement) over a *network* and infects other computers on it. Similarly, it too often contains malicious code. A *trojan* (horse) is a program disguised to look innocent, even useful, but always conceals within itself a malicious or unwanted payload. It too can lead to a number of very undesirable results, including the installation of harmful *software* on your system such as *diallers* (mentioned above).

Rootkits are programs, or combinations of programs, designed to take control of your computer without your authorization, or even knowledge. They obscure their presence on your system by evading normal security mechanisms. Often, they are *trojans* too, thus fooling you into believing they are safe to run. They work on most operating systems, including Microsoft, Mac, Linux and Solaris. *Rootkits* often modify parts of the *OS* or install themselves as *drivers* or kernel modules, depending on the internal details of your *OS*'s mechanism. Because they can be so difficult to detect, they are gaining increasing popularity among privacy invaders and other malicious intruders. *Backdoors* are security 'holes' in your system deliberately set up for the purpose of bypassing normal authentication, thereby allowing remote access to your computer. They often take the form of an installed program or a modification to an existing program or hardware device.

4.5 Space Invaders

We're talking here of **your space** or space on your computer. *Adware* is an example. Once these programs are installed you are at their mercy if, for example, they decide to bombard you with *popup* ads. Not only that but they use up your bandwidth and slow down your *browsing* activities. Sometimes you might allow *adware* to be installed on your computer, such as when it is part of a free program that you find useful and it's included as a condition of use. This is common practice. Even some of these can be a problem though, such as when you decide you no longer need the program so you uninstall it, only to find that the *adware* component won't go away.

The really intrusive ones though, are typically installed by *trojans*. Not only do they show unwanted ads when you least expect them, but they sometimes work in conjunction with another privacy invader: *spyware*. I'm sure I don't need to explain what *spyware* does. When *adware* works in tandem with *spyware*, it produces so-called 'contextual advertising', which really means "because we know what you're reading, we're going to show you ads that match, whether you like it or not". Do you really think this is "informative and useful" as the program owners say in their sales pitches? Of course it isn't. It's a conspiracy based on profit between the advertisers and the *adware* owner.

Some really vicious uses of *spyware* are also all too common. Any data on your computer can be stolen, and certainly will be eventually, unless you take steps to prevent it. Credit card details, passport numbers, passwords... all are vulnerable to theft. Not only that but *keyloggers* mean the information doesn't even have to be stored on your computer. It can be stolen just because you typed it. Some kinds of *spyware* log everything you view, whether it's *files* on your computer or pages on the *net*, and once they know where your interests lie they can use *adware* to advertise things related to those interests. It doesn't take much imagination to see how this information might be used by the totally unscrupulous. How comfortable do you feel knowing that someone with an ulterior motive might be viewing your every

move?

4.6 Cookies

Personally, I don't count 'cookies' as privacy violators. These are very small text *files* that are lodged on your computer by *websites* you visit, to identify you when you return to those *sites*. A text *file* is completely harmless and can only carry the information on it that the *site* from which it originated put there, usually just your name and the *URL* of your *site*. You can read them if you wish, or delete them, or disallow them altogether. Some *websites*, such as many membership *sites*, insist on them so only you can make the decision as to whether to allow them or not. Having said that, I understand there is now special *software* that can track what *sites* you've visited by reading your cookies, but most anti-*virus* programs can easily get rid of these. As I say, they are relatively innocuous but still, you may decide it is unacceptable that someone else should assume the right to intrude on your computer. (There is a link in Appendix III leading to advice on how to configure cookies.)

4.7 Offensive Behavior

One of the first things that *newbies* are often taken aback by on the *Internet* is how nasty some people can be. It doesn't take long before, in an *online forum* or an *Internet chat room*, they find themselves subjected to a stream of venom and rudeness for misunderstanding the rules or asking a simple question. It's called *flaming* and is accepted as normal behavior by many. It has come about due to the anonymity that the *Internet* provides. The perpetrators know that, because they operate behind a *handle* and nobody really knows who they are, they are free to say whatever they like and display their obviously warped personalities to the world. This behavior can be quite shocking to some, especially children, who should be forewarned.

4.8 The Dark Side

Unfortunately though, it gets worse. The sad truth is that, just as there is every kind of criminal activity on the *net*, so too is there every kind of deviant or anti-social behavior and manifestation of mental shortcomings.

Everyone knows about child pornography, for example, because it has received such heavy press due to the media's obsession with the sensational. The reality is that just about every sexual taste (or deviance, if you prefer) is catered for and is, of course, thriving on the *Internet*.

Equally disturbing, to some at least, are the many other deviations from what were once accepted norms. A good example are hate *sites*, which provide a platform for the paranoid to display their intolerance towards anybody with a different viewpoint. Racial and religious hate are just two of the many 'tunnel vision' hatred *sites* that seem to be growing in numbers and membership. And with the arrival of *Web 2.0*, pictures and movies depicting real-life *graphic* violence have proliferated incredibly.

4.9 The Poison Of Spam

UCE or *UBE* is electronic mail sent out in bulk by people who are quite happy to abuse the *email* system in the hope that by sending out huge numbers of *emails* they will find at least **someone** silly enough to buy their worthless products. The word *spam* has the same meaning but is broader and encompasses all types of unwanted or illicit messages, including those that can be found in *forums*, *blogs*, *newsgroups* and so on.

Not all *spammers* do it to sell things. Everyone knows perfectly well that the vast majority of people despise *email spam* so some *spammers* actually use it as a form of revenge or intimidation. This is called mail bombing. There are even *spammers* who do it simply to annoy people. These are called 'the mentally challenged'.

Some of the most destructive aspects of *spam* are:

1. It brings into question the future value of *email*.
 2. It can be incredibly time-wasting as it forces recipients to take evasive action.
 3. It is very costly for ISPs and in the end it is all users who pay.
 4. It voraciously consumes bandwidth that is in short supply.
 5. One consequence of it is the taking over of thousands of private computers as *zombies*.
 6. It makes the sending and receiving of *ezines* a problem.
-
-

Chapter Five

Primary Defenses

5.1 Downloading Files

Now that you know what might happen, no... make that **will happen**, if you don't adequately protect yourself, you probably want to know exactly what it is that you can do. The good news is that it's not that hard. Having said that though, the sad fact is that only a very small proportion of *Internet* users do everything listed in this chapter. At least you'll know by now how necessary these primary defenses are.

The first thing I would advise is never ever *download* any *file* if you are in the least unsure what it is. The commonest method used to invade your space is to invite you to *download* a *file* on the basis that it is useful or necessary, or to simply pop up a *download* dialog saying “you have requested the following *file* for *download*. Press OK to continue”, or something similar. Just say NO! Unless you are certain it is legitimate and that it is going to benefit you and you trust the *site*, **leave well alone**. This is potentially the most dangerous thing you can do and that is why it's so common. *Files* can be any size and carry any number of evils.

5.2 Email Attachments

Never open an *email* attachment unless there is something in the body of the message telling you to expect it, **and** you trust the sender. Likewise, tell everyone you correspond with that you won't open attachments unless they mention them in the text of their message. This is because *viruses* etc are often transmitted as *email* attachments from infected computers and **the senders don't even know they are infected**.

5.3 HTML Emails

Unless you have a particular reason for wanting to view your messages in *HTML*, always opt for text format instead. That way you'll never get an *email virus* infection just from reading your *email* since it's impossible to transmit them via plain text (*ASCII*). Also, never get in the habit of handing out your *email* address to all and sundry. If you do, it will eventually result in a deluge of *spam*. If you want to include it on a *website*, either disguise it, or use a *software* program to hide it for you. *Email* addresses on *websites* are notoriously easy to harvest using special *software* called mailbots and, once it gets on a *spam* list, it can make your life a misery.

5.4 Mind Your Own

Never give out personal information in an *email*, *forum*, *chat room* etc. Your social security number, passwords, credit card numbers etc should remain strictly private. Obviously, this doesn't apply if you are **absolutely certain** you are on a trusted *site*, particularly if it is secure (i.e. one that starts with *https*) but otherwise I would say don't even make your phone number or address known. And never use a password that anybody might be able to guess, such as your birthday, kid's names, and the like.

5.5 Choose Your Software

Use Thunderbird rather than Outlook or Outlook Express. I'm not implying that Microsoft products are inferior or more prone to security holes but they are **more prone to attack** because Microsoft has captured the *email* application market, which means they have many more users. The same applies to *browsers*; use FireFox rather than *Internet Explorer*. Both of these are free, both are excellent programs and more information on them is provided in Appendix II.

5.6 Check Your Preferences

Look carefully at your *email* client and *browser's* security and similar settings (go to the 'Tools' menu, then Options or Preferences). Make sure that browsing and *email* have the highest security settings your normal *Internet* usage will allow. If you're a *newbie*, the default settings should be fine, but don't tamper with them unless you're sure you know what you're doing and why. All security settings are a compromise in that, to be completely and utterly safe, you would need to have every setting as high as it would go. Unfortunately that would mean you wouldn't be able to access the *WWW* or send or receive *email*! You need to apply common sense, like not allowing risky settings (such as *ActiveX*) to be turned on to 'automatic' when you could use the option to have the *software* seek your approval first. (See also Appendix III.)

5.7 Temporary Internet Files

You need to apply caution with *temporary Internet files* too. These are copies of all the *files* you've viewed on different *sites* you've visited and are held in a special type of folder known as a *cache*. The idea originally was that it would speed up your browsing if your computer kept these *files* for you, in case you wanted to return. Caution is suggested because they are now a record of everything you've done *online*. If you are on a *broadband* connection or a shared computer, and use *Internet Explorer*, you might want to clear your *Temporary Internet Files* folder after every session. Most *browsers* have an 'automatic' setting to allow you to do this but please understand that all *browsers* have their own *cache* folder and don't necessarily use the Windows *Temporary Internet Files* folder. Firefox, for example, talks of your 'private data' and you'll find all the settings related to it under Tools; Options; Privacy.

5.8 Built-in Firewalls

It depends on the age of your *OS* whether it has a built-in *firewall* or not. If it is Windows XP or later, make sure that the *firewall* component is **turned on**. If you get an error message that says your *firewall* is not operating, don't just shrug it off. **That's serious!** Built-in *firewalls* are usually pretty basic at the best of times so make sure that it's turned on, at least, and working.

Windows Vista also has an application called Microsoft Defender built into it, which is designed to prevent, remove and quarantine *malware*. It can be *downloaded* for free and installed on Windows XP too, which is what I recommend. Details are in Appendix II.

5.9 Downloadable Defenses

If your *OS* does not have a *firewall*, you need to acquire one as soon as possible. This is **very important** as it is your best defense against surreptitious intrusion. There are a lot of excellent choices available, including free ones as well as those for sale. More details appear in Appendix II.

Another vitally important protection is an adequate anti-*virus* program. Most of these will actually neutralize other forms

of *malware* as well, including *trojans*, which are responsible for hiding many types of potentially damaging *software*. There are one or two excellent free ones available as well as some highly respected commercial ones for sale. There is more on these in Appendix II.

If your anti-*virus* program doesn't provide comprehensive protection against *malware* such as *spyware*, *rootkits*, intrusive *adware*, *backdoors* and other types of malicious *software*, you will need to look for something that does. More help is in Appendix II. Whilst there, you may want to consider some anti-*spam software* as well.

You may want to install some 'parental control' filtering *software* or, less euphemistically, *ensorware* if you have children to protect (or who may need protecting against themselves). Also, insist on your right to monitor their *online* activities. If they think you are going to be thorough in tracking what they do, they're less likely to get themselves into trouble. And remember, girls nowadays are every bit as likely to try to access the sort of *sites* you don't want them to see, as boys. Look in Appendix II for some ideas.

Lastly, always remember to regularly *download* all security patches to your computer as soon as they come out, whether your system is Windows, Linux, or whatever. Daily updates of your anti-*virus* programs etc are crucial too. In fact, automate the process. Most have their own automatic schedulers but, if not, use the one built in to Windows or, if necessary, install one.

All of these are important, some more than others depending on your circumstances. Most anti-*virus* vendors advise against installing more than one such program, due to the possibility of conflicts, but most of the other types are quite compatible with each other. You need to read the installation documentation that comes with each of your choices. Remember, no one program or system can give you complete protection. You need the whole raft of measures discussed above to be reasonably safe.

In the next chapter we'll be looking at another side of the lawlessness of the *Internet* and what you need to do. As you can see from what has gone before, you have to know your enemy if you want to beat him.

Chapter Six

A New Gold Rush

6.1 The Fortune Seekers

The Klondike gold rush, like all the gold fever phenomena that preceded it, made fortunes for some but broke the hearts and shattered the dreams of many others. Now, the new Klondike is doing the same. Sure, there are dozens of *Internet* millionaires but for every success there are hundreds, perhaps thousands, that fall by the wayside hurt and disillusioned. Sometimes they are undone simply by their own incompetence, sometimes it is caused by bad personal habits such as procrastination, often it is a result of their inability to delegate or just trying to take on too much for any one individual. Probably the commonest cause of failure is plain inexperience.

However, these are all personal problems that can be overcome with more experience or the right kind of training.

6.2 Trickery, Lies And Deception

What is far worse is when the budding *online* entrepreneur or *Internet* user is subjected to trickery, lies, and deception. Fancy *websites*, dazzling *graphics*, soothing words and promises of great things to come are all used with abandon to entice them to buy or sign up. Of course, all *Internet* marketers apply 'power' words and phrases and various other gimmicks to put prospects into a 'buying' mood. This is no different to the real world. The unscrupulous though, use every trick known to man to sell worthless stuff or hype up mediocre products to the point where they become irresistible. They are often better at it than many legitimate marketers. And it's not only words that they manipulate; they know which colors soothe the anxious, which *graphics* are best for which products, when to use music, and so on.

What the unwary and inexperienced have to realize is that there are many rogues *online* selling what amount to garbage products for \$35, \$49, \$75 and often very much more, using high quality professional copy and successfully managing to repeat the process over and over again—sometimes for years. Or products that are simply not worth anything like the price they are asking but which they need to sell at that inflated price to cover the cost of the sales copy that they have paid for and huge commissions for their *affiliates*. A number of these people are looked upon, or tout themselves as, *IM gurus* and they know exactly how to trap inexperienced *newbies* into putting their energies into promoting these same products.

Many of these inexperienced *newbies* are good people who allowed themselves to get caught up in the hype. They find themselves promoting things that they know to be worthless but, once they've paid their money or invested their time, feel compelled to continue their efforts, including the use of sales copy that they know is full of lies.

6.3 Applying Caution

So how do you know when you're being had, whether it's as a potential buyer or as a potential *affiliate*? How can you recognize a dishonest or exaggerated pitch for what it is and give it a wide berth? The answer is... **you can't!** Not always. Nobody can ever be quite sure. It takes vigilance, a lot of common sense and, to a large extent, the wisdom that comes from experience. But you can, of course, acquire that same wisdom by **learning from** the experienced, which is one of the reasons for *ITRAPS*. But there are two well known sayings that always help and that you should never forget.

They are:

1. If it sounds too good to be true... **then it probably is.**
2. Let the **buyer beware!**

6.4 Get Rich Quick

There are some scams that can be recognized immediately, of course. They are so obvious because they just don't add up. In this category I would put HYIPs (High Yield Investment Programs), doublers etc. I would go so far as to suggest that any program that raises a question mark in your mind about where the money comes from should be avoided. It's a well-known fact that all successful sales pitches appeal to the emotions, such as the need to be liked, the need for security etc. The trouble with these types of schemes is that they sell based on one of the strongest emotions of all: **greed**. And only on greed. It's instinctive, and the emotional appeal is so strong, that your mind wants to believe it, and all common sense goes out the window.

The same applies to any so-called program that suggests that, in return for doing very little, or even nothing at all, they promise to pay you such enormous sums of money that in a month, or three, or six, you will be able to retire in great comfort. Come on! I'm tempted to say that if you believe that, you'll believe anything. But thousands fall for the same pitch again and again. **I'm no fool but I have too!** The actual time they state before you reach your El Dorado is based entirely on what **they** think would be **almost believable** to you. The amount they want you to 'invest' is what they hope **you'll be willing to risk**, just to test it in case it's true. They spend large sums of money testing these figures until they know they've got them just right.

You really need to remember the most **fundamental rule of commerce**. You can't possibly make money from nothing! One gives, and in return, one receives. In other words, someone has to **sell something** and someone has to **buy it**. That is the only basis on which money changes hands in the realm of business. Whether it's a physical product, a *virtual* product or a service of some kind, something has to be sold and that something has to be bought. If you can't figure where you are supposed to fit in this exchange process when considering some new program, **leave well alone**.

6.5 Dreams For Sale

All the scams mentioned above come in many different disguises. Instead of concentrating just on your dreams of striking it rich they may appeal to your business needs, for example by undertaking to help you with prospecting, for a fee of course. The most common of these types is the 'leads for sale' scam but there are many variations that have nothing to do with leads. Every *Internet* marketer needs leads (remember, substitute any product that is in demand), i.e. potential buyers for their products, usually in the form of *email* addresses that can be added to their *mailing list*. The trouble is there's no way of telling where they've come from (apart from the vendor's sales pitch). Targeted leads are the most sought after; in other words, when they represent people who are actually in the market for whatever the product is that you're selling. That, of course, is most often what they say they are. But, emotion aside, how can that be? And why are you so disappointed when none of them buy?

What's worse is when the vendor tells you that his leads will automatically sign up for your program or buy your product and he guarantees it! Even if they do sign up to your free program (they won't buy or sign up if there's a charge) you will very soon find out that they will do nothing further. This is an example of an actual product being sold but, the trick is, nothing is delivered.

6.6 Scams Galore

So what others do you need to look out for? Well, quite frankly, there are just way too many to mention by name.

Randomizers, chain letters, ponzi schemes... the list could go on and on. The actual names they use for individual scams are not worth listing either—they change all the time. There are some *websites* that purport to list all the scams currently in vogue but I deliberately don't list these either, at least for now. The reason is that, like most anti-*spam sites*, it seems that they only need to receive one or two complaints before they consider that as sufficient evidence to list a *site* as suspect. This is unfair. Who are the complainants? What is their motivation? Are they really competitors? If, in truth, they are naming a *site* because they just suspect an 'opportunity' is a scam (most seem to fit this category), is this a good enough reason to blacklist them? I would say no, but if I come across a *site* that seems to give more balanced appraisals, I may change my mind.

There are many, many *email* scams too. However, if you treat *spam* with the contempt it deserves, you'll bypass ninety nine per cent of them. But never forget, it is not the obvious ones that you need to watch out for. After all, you don't need to be very bright to realize that the notion of a pill or a wearable patch that enhances a specific body part, has a strong whiff of scam about it (quite apart from raising the question “why would I want to do it?”). My main purpose in this little booklet is to try and encourage you to remove your emotions, as much as possible, from your deliberations when considering spending your hard-earned cash *online*. Look at the evidence. Do they give you sufficient **information** to make a sensible judgment? If they do, does it make sense? If not, or if they don't give sufficient information, give them a miss. Don't just give them a miss because at first glance it looks like a pyramid plan or whatever. Remember, even the scammers need to have a ring of truth about them so, by the same token, genuine opportunities might, on the surface, look as if they're not quite right. Study them with an open mind and a clear eye before making a final judgment.

Chapter Seven

Cautionary Tales

7.1 Buyer Beware

To make things easier for those who need something a bit more concrete to go on, here are a few of the things to look out for. By saying 'beware', I am not implying that all *Internet* marketers are guilty of deception, or even that any particular one is likely to be guilty of anything inferred here. What I am suggesting is that it's naive to think that, just because it appears in print or on a *website* (or anywhere else), it must be true. The experienced will read everything with a healthy degree of skepticism. The following cautions are based on my experience, so I am sure there are others that I have so far not been faced with or have forgotten.

7.2 Beware Of Gurus

Reputations are usually hard-earned but they can also be invented. Just because someone touts himself as one of the *big dogs* doesn't automatically make it true. One of the biggest earners on the *Internet* today gained his marketing lead and built up his *mailing list* largely from *spamming*, starting early on (when admittedly, it wasn't quite so frowned upon). Although he now says he doesn't believe in it any more, he stuck firmly to his guns until just very recently. Now he's looked upon as one of the *Internet's* great success stories. I'm not for a moment doubting his expertise or casting aspersions on his marketing advice or *guru* status, but I'm sure you'll understand my point.

7.3 Beware Of Recommendations

A much more honest word for these, more often than not, would be 'referrals'. In other words the recommendations you get, even from well-respected *gurus*, are very often prompted by the large commissions they can look forward to. A majority of the best-known *gurus* on the *web* are on each other's 'A' list for *pre-launches* and the mad scramble that follows them is a sight to behold. *Gurus* love the big fat commission checks that are sourced from **your** bank account and that of the other believers on their lists. Do you think they all try out these programs and give an honest assessment based on worth? Think again.

7.4 Beware Of Testimonials

Never believe without question what can so easily be faked. There have been so many revelations of scams involving fake testimonials that it's really surprising that so much of it still goes on. But it does! No names, no pack drill, but there was another one just recently that involved an extremely well-known *Internet* marketer that I myself have bought from and who is a recognized top *guru*. I'm not saying it's particularly common among the big names, but it is common.

7.5 Beware Of 'Facsimilies'

This is very similar to the fake testimonial situation. Don't be taken in by one of the favorite tricks of all time. Like fake testimonials, it was popular way back in the days before the *Internet* was ever heard of and is every bit as popular now as then—but so much easier. Anyone can produce a fake copy of a PayPal account activity page, ClickBank revenue

page, bank statement etc. With modern *graphics* programs it's just so simple. Taking this into account, plus the fact that it's so rife, I just take no notice whatever of these pages when I come across one, no matter who's posting it. Am I saying that they're all forgeries then? No, of course not, but I take a lot more convincing than the use of these imply—and so should you!

7.6 Beware Of Guarantees

Proclaiming a no-questions-asked money-back guarantee (or any other) is no guarantee at all. Your best bet is to find out what the payment processor's policy on refunds is before even reading the so-called guarantee. Always read the small print part too. Just as in the real world, these often contain carefully worded clauses that mean, in essence, that they themselves (in other words, the vendors) are not liable in any way.

7.7 Beware Of Secrets

There are precious few genuine secrets left and certainly no new marketing ones. To be fair, I am constantly learning about advances in the world of technology that open up new ways and methods of doing things but I'm very doubtful that these can honestly be described as 'secrets'.

7.8 Beware Of The 'Easy' Tag

Making money, more than anything else, is never easy. It's hard work. The trouble is that all vendors want you to believe that what they're offering is “so easy a chimpanzee can do it”. (And yes, I've put this in quotation marks because I actually read this very statement just a few days ago!).

7.9 Beware Of The 'Buy Now' Tag

Known to marketers as the 'call to action', the penalty for not acting is rarely applied. This is no biggie and it's not necessarily a scam. I'm just saying don't get taken in because it's been made to look as if you've just arrived in the nick of time. If there's a 'countdown' meter on the page, you can usually safely ignore it. As often as not it will start again at the same place if you return to the page later.

7.10 Beware Of Pre-Launches

So-called *pre-launches* are a total non-event for ordinary people. You will see them mentioned as if you are being allowed a special privilege. The truth is that these special offers (made **prior** to many new *bizopp* launches) are only for *big dogs*, in other words *gurus* and other marketers with huge *mailing lists* made up of people who regularly buy from them. They are not for mere mortals like you and I. A lot of new launches are not expected to have a very long life before they are eclipsed by the next 'big thing'. One of the reasons for *pre-launches* is that the program owners try their very hardest to totally saturate the market before the thing is officially released. They are invariably ridiculously inflated in value and once their objective has met with success, they expect only crumbs to trickle in from all the other minor players after the so-called *pre-launch*. Unethical? Of course it is, but that's just the way it is. You don't really expect ethics in this environment, do you?

7.11 Beware Of Guaranteed Sign-Ups

Nobody can guarantee worthwhile sign-ups to something the 'signers' themselves know nothing about. How could they? Especially where money is involved. The vast majority of these sort of schemes will produce absolutely nothing of any

value at all. But you might waste a lot of time and energy *emailing* and posting on their site's support form before you realize that it's time you gave up and waved your 'investment' goodbye! There are some cases where it's even superficially true; where they actually systematically collect the genuine *email* addresses of people in some poverty-stricken nation in return for a pittance, or even pay them to join what they tell them to. But, come on! What are they worth? Not so much as a dime.

7.12 Beware Of Long Downlines

If you recruit A, and he recruits B etc... somewhere down the line it will all fizzle out. *Downlines* of any sort tend to be frowned upon now but any ridiculously long ones (over fifteen levels or so) are sold on the basis that the seller knows that hardly anyone will be left by the time level 10 is reached. It just sounds good. There are many reasons for this and I am only talking about plans where the participants actually pay to join. I have several *downlines* in free-to-join programs exceeding ten levels. But for programs that require a fee to join, don't expect it to last if part of the remuneration depends on a long *downline*.

7.13 Beware Of High Payout Targets

Need to aggregate total sales to \$50 or \$100 before they'll pay you? Forget it. Of course, it really depends on the program concerned what the actual figures are but you need to try working it out on the basis of expected income figures. If, for example, a program only pays a fraction of a cent for, say, opening and reading *email* ads (a favorite for some) but the amount you have to accumulate before payout is in the area of fifty or sixty dollars, I can tell you now that nearly everyone involved is working for nothing. Most people drop out before they even get near the payout figure. And the companies running these scams know it.

7.14 Beware Of Graphics

Big house, big car, guy on a hammock with a cocktail in his hand, under a palm tree by the beach with a gorgeous bikini-clad girl just coming out of the surf... the ultimate appeal to your emotions. But you don't fall for these do you? **Of course you do!** The appeal is to your subconscious and they always work, unless you train yourself to see the humor and laugh at them. It's a form of subliminal advertising and it works on all of us. As I say, don't just ignore them, remember what they are really trying to do and laugh at them because then at least you have the satisfaction of knowing that the joke is on the advertiser.

7.15 Beware Of Automatic Payments

Small recurring payments (or, even worse, large ones?) can be a big problem for the inexperienced. Why? Two reasons: you forget what they're for but the amount is so trivial you never get around to canceling them. Or, you forget what they're for and you have a really hard time trying to find out who they're going to. Either way they can bleed you of hundreds before you know it. I'm really joking when I say it might apply to large amounts too (though it can sometimes). Most often though, they're small by design. The vendor that got you to sign up used a recipient name or product code that is totally unrelated to his business in the hope that you'll forget and possibly not even notice and, as a result, not know where to go on the *net* to cancel. The ambiguous name is only part of the problem. Most credit cards companies won't stop paying until you come up with firm evidence that you've tried every other avenue first. It might be your money but it's not always you that has total control.

Chapter Eight

Opportunities For All?

8.1 Working From Home

If you're new to the *Internet*, you won't get far into this new experience before you realize that every other *site* you visit is touting a way to make money. If you're an experienced user though, you might be used to this and maybe have even tried a few such programs, only to end up disappointed. That doesn't mean that there are no genuine *bizopps*; you just need to know **what to look for**. As I tried to point out in the last couple of chapters, you will be disappointed unless you adopt a mindset that will allow you to look at all opportunities with a clear eye and avoid the scams.

8.2 The Method

The types of opportunity that exist on the *Internet* are many and varied and the earning methods depend on your circumstances. However, if you're looking for a way to turn your life around, at least in the long term, the first thing you have to accept is that **sales and marketing** is where the money is. This is no different to the 'real' world. The highest paid people in all fields of commerce and industry are those who know how to close a deal or plan a marketing strategy. And so it has always been. That then, defines what this and the following chapters are about.

If you have a product that you already own (by 'product' I mean anything of value for which there is a market, including a service) and your ownership includes sole Resale Rights, then your marketing plan would reflect that. Chances are that your main efforts in that case would be directed towards recruiting, training, supporting and servicing a sales team.

However, most people do not have a product of their own, or possibly even a *website*, so the choice would be between creating their own product (too hard), acquiring the sales rights to one (too costly), or becoming a sales agent and getting paid a percentage of the sale. For obvious reasons, the latter is by far the most popular choice and the one for which there are the most ready-made opportunities. That is what we shall be concentrating on here.

It is referred to in *IM* as '*affiliate* marketing', which simply means operating as a marketing and sales agent for the principal product owner (the sole owner of the Resale Rights). The commissions payable are usually much higher than they would be in the 'real' world. Most pay over fifty per cent, whereas comparable products *offline* would only pay up to a maximum of twenty five per cent. As in the real world, the principal product owner usually provides sales material and looks after dispatch, support etc. All the *affiliate* has to do is market it.

8.3 The Marketing Mix

What often doesn't seem to be generally understood is that marketing is **much more than just a sales process**. It is all those factors that are brought into play to **maximize the chances of a sale**. This is a very important point that should also be taken seriously by anyone considering becoming an *affiliate*, though you will hardly ever hear it mentioned in the *IM* arena. As an *affiliate*, you are unlikely to have any say about the individual factors that make up the marketing approach but, if you know what to look for, you can take them into account when choosing a suitable opportunity.

There are four main elements, known as the 'Four Ps' of marketing, to consider. This is a well-known formula for remembering what makes up the 'marketing mix'. Choosing the right product, ensuring that the price is right, and that it

is displayed optimally and made available in the best place, are vital forerunners to the grand finale—promotion and sale of the product. Get any of the first three wrong and any energy spent on promoting goes to waste. The four Ps then, are:

1. **Product:** choosing the right product to market.
2. **Price:** making sure the price is right for a sale.
3. **Place:** getting it to the right place for the buyer.
4. **Promotion:** implementing a campaign to get the word out.

Each of these is vital for marketing success and they are the focus of the next four sub-chapters.

8.4 The Product

Ideally, it should be something for which you already have an affinity. If you're a keen para-sailer, for instance, look at whether there is an established market segment, or in *IM* jargon, a *niche*. That simply means that there are people searching for the *keyword* 'para-sailing' and variations of it, via the search engines. If there isn't such a *niche*, or if it's too tight (not enough searchers), cast your net a little wider. For example, if para-sailing qualifies as an 'extreme sport', that would logically be where you would look next for a suitable opportunity.

Mark Twain once said, "Wealthy (gold) miners are a rarity—but those that sell them the shovels always make their fortunes". Truer words were never spoken. Don't dig for gold; **sell the tools!** In other words, regardless of the focus of any particular *niche*, the most reliable way to make money is to sell the tools that will help them achieve their objectives. It's called fulfilling a need and is one of the fundamental requirements for commercial success. Choose the tool you want to market carefully enough and you'll find it that much easier to market because you'll be **making money by helping other people**. And *affiliate* marketing particularly well suits this type of operation.

Choose a product of **real value**; in other words, one that **you would buy**. Better still, **buy it**. There is no better way of appreciating its benefits, or learning about its idiosyncrasies, than as an owner. You will find your experience in using it enormously useful too if, for example, you decide to review it (i.e. write an appraisal—the best way of prospecting and pre-selling).

Another thing about the product: **always go digital** (*ebooks, software, etc*) and avoid representing those companies that offer hard goods (physical products) whenever possible.

8.5 The Price

Buying the product you want to market also raises the question of price, which is a good thing because it **forces** you to think like a buyer in terms of value over cost. A perception of **high value** and **low cost** is what eventually decides the issue for the buyer. The nearer together these two variables seem in the buyer's mind, the less likely they are to buy. Obviously, if the cost actually exceeds the perceived value, it will be very difficult to sell at all. You, as the seller, need to think like the buyer and actually becoming a buyer is the most obvious way to do it. Being both buyer and seller gives everything you say about the product a degree of genuine credibility too, that you simply couldn't acquire any other way.

A very important factor that directly affects the price, when considering products to be sold using the *affiliate* marketing method, is **commission**. This is often a dilemma because, at the same time as trying to make the price attractive to buyers, the owner must try and set the commission high enough to attract *affiliates*. My experience is that most owners give up trying to solve the problem and instead opt for setting the commission as high as possible in order to get as many *affiliates* as possible. This, of course, **forces the price up** but they hope that this will be offset by having more *affiliates*. To put it in simple terms, **higher price equals fewer sales** but more *affiliates* equals more sales. So they end up with lots and lots of *affiliates* promoting their product and the fact that each one makes a mere pittance, or no sales at all (because the product is overpriced), doesn't bother them at all. They (the owners) and a very small pool of *big dogs* still

make a lot of money.

Unfortunately, it's that old appeal to greed again. Big commissions do **not** mean big income. In fact, they usually mean the opposite. You have a far better chance of making a sale if the product is fairly priced. (There is a solution to the dilemma of the commission/price problem but I'll explain more in Chapter Ten.)

8.6 The Place

When you are dealing with a *digital* product, especially when you are promoting it *online*, the *online* world **is the place**. The *virtual* point of sale is the **sales page**. It will often be totally under the control of the principal owner, although sometimes you may find that you do get offered a genuine page of your own. The *virtual* place of delivery is the 'thank-you page', the place the customer is sent to for details of how to *download* the product he or she has just bought. This is all so much more convenient than when dealing with hard goods, plus the fact that the customer gets instant gratification which has the effect also of reducing returns.

You need to **study the sales page closely**. Remember, this is the all important *POS*. All your marketing efforts will lead your prospects here. Is everything explained clearly, or are some things about the product (deliberately?) vague? Does it do a good sales job? In other words, **does it make you want to buy?** If you are open to my earlier suggestion that the ideal thing is for you to buy it, then do so. If it doesn't persuade you, **why not?** Is it too expensive? Remember the points raised in the previous chapter about what to beware of as well. Is it over-hyped? There is a fine line between over-enthusiasm and under-playing a product's benefits but only you can make that judgment here. However, if the sales page does not convince you, **neither will it convince your prospects**. At best it will result in a low conversion rate which means that you will have to work particularly hard to get enough sales. Conversion is simply the percentage of people who buy (calculated on the total number of visitors divided by the number who actually buy). A rate of between 1% and 2% is a rough average for most *online* sales. Any more would normally be looked upon as a good return, any less not so good.

8.7 The Promotion

Your main job as an *affiliate*, for any program or product, is to **promote it**. So, once you've sorted out the first three Ps, you need to work out a prospecting initiative that will allow you to **collect leads** (people you can write to) and/or **produce targeted traffic** (people interested enough in the product to visit the sales page). This is all a matter of advertising and publicity. The end result of these efforts is that you then get credited with any sales that result from those visitors. This is achieved by means of your referrer ID, which is part of the sales page *URL* (if you're not lucky enough to have your **own** sales page), and/or by cookies, which identify you and are picked up from whatever page you use to promote it (a *splash page*, for example).

This sounds simple enough, doesn't it? The principal supplies you with a selection of banners and a couple of *email* sales letters. Possibly, but rarely, a *splash page*. Then off you go, full of enthusiasm, with dreams of all the commissions you are going to collect. Duh?! Where do you go from here? Most new *affiliates* don't have a clue. They are often not even pointed in the right direction. It's scandalous how many principals are very energetic at recruiting *affiliates*, only to let them down so badly when it comes to supporting them. Look for a program that offers **marketing support** if you're inexperienced.

8.8 Getting Past The Hype

You need to see past the hype when you look at *affiliate* offers, especially the marketing support and guidance they give you. In my experience, most new *affiliates* need help finding **free and low-cost advertising** and with building and *emailing* their *mailing list*. Most principals however, only offer yet another cost in the form of a program or package of 'can't-do-without' goods for sale. It may come in the shape of an *OTO*, or by subscribing to a 'Pro' version, or any of a

dozen other ways. This is called 'back-end selling' and is just another way of screwing more money out of you. There's another well-known name for it, of course: **hidden extras**.

In order to be able to promote a product or program efficiently and generate enough sales to make a good income, look for one that has a marketing program that **really works**, that has a full and open explanation of **how it works**, one where **no experience is required** (if you are inexperienced), that's **easy to understand**, that's **free of hidden extras** and that offers free and valuable **marketing advice** that can also be used for any other program you may be involved in.

Chapter Nine

The Holy Grail

9.1 Finding A Genuine Bizopp

Taking all the above into account, are there **any** genuine business opportunities *online*? The answer is yes, of course, but to be on the safe side you need to take special care. You need to dissect the sales page and the *affiliate* offer before you jump in, or you risk drowning.

OK then, how do you recognize that holy grail of *Internet* marketing, the perfect opportunity? Well, that's a different story, assuming that there is such a thing, of course. I would suggest that there isn't one, for several reasons. First, everybody is different and the best business for one isn't the best for another. Second, despite searching, I have never yet come across one that fulfills **all** the requirements that I would say would make it ideal for the average person. (Having said that though, **I have a surprise for you in Chapter Ten**. Don't go there yet though; you need to understand some other important things first.) The emphasis in this chapter is what to look for in order to get as close as possible to that ideal when considering any *online bizopp*.

9.2 Hidden Income

Instead of hidden extras, what you really need is hidden income; in other words, **extra methods of earning** over and above what you might normally earn as an *affiliate*. For example, if the product you are selling consists of a package of goods, rather than a single item, your purchase is enhanced if the items in the package, or some of them, come with individual **resale rights**. That way you can earn as an *affiliate* for the total package plus earn extra by offering each single item separately. In cases like this, the master rights holder (principal product owner) usually only allows you to sell them for a set minimum price (that is much higher, collectively, than the price of the package) but **you receive all the money** from any sales that result. The drawback, of course, is that this kind of plan would only apply if you bought the product for yourself, which is what I recommend anyway, but there are many other plans that allow you to earn extras in other ways; this is just an example.

9.3 Your Own Sales Page

Another method sometimes used to help *affiliates* earn more than they might otherwise do is when the principal hosts each *affiliate's* own **individual sales page** on their *server*, and **allows additions** to that page. They rarely allow full editing, of course, but a small space to accommodate a *link*, or even *links*, to other programs is not unusual. Sometimes they even allow space for **advertising banners** as well. There is often a small charge for this extra and the principal normally reserves the right to approve the copy but it can be quite a profitable extra for some *affiliates* who also have other products to promote.

9.4 List Building

Unfortunately, very few *affiliate* marketing plans allow the *affiliate* any way of capturing the addresses of their customers. There are a few though and if you come across one that does, **count it as a major plus**. I'm sure you have heard the well-known maxim "the money is in the list". Well, it's true, provided it's the right sort of list. By far and away

the best kind is when it's made up of **your customers**. They have bought something off you, so they've already indicated a degree of trust. Not only that but they are **known buyers**, not tire-kickers, and you need to hang on to them for all you're worth. If your *affiliate* program allows you to keep in contact, send them a regular *e-zine*, send them the occasional gift, **pamper them for heaven's sake!** Many will buy off you again, if you do.

Unfortunately though, the accepted norm is that the people who bought a product through your *affiliate* ID just disappear into the ether because there is no way for you to record their contact *email* addresses. As previously stated, this is a drawback that most *affiliate* programs suffer from. So what happens to their addresses then? The principal running the *affiliate* program **adds them to his list**, of course!

9.5 Multi-Tier Affiliate Plans

Due to the actions of crooks and scam artists on the *net*, as well as off it, the number of genuine multi-tier *affiliate* plans has shrunk drastically over the last couple of years. Some well known payment processors like ClickBank now totally shun them. They've just become too much trouble. It's a similar scenario to the way *spammers* have come close to ruining *email*. Have you ever received an *email* from a known and respected source that says something like "Thank you for your pay/ment"? They have to disguise the word payment because their *email* will otherwise run the risk of getting sent to your junk folder, or worse, to your *ISP's* deletions bin. You just can't write in plain English any more for fear that the *email* recipient will never see it. It's the same with multi-tier *downlines*.

9.6 A Respected Principle

Yet the principle of multi-tier payments has a long history. I used to be paid over-riding commissions, which are the very same thing, two levels deep as a sales manager in the real world twenty years ago and I don't ever remember anyone, either above or below me, raising any objections. Or trying to trick the system. Pyramid scams were well known but nobody ever suggested that it was the multi-tier payment system that was at fault. It seems that in the *virtual* world, everyone opts for the easiest way out and looks for a scapegoat instead of blaming the real perpetrator of the evil. Or perhaps that's just the way of the world nowadays.

Anyway, my point is that there are precious few multi-tier *affiliate* programs around any more, presumably because of the stigma attached to pyramids, *MLMs* etc with which they are so easily confused. It is such a pity though, as they can be an **excellent and viable system** that allows ordinary mortals the chance to grow a long term substantial income.

9.7 The Wheat And The Chaff

What makes any scheme dubious is when the participants get paid for recruiting so-called 'distributors', and when that is the primary objective regardless of whether the product itself has any value (it rarely has, though). Everything else is secondary (and sometimes no product even exists). Their remuneration comes from the 'fees' of future recruits and, at the same time, the number of levels is almost always close to infinite, or very long anyway, which is clearly unsustainable.

In the case of a genuine multi-tier *affiliate* plan, the '*downline* levels' are restricted to a certain number (as opposed to being open-ended) and are usually not more than four or five levels deep. Also, the total commission payable is shared between the referring *affiliate* and **his upline**. The remaining funds 'in the pot', i.e. after deducting the total commission, must be sufficient to cover all the normal expenses, such as development costs, *virtual* shelf space, owner's profit etc. and still make mathematical sense for it to be viable.

9.8 Example Of A Multi-Tier System

As an example, let's say that *Affiliate A* sells to B, who becomes *Affiliate B*. *Affiliate B* then sells to C, who becomes *Affiliate C*. *Affiliates B* and *C* therefore, are now in *Affiliate A's* *downline*. Conversely, *Affiliates A* and *B* are *Affiliate C's* *upline*. In a '3 tier' type of arrangement this is where it would stop. By that I mean that *Affiliate C* can go on to sell to D, for example, but all it would mean in terms of the *commission tree* is that *Affiliate A* would drop out of the picture. (By the way, I talk here of *affiliates selling* just to try to make things clear. In actual fact, of course, all the *affiliate* has to do is **refer** people to the sales page.)

So for argument's sake, let's say that commissions are set at 35% on the 1st tier, 10% on the 2nd tier and 5% on the 3rd tier. That means that, after total commissions are deducted, there is still 50% remaining. It doesn't matter what the remaining figure is, so long as there is an amount left to cover expenses, including the owner's return on investment. In the above example, if *Affiliate D* were to refer someone who then bought the product, he (*Affiliate D*) would be credited with 35%, his immediate *upline* (*Affiliate C*) would get 10%, and the top one in his *upline*, *Affiliate B*, would receive 5%.

So why not simply pay out the full 50% from the word go? The answer is that it gives each *affiliate* the incentive to sell more, which recruits more *affiliates*, which gives him more income. And all the time the system remains viable. Also, your *downline* (to the level specified) becomes your **sales team** meaning they're all working for **you**. Lastly, it means that the commission/price problem that I mentioned earlier (in Chapter Eight) can be solved because of the volumes involved.

If you really want ultimate success from *affiliate* marketing, this is the type of plan you should look for. Be careful though, the genuine ones are rare while there are lots of very dubious copycats and rogues around who simply don't spell everything out properly and whose real aim is to trap you. Remain vigilant and keep in mind all you've learned in preceding chapters.

9.9 Other Things To Look For

So, what else do you need to look out for? Number one would always have to be full *downline* and sales **tracking**, including commissions earned and commissions owed. Your principal should have an **automated** system to calculate these and you should always be able to look them up whenever it suits you—*online*. Number two, in my book, would be a **clear commission structure**. And lastly, **downline support**. The value of having someone else constantly encouraging and helping members of **your** *downline* to succeed (and therefore, **you**) goes completely beyond monetary assessment. It is, quite simply, invaluable.

Chapter Ten

Conclusion

10.1 What Now?

Twenty years ago the *Internet*, as we know it, didn't exist. Now it's a major force in technology and promises to dominate all communications and the dissemination of most of the world's information as far as we can see into the future. This is no fad, as some believed until quite recently, but the problems outlined in this little booklet are real and are not going to go away any time soon. If anything, they are going to get worse as the crooks and rip-off merchants learn to use technology more and more to their advantage.

Technology though, can be a two-edged sword. Just as they can use it against us, so we can use it to protect ourselves. It's the need to stay ahead of the game that's the key, and that's what *ITRAPS* has been largely all about.

However I know, once again from personal experience, that a lot of people will read this far and then, despite their best intentions, never get around to doing anything about protecting themselves, until it's too late. So the answer to the question "what now?" is **put what you've learned into effect!**

10.2 Summing Up

We've looked at what the *Internet* is, how it evolved, its various parts and what they're used for. We've looked at the hopes people had for it and the problems that have arisen with it. We've looked at some of the dark and nasty aspects of it and the criminal behavior that is rampant, both in technological ways that can be turned against us and, in the commercial area, scams and rip-offs that we can so easily be lured into. We've covered the ways that we can protect ourselves by what we do and, sometimes more importantly, what we shouldn't do. And we've discussed the *software* that we can buy, or *download* for free, that is absolutely vital in helping to protect us. Lastly, we've considered how we can use the *Internet* to better our lives in ways that were previously impossible; namely, using it to **work from home**, in our own time, to earn a decent, ethical income (more on this later in this chapter).

10.3 Using The Internet More

I have hardly touched at all on how the *Internet* can be used for entertainment, education, science, politics, literature, the arts and many, many other areas, but these are subjects to which whole books are devoted and that are outside the scope of *ITRAPS*. However, I **have** included three appendices that offer further help.

10.4 Appendix I: A Glossary

A glossary of some *Internet* (plus some marketing and general computer) words, phrases and acronyms that you are likely to come across fairly frequently in the course of *surfing online*. These are just a few of many but I will be adding to them from time to time as others come into current use or are pointed out to me.

10.5 Appendix II: Recommendations

Contains further information about what programs discussed in *ITRAPS* are available and where to get them, as well as some that we particularly recommend. This is a very important aspect of this *ebook*, so please don't overlook it.

10.6 Appendix III: Useful Tips And Links

A list of useful tips that might help with your *online* experience in some way or will add further information about an area already covered within these pages. There is also a list of what I consider to be some very useful *links*, especially for *newbies* but that some busy experienced users might find handy too.

10.7 Newsletter Publishing

There are several places in *ITRAPS* where I mention the value of building and using a *mailing list* for promotional purposes. By far the best way to use it, of course, is to send out a **regular newsletter** in the form of an *ezone*. If you are one of those people who find that prospect a bit daunting, I highly recommend the following two *sites* for information and help in this area (because we own them and we think they're the best!). They are:

1. [ClipCopy Content Solutions](#)
2. [101 Newsletter Answers](#)

10.8 A GENUINE BIZOPP SOLUTION

Did you feel as if you were left 'hanging in the air' a bit at the end of Chapter Nine? I'm only too aware that finding a *bizopp* with **all** the specifications advised might be really difficult, if not impossible. What you need to do then, is find one with as **many of the features** recommended as possible. If you find there are hardly any *bizopps* with more than one or two of the benefits mentioned, that just confirms my point about the difficulty of finding a **truly viable and easy online business** that you can start in your spare time at home. Believe me, despite all that's said, they are pretty rare!

So I decided to solve that problem by coming up with one myself!

The program I've put together is called **Easy-Earn**. It has been **purposefully** designed to include **all the features** recommended in this *ebook*—**and more!** What do I mean by more? Well, for example, if you become an *affiliate* for **Easy-Earn**, you will also get your **own branded copy of ITRAPS** (in fact, this is a branded copy you are reading right now). What branding means is that it includes a *link* to **Easy-Earn** (see below) that **already has your referral ID embedded in it**. So anybody who becomes an *affiliate* after reading **your copy of this ebook** will automatically go **straight into your *downline!*** All you have to do is **give away ITRAPS** and you **will** succeed.

"But what's the product?", I hear you ask. Well, what do you want it to be? There are many products (we call them *ValuePaks*); you just choose the one that's closest to your own interests. Or more than one if you want. There are now eight *ValuePaks*, but we are going to be adding more over time, to cover as many 'in demand' *niches* as possible. **All** of them consist entirely of digital products (i.e. software, ebooks etc.), all are **extreme bargains**, and all are instantly downloadable on purchase. The ones we currently have are shown on the [ValuePaks](#) website (click the link to have a look at them).

More additions to our suite of *ValuePaks* will come out as time goes by. As you saw, if you looked through the current

range, we chose the name *ValuePak* because it most closely describes what these special collections of ebooks and software are all about. Each is focused around a particular theme, or marketing niche, and they are priced at **second-to-none** bargain rates to **sell fast**. Also, many items in each collection come complete with **Resale Rights!** Remember, these were put together to solve some of the main problems associated with business opportunities on the Internet. It's an easy, attractive proposition that works—with no catches.

"Sounds great", you might say, "so I don't really have to do any work?" Well, if you mean you just want a *ValuePak* and don't want to promote it, then no, you don't have to. On the other hand, if you mean as an *affiliate*, then of course you have to work! As I've said before in this book, making money is hard work. **But it doesn't have to be tough.** With Easy-Earn, all the really **tough bits** have been done for you! It's simply a matter of promoting the *ValuePaks* and the opportunity that goes along with them—and giving away *ITRAPS* is one way of doing this.

So, do you think **you** can **give away** lots of **free copies** of this **really useful ebook** (without spamming, mind you)? Of course you can!

Just *click* the following *link* to have a look at Easy-Earn for yourself—and **prepare to be amazed!**

[Easy-Earn: The Quickest And Easiest Way To Make Real Money On The Net —Legally!](#)

10.9 Updating 'Internet Traps, Rip-offs And Pitfalls'

If you found this *ebook* useful, **don't just forget it!** We update it from time to time so it's worth using the *link* that brought you here to return occasionally and *download* a more recent version. For this reason, **make a note of the link** you were given that first brought you to the *ebook*. You can also **give away** the same *link* to **your friends, members of your *opt-in mailing list*, or anyone else you know** who may benefit from it (**but don't spam**). Don't give away the actual *ebook* though; **give away the link** so that everyone gets the latest version. (If you've lost the *link*, [click here](#).)

Appendix I

Glossary

The Online 'Language'

Nearly all trades, professions and interest groups have their own language, or jargon, and the *online* world is no exception. In fact, if anything, you need to understand even more new words and phrases than a lot of other comparable interests because of its highly technical nature. Not only that but the prevalence of acronyms is matched only by the number of technical advances that arise with such frequency. For these reasons this glossary is made up of words and phrases that are in common use in the areas of general computing and computer *networking* as well as *online* sales and marketing.

ACTIVEX	A Microsoft reusable <i>software</i> component developed for Windows
ADSL	Asymmetric Digital Subscriber Line; uses one phone line for simultaneous voice calls and fast data downloads/uploads
ADWARE	<i>Software</i> that displays advertisements on a computer
AFFILIATE	<i>Virtual</i> salesperson who gets paid on commission
AFFILIATE TREE	Sometimes <i>Commission Tree</i> ; hierarchical order of <i>affiliates</i> , <i>upline</i> being those above and <i>downline</i> those below any specific one
ANALOG	Electronic representation analogous to the original
ANSI	American National Standards Institute; standards for computing and <i>IT</i>
AOL	America <i>Online</i>
ASCII	American Standard Code for Information Interchange; code built-in to all computers representing the characters on the keyboard
AUTORESPONDER	Program that automatically replies to incoming <i>email</i> messages
BACKDOOR	Security 'hole' deliberately set up for the purpose of bypassing normal authentication
BACK END SELLING	Offering further products for purchase to a buyer who already bought
BIG DOGS	<i>Gurus</i> with large <i>mailing lists</i> , often contacted first for <i>pre-launches</i>
BINARY	Data that has been converted into lots of 2 digits (bits) of 1 and 0, or + and – (see also <i>digital</i>)
BIT	<i>Binary</i> Digit; smallest element of computer storage (8 <i>bits</i> = 1 <i>byte</i>)
BIZOPP	Business opportunity
BLOG	<i>Website</i> where entries are seen in chronological order (usually reverse); used for displaying topical news or as an <i>online</i> diary
BOOT	Act of executing <i>digital</i> start-up instructions
BOT	<i>Virtual</i> robot; a program that scours a <i>network</i> to carry out a specific task
BROADBAND	Fast <i>Internet</i> connection, most often refers to <i>ADSL</i>
BROWSER	<i>Software</i> application designed mainly for viewing <i>webpages</i>
BUFFER	Reserved memory segment used while data is processed
BUG	Programming error that causes an unexpected event or occurrence
BYTE	Set of 8 <i>bits</i> that represent a single character (such as 'a', 'b', etc)

CACHE	Temporary storage area for frequently accessed data
CAD	Computer Assisted Design; <i>software</i> used to help solve design problems
CENSORWARE	Censoring software for restricting access to potentially inappropriate material
CD-R or DVD-R	Recordable (once only) <i>CD</i> or <i>DVD</i> disk
CD-RW or DVD-RW	Re-recordable <i>CD</i> or <i>DVD</i> disk
CD	Compact Disk; removable storage device for <i>digital</i> data up to 680 <i>MBs</i>
CGI	Common Gateway Interface; for executing programs on the <i>WWW</i>
CHAT ROOM	<i>Virtual</i> room whose users can send and receive messages in real time
CHIP	Integrated circuit, usually made of silicon
CLICK	Press and release the left mouse button
COMMISSION TREE	See <i>Affiliate Tree</i>
COOKIE	A small text file placed on to a computer by a website to remind it that you've visited before
CPU	Central Processing Unit; the main microprocessor <i>chip</i>
CYBERSPACE	An imaginary universe representing the <i>online</i> experience
DHTML	Dynamic <i>HTML</i> ; <i>web</i> language that allows interaction and animation
DIALLER	Program that uses your phone line to call a number from your computer
DIALOG	Miniature window mainly used for system information messages
DIGITAL	Made up of numbers (see also <i>binary</i>), for transmitting electronically
DNS	<i>Domain Name Server</i> ; program that translates <i>domain names</i> into their correct <i>TCP/IP addresses</i>
DOC	Common <i>file extension</i> for a document <i>file</i> (usually Microsoft Word)
DOMAIN NAME	Unique name for a <i>website</i> ; works in conjunction with <i>TCP/IP address</i>
DOUBLE OPT-IN	Same as <i>opt-in</i> but confirmed again by <i>email</i>
DOWNLINE	<i>Virtual</i> sales team; usually made up of <i>affiliates</i> recruited by each <i>affiliate</i> above in the <i>affiliate tree</i>
DOWNLOAD	Copy a <i>file</i> from an exterior source to your own computer
DPI	Dots Per Inch; used for calculating screen or printing <i>resolution</i>
DRIVER	Program that interprets software commands as hardware instructions
DTP	Desktop Publishing; using a computer to produce a publication
DVD	<i>Digital</i> Video Disk; removable storage device for data up to 4.7 <i>GBs</i>
EBOOK	Electronic book
EMAIL	Electronic mail
EXE	Common <i>file extension</i> for an executable <i>file</i> (could be a program, <i>ebook</i> or self-opening compressed <i>file</i>)
EZINE	Newsletter distributed by <i>email</i>
FILE	Data stored as a record on your computer (or on paper)
FILE EXTENSION	Characters after the dot in a filename that identify the <i>file</i> type
FIREWALL	Component for preventing unauthorized users from gaining access to your computer through a <i>network</i> , including the <i>Internet</i>
FIREWIRE	Fastest of the 'plug-and-play' alternatives to serial and parallel ports
FLAMING	Abusing someone for a trivial misdemeanor in a forum or chat room
FLOPPY DISK	Older removable device for data storage
FORM FACTOR	Size of a component measured by amount of desktop or floor space used
FORUM	Discussion group or <i>virtual</i> message board for posting/reading messages
FREEWARE	Free <i>software</i> , sometimes <i>Open Source</i> or no restrictions
FTP	<i>File Transfer Protocol</i> ; for copying files from one computer to another
GB	Gigabyte; just over 1000 <i>MBs</i>

GOOGLING	Searching the <i>Internet</i> using <i>Google</i> , the largest search engine
GRAPHIC	Data that displays as a picture or image
GURU	So-called <i>Internet</i> marketing expert
HANDLE	Pseudonym or nom de plume
HARD COPY	Paper printout of computer <i>output</i>
HARDWARE	Physical elements of a computer, such as monitor, keyboard, soundcard
HOME PAGE	Entry page for a <i>website</i> or the start page on your <i>browser</i>
HTML	HyperText Markup Language; displays <i>webpages</i> or <i>web-like emails</i>
HTTP	HyperText Transfer <i>Protocol</i> ; used to go to and from, or to locate, <i>URLs</i>
HTTPS	Same as <i>HTTP</i> but signifying a secure (encrypted) <i>site</i>
HYPERLINK	<i>Clickable link</i> for moving between or within <i>files</i>
ICON	Small <i>graphic</i> in many computer applications that represents a frequently used command
IM	<i>Internet</i> Marketing or <i>Internet</i> Messaging
INK JET	Printing method that uses nozzles to spray ink droplets onto paper
INPUT	Data entered into a computer for processing
INTERNET	Huge world-wide <i>network</i> of inter-connected computers
INTRANET	Closed <i>network</i> of computers, e.g. a company <i>network</i>
IP	<i>Internet Protocol</i> ; governs how packets are sent over a <i>network</i>
IP ADDRESS	Numbers used by routers to direct packets. Humans use <i>domain names</i>
IRC	<i>Internet</i> Relay Chat; see <i>chat room</i>
ISP	<i>Internet</i> Service Provider
IT	Information Technology
ITRAPS	Acronym for this ebook, 'Internet Traps, Rip-offs And Pitfalls'
KB	Kilobyte; just over 1000 <i>bytes</i>
KEYLOGGER	<i>Spyware</i> that records everything you type and (sometimes) every <i>click</i>
KEYWORD	Word or phrase (<i>keyword</i> phrase) entered in a search engine form
LAN	Local Area <i>Network</i>
LASER PRINTER	Printer using laser beam technology to produce letter-quality results
LETTER-QUALITY	Printed <i>output</i> that is superior to typewriter quality
LINK	See <i>hyperlink</i>
MAC	Abbreviation for a Macintosh computer
MAILING LIST	List of <i>email</i> addresses of people willing to receive messages from you
MALWARE	Malicious <i>software</i>
MB	Megabyte; just over 1000 kilobytes
MLM	Multi-Level Marketing; commission sales method where payments come from sales of <i>downline</i> members. Some of these are pyramid schemes
MODEM	Device that translates audio phone line data into <i>digital</i> data
MONITOR	Video display component of a computer
NET	See <i>Internet</i>
NETWORK	Connected computers; as small as two or worldwide, such as the <i>Internet</i>
NEWBIE	Person new to the <i>Internet</i>
NEWSGROUP	Type of <i>forum</i> on <i>Usenet</i> run by volunteers, similar to the modern <i>blog</i>
NICHE	Market segment on the <i>Internet</i>
NNTP	<i>Network</i> News Transfer <i>Protocol</i> ; connects <i>Usenet</i> groups to the <i>Internet</i>
OCR	Optical Character Recognition; <i>software</i> for converting printed characters into <i>digital</i> data
OFFLINE	Not connected to an <i>online network</i>

ONLINE	Connected to the <i>Internet</i> or any other external <i>network</i>
OPEN SOURCE	<i>Software</i> license that allows source code to be available with few or no copyright restrictions
OPT-IN	Voluntarily signing up or subscribing, usually to a <i>mailing list</i>
OPTICAL SCANNER	Electronic device for converting <i>hard copy</i> into <i>digital</i> data
OS	Operating system, such as Windows or Linux
OTO	One Time Offer; a package that the seller hopes you can't refuse
OUTPUT	What your computer produces in response to user <i>input</i>
PC	Personal Computer; usually what was once known as an IBM compatible
PDF	Common <i>file extension</i> for an Adobe Reader <i>file</i>
PHYSICAL MEMORY	See <i>RAM</i> .
POS	Point Of Sale; usually a <i>webpage</i> for <i>digital</i> goods on the <i>Web</i>
POPUNDER	Small extra window that pops up underneath your <i>browser</i> screen
POPOP	Small extra window that pops up on your <i>browser</i> screen
PORTAL	Directory of <i>websites</i> , usually centered around a common theme
PRE-LAUNCH	Special offer for <i>big dogs</i> only, prior to new <i>bizopp</i> launch
PROTOCOL	Set of rules covering the transmission and receipt of data
RAM	Random Access Memory; memory <i>chip</i> for temporary storage of data
RESOLUTION	Sharpness of screen or printer <i>output</i> measured in <i>DPI</i>
RIGHT CLICK	Press and release the right mouse button
ROM	Read Only Memory
ROOTKIT	Program that takes control of your computer without your knowledge or authorization
SERVER	<i>Network</i> computer shared by multiple users, specified by the type of data it serves (mail <i>server</i> , news <i>server</i> etc)
SITE	See <i>website</i>
SMTP	Simple Mail Transfer <i>Protocol</i> ; the standard <i>email protocol</i>
SOFTWARE	<i>Digital</i> instructions in the form of programs, <i>hardware</i> drivers, etc.
SPAM	Unsolicited and/or unwanted electronic message
SPIDER	<i>Virtual</i> robot specifically made to crawl (search) a <i>network</i>
SPLASH PAGE	Small promotional page pointing at a sales page, used for pre-selling
SPOOF	Forgery of an <i>email</i> or <i>website</i> address by impersonating a genuine one
SPYWARE	<i>Malware</i> used to spy on a computer's data
SURF or SURFING	<i>Clicking links</i> to move from one <i>webpage</i> to another
TCP	Transmission Control Protocol; core item of the <i>Internet protocol</i> suite
TEMPORARY INTERNET FILES	Windows <i>cache</i> where <i>Internet Explorer</i> stores <i>files</i> from <i>sites</i> you've visited. Other <i>browsers</i> use different folders.
TEXT EDITOR	Program for manipulating and editing plain text (<i>ASCII</i>) <i>files</i>
TROJAN (HORSE)	Program disguised to look innocent but hiding <i>malware</i> within it
TXT	Common <i>file extension</i> for a plain text <i>file</i>
UBE	Unsolicited bulk <i>email</i>
UCE	Unsolicited commercial <i>email</i>
UPLINE	Those <i>affiliates</i> above any specific one in the <i>affiliate tree</i>
UPLOAD	Copy a <i>file</i> from your own computer to an exterior one
URL	Uniform Resource Location; address of a <i>webpage</i> or <i>email</i> address
USB	Universal Serial Bus; new and faster 'plug-and-play' port
USENET	Major <i>network</i> maintained by volunteers that preceded the <i>WWW</i>

VALUEPAK	A package of digital goods at extreme bargain rates (or the site where they are)
VIRTUAL	Existing only <i>online</i>
VIRUS	<i>Malware</i> that infects a computer when activated (unwittingly) by user
VOIP	Voice Over <i>Internet Protocol</i> ; using the <i>net</i> to transmit (voice) telephone calls
WAN	Wide Area <i>Network</i>
WEB	See <i>World Wide Web</i>
WEB 2.0	<i>Websites</i> using the latest technology to produce 'user-generated content' such as video via YouTube or social interactivity via MySpace
WEBCAM	Movie camera for sending live video over the <i>web</i>
WEBMASTER	Person responsible for managing a <i>website</i>
WEBPAGE	Viewable <i>file</i> that is part of a <i>website</i> , usually with <i>links</i> to other <i>files</i>
WEBSITE	<i>Virtual</i> space identified by a unique <i>domain name</i>
WFH	Work From Home
WHITELIST	Mark an <i>email</i> address as 'allowed' in an <i>email</i> filtering program
WORD PROCESSOR	Application for entering, editing, formatting, and printing text
WORLD WIDE WEB	Largest multi-media network of computers in the world
WORM	<i>Malware</i> that spreads by itself over a network
WWW	<i>World Wide Web</i>
WYSIWYG	What-You-See-Is-What-You-Get; accurate representation of documents on screen while editing
ZIP	Common <i>file extension</i> for a compressed <i>file</i>
ZOMBIE	Computer that's been surreptitiously taken over and used to relay <i>spam</i>

Appendix II

Recommendations

This section is comprised of lists of various software applications and programs that I think are worth considering. Numbers 1 to 5 below are the recommended **types** of software that I believe you need to install to be reasonably safe. They are my best pick of the free or inexpensive programs that are available but within each list they are in no particular order. You have a much wider range of choices if price is no object, which I'm sure you will be able to find for yourself by *googling* for them. It is your choice of course, and will depend on the 'free' versus 'paid' conundrum, the OS you are running, other programs you may have installed, and personal taste.

Number 6, is a short list of some free Open Source software that I mentioned in the book because I believe they will enhance your email, browsing, office services and file uploading and downloading experiences. These, and many of those mentioned in the first five lists, give the lie to that old saying "you get what you pay for". It is no longer true, at least as far as the Internet is concerned. There are many freeware programs on the net and, despite what the gurus may tell you, many of them are top of their range.

Number 7 is a list of 101 Answers sites (i.e. sites owned by myself and my team) which I hope you will find useful.

Firewall Software (Commercial)

Firewall Gold

It's never been so easy to secure your computer before! Simply download, install and run!

[Click here to view on the web](#)

Jetico Personal Firewall

Windows XP or higher, uses multiple level filtering scheme to provide highest protection level.

[Click here to view on the web](#)

Firewall Software (Free)

Comodo Firewall Pro

Windows XP and Vista, free out-of-the-box protection against identity theft hackers.

[Click here to view on the web](#)

Sunbelt Personal Firewall

Highly recommended, free or full versions, comparison chart available.

[Click here to view on the web](#)

Online Armor

Easy to use right out of the box, free and full versions, comparison chart available.

[Click here to view on the web](#)

**Also try [here](#) for a wider selection.

Anti-Virus Programs (Commercial)

AntivirusPremium

Is your computer running slower than usual? Using anti-virus software is more important than ever. Keep your PC safe from virus attack.

[Click here to view on the web](#)

AV Advance

If you've used the Internet over the past month, your computer may be infected with a virus that your current software has failed to detect and remove.

[Click here to view on the web](#)

macrovirus on-call

Redefines the term 'anti-virus'. Why install several different programs when you can solve all your virus and popup problems with this single solution.

[Click here to view on the web](#)

MicroAntiVirus

The world's most trusted anti-virus solution. It protects email, instant messages, and other files by automatically removing viruses. Also detect threats such as spyware.

[Click here to view on the web](#)

VirusNuke

Protects your PC against virus attacks, Trojans, Internet worms and other forms of malware.

[Click here to view on the web](#)

Anti-Virus Programs (Free)

Avira AntiVir

Free virus protection for Windows 2000/XP/Vista 32Bit and 64Bit and for Linux/FreeBSD/Solaris

[Click here to view on the web](#)

BitDefender Antivirus

State of the art protection against viruses, spyware, phishing attacks, rootkits, and more.

[Click here to view on the web](#)

AVG Anti-Virus Free Edition

Recently awarded PC Pro's Software of the Year award 2007.

[Click here to view on the web](#)

avast! 4 Home Edition

Full-featured anti-virus package designed exclusively for home users and non-commercial use.

[Click here to view on the web](#)

**Also try [here](#) for a wider selection.

Anti-Malware Programs (Commercial)

AdwareDeluxe

Eliminate malicious applications before they can steal your private, confidential information, or even your identity.

[Click here to view on the web](#)

Alert Spy

Protect your privacy, stop identity theft, popup ads and privacy invasion.

[Click here to view on the web](#)

Antispy Advanced

Spyware generally reports your activities to advertisers' websites but sometimes it can be a lot more invidious.

[Click here to view on the web](#)

AVG Anti-Malware

Virus, spyware and identity-theft protection for home and office.

[Click here to view on the web](#)

Anti-Malware Programs (Free)

AVG Anti-Rootkit

A very effective free (for now) rootkit detector and remover.

[Click here to view on the web](#)

Spyware Terminator

Award winning, free comprehensive protection comparable to competitors' paid versions.

[Click here to view on the web](#)

Windows Defender

Free program that protects against pop-ups and security threats caused by spyware and other potentially unwanted software.

[Click here to view on the web](#)

Panda Anti Rootkit

Good at detecting rootkits and also quite effective at removing them.

[Click here to view on the web](#)

Microsoft Windows Sysinternals RootkitRevealer

Advanced detection utility for indicating the presence of user-mode or kernel-mode rootkits.

[Click here to view on the web](#)

ThreatFire

Anti-intrusion software that provides protection with no difficult configuration decisions or time-consuming signature downloads.

[Click here to view on the web](#)

**Also try [here](#) for a wider selection.

Censorware

Net Nanny

Net content filter that blocks users selectively from using the Internet, instant messaging, newsgroups, or peer-to-peer software.

[Click here to view on the web](#)

CyberPatrol

One of the most powerful and popular browser independent, Internet blocking software solutions for Windows-based standalone PCs.

[Click here to view on the web](#)

CYBERSitter

The original Internet filter and the best choice for families and public/educational/institutional use.

[Click here to view on the web](#)

MaxProtect Filtering Software

Gives parents complete control over what comes into their homes through the Internet.

[Click here to view on the web](#)

**Also try [here](#) for a wider selection.

Anti-Spam Programs

Anti-Spam Assistant

Block email viruses, phishing attempts, and more—all with one easy-to-use program.

[Click here to view on the web](#)

SpamWasher

The ultimate defense against spam, junk email and phishing attempts.

[Click here to view on the web](#)

MailWasher

The easiest way to check and manage your e-mails before you download them.

[Click here to view on the web](#)

OnlyMyEmail Personal

Works with any e-mail client, and is among the most accurate on the market.

[Click here to view on the web](#)

Cloudmark

Provides unmatched spam, phishing and virus protection at all points of the messaging environment.

[Click here to view on the web](#)

**Also try [here](#) for a wider selection.

Open Source (Free) Software

FireFox

As with the above, this is a *freeware* web browser with an excellent reputation. It is fast becoming a serious contender for top spot against Microsoft's Internet Explorer and has all the advanced features you would expect in a modern browser.

<http://www.mozilla.com/en-US/firefox/>

FileZilla

A fast and reliable cross-platform FTP, FTPS and SFTP client with lots of useful features and an intuitive interface.

<http://filezilla-project.org/>

Open Office

A completely free and totally viable Open Source alternative to Microsoft Office. Includes a word processor, spreadsheet, database application etc.

<http://www.openoffice.org/>

Thunderbird

A free *email* and *newsgroup* reader from the Mozilla organization. Very fast, versatile and secure.

<http://www.mozilla.com/en-US/thunderbird/>

101 Answers Sites

ClipCopy Content Solutions

Premier ready-made (i.e. canned or off-the-peg) written copy for newsletters or websites. Includes articles, jokes, quotations, amusing verses, quizzes, unusual facts and anecdotes, recipes, word puzzles, and much, much more.

<http://www.clipcopy.com/>

Easy-Earn

A truly unique affiliate program that markets 'ValuePaks'; 101 Internet Answers packages of outstanding value. It pays out often, and builds a massive mailing list—all for practically nothing!

<http://www.easy-earn.biz/>

101 Newsletter Answers

Newsletters are by far the most powerful way to communicate with a group (any bunch of people who share something in common) on a regular basis. Learn how to make the most of them for free.

<http://www.101newsletteranswers.com/>

101 Internet Answers

Crammed with tools and services that are likely to be of use to anyone who wants to use the Internet in a practical way; particularly those needing to advance their small business presence online. Includes The FAT System and our amazing *ValuePaks*!

<http://www.101internetanswers.com/>

101 Answers Mailing Lists

Free Ad Tips

These bulletins are chock full of useful marketing advice and information about **free** (and nearly free) advertising. It's a 'double opt-in' list so you will receive an email with a confirmation link. Click the following link to go to the sign-up page.

<http://www.easy-earn.biz/bullets/>

101 Newsletter Answers

A monthly (approximately) ezine with the primary focus on content (what's appropriate, where to find copy, how to improve it etc) and usage (using newsletters for PR, communicating, marketing, etc). Click the following link to go to the sign-up page.

http://www.101newsletteranswers.com/e_nlas.htm

Appendix III

Useful Tips And Links

Opening A Newsgroup Account

If you want to take advantage of the availability of newsgroups, you first need to set up a newsgroup account. To do this, simply carry out the same procedure as for setting up an email account but where you are prompted for the type of account, check Usenet or Newsgroup, as applicable. You will also need to know the *server* name (it starts with the word news) for the news provider you want to use. Most *ISPs* offer this service so it is usually just a matter of looking up their configuration options.

Whitelisting

Most anti-spam software has a whitelisting feature, which is a way of permitting selected email addresses (or sometimes, email domains) to bypass the filters used by these programs. The following list covers whitelisting in some of the most popular email programs and email providers. Unfortunately it is not possible for us to provide this advice for **all** such programs, and certainly not individual *ISPs*, since there are too many. However, if you or your *ISP* use one not mentioned here, there is a certain consistency among them that should hint at the action you need to take with yours.

AOL

1. (version 7) In the Exclusion and Inclusion Parameters section, type or paste the email address you want to whitelist.
2. (version 9. Add the email address you want to whitelist to the People I Know list.

Earthlink

1. Click on Address Book.
2. Click Add.
3. On the Add Contact screen, find the Internet Information box.
4. Enter the email address you want to whitelist.
5. Click Save.

Hotmail

1. Click the Mail tab.
2. Click Options.
3. Click Junk e-Mail Protection.
4. Select Safe List and enter the email address you want to whitelist.
5. Click Add and when the address you entered appears, click OK.

Or another way is to simply add the email address you want to whitelist to your Contacts list or Address Book.

Microsoft Outlook

1. On the Tools menu, click Options.
2. On the Preferences tab, under E-mail, click Junk E-mail.
3. Click Safe Senders.
4. Click Add.
5. In the Enter an e-mail address, enter the email address you want to whitelist and then click OK.

MSN

1. Click on Settings: E-mail | Junk e-mail.
2. On the E-mail settings screen, click Junk E-Mail Guard.
3. Select Safe List.
4. In the space provided under Add people to the safe list, enter the email address you want to whitelist.
5. Click Add.

For older versions:

1. Click on E-mail settings.
2. Click Junk Mail.
3. Select Safe List.
4. Click Add an item to this list.
5. Enter the email address you want to whitelist into the space provided.
6. Click Add.

Verizon

1. Go to E-Mail & More.
2. Go to Check My E-Mail.
3. Click Options.
4. Click Block Senders.
5. Add the email address you want to whitelist to the Safe List.

Yahoo! Mail

1. Click [Mail Options](#).
2. Click [Filters](#).
3. Click [Add Filter](#).
4. In the top row, labeled [From header](#), make sure [contains](#) is selected in the pull-down menu.
5. Click in the text box next to that pull-down menu and enter the email address you want to whitelist.
6. At the bottom, where it says [Move the message to](#), select [Inbox](#) from the pull-down menu.
7. Click [Add Filter](#) .

Or if the email you want to read is filtered to your [Bulk](#) folder, open the message and click on the [This is not Spam](#) link.

Other Providers

If emails you want to read are being filtered, try adding the address you want to whitelist to your [Address Book](#) or [Contact](#) list. If this option is not available, try moving the message to your [Inbox](#) or forwarding the message to yourself.

If these tips don't work, email your *ISP's* tech support and ask how you can be sure to receive all emails from a specific domain or email address.

Browsing And Emailing

In this section we provide a short list of websites with suggested browser and mail client settings for Internet use. Although they were written for [Internet Explorer](#) or [Outlook Express](#), they apply equally to their competitors (many of which have them as the default settings).

[Configure the Security Settings In IE7](#)

Although changes have been made to Internet Explorer 7 (IE7) to make it safer than IE6, security issues remain and many of the same considerations for IE6 are also pertinent to IE7. In fact, possible exploits using active scripting surfaced immediately after the release of IE7 to the general public. This site lists all the default settings alongside their recommendations.

[IE6 and Outlook Express Tweak Guide](#)

TechSpot provides a wealth of useful advice for all levels of computer users and once again comes up trumps. This site is well worth bookmarking.

[Recommended Internet Explorer Settings](#)

This site has even more security, privacy, and advanced options than the previous ones since they cover Intranet, trusted and restricted sites as well. Not only that but they have a downloadable executable file that will make the necessary changes (in accordance with their chart) for you.

[Customize Cookies Settings in Internet Explorer](#)

This article describes how to configure and customize cookies settings in Internet Explorer.

Search Tips

Most people should find the tips at the following URLs quite useful.

[Spider's Apprentice \(The\)](#)

The purpose here is to help you understand and use search engines. How do they work? Why do certain results come up frequently and others not at all? Which search engines are most useful and efficient? How can you improve your searches and find what you want more easily?

[Recommended Search Strategy And Tools](#)

This tutorial presents the substance of the web searching workshop offered by the Teaching Library at the University of California at Berkeley. It covers search engines, subject directories, meta-search engines, and what is known as the invisible web.

[Tips For Searching Library Databases](#)

This is a useful page of tips for searching library databases from the [University of Edinburgh](#) website. The tips are equally useful for web searching since they cover using appropriate key words, using Boolean operators, using appropriate truncation etc.

[Google Web Search Help Center](#)

Doing a search on Google is easy. Simply type one or more search terms (the words or phrase that best describe the information you want to find) into the search box and hit the 'Enter' key or click on the Google Search button. Choosing the right search terms, however, is the key to finding the information you need.

[Tutorial On Evaluating Information](#)

Information on the Internet should always be treated as suspect until you have determined its validity. This [University of Southern Queensland](#) tutorial will show you how to assess your search results for quantity, quality and relevance, how to revise your search strategy and how to apply criteria for evaluating information.

Making Contact (Other Than By Email)

This section largely features sites that list some of the most frequently used forums, blogs, web telephony and messenger sites on the Internet. It is not an exhaustive list, nor does it cover every means of contact available to Internet users, but newbies in particular might find it a useful starting point.

Forums

Big Boards

Here you can sort the forums in our database by various metrics, and apply filters on the language or software used. Offers a ranking system for evaluating the popularity of all software forums.

<http://rankings.big-boards.com/>

BoardReader

A search engine for forums and message boards. Get fast and quality searches for your own forum.

<http://boardreader.com/>

Blogs

Technorati Blogger Central

Lists its own version of the top 100 blogs.

<http://technorati.com/pop/blogs/>

eBizMBA's 30 Most Popular Blogs

Combines data from multiple sources, including inbound links from Yahoo Site Explore, Alexa Rank, etc for a different ranking measure.

<http://www.ebizmba.com/articles/popular-blogs>

Bloglines Top Blogs

A list of the current most popular feeds.

<http://www.bloglines.com/topblogs>

The Guardian (UK)

The world's 50 most powerful blogs, including a comprehensive thumbnail outline of each entry.

<http://www.guardian.co.uk/technology/2008/mar/09/blogs>

VOIP and Messenger Service Providers

voxalot

Provides a comprehensive list of VoIP providers around the world, each ranked by users according to value, quality, features and support.

<http://www.voxalot.com/action/globalProviderList>

Skype

The biggest international VoIP and video messaging service in the world, with over 300 million users.

<http://www.skype.com/intl/en/>

Yahoo! Messenger

One of the most popular video messaging services on the web.

<http://webmessenger.yahoo.com/>

MSN Web Messenger

Lets you talk online and in real-time with friends and family using just a web browser. Use it on any shared computer—at school, at work, at a friend's house or anywhere you can't install the MSN Messenger software.

<http://webmessenger.msn.com/>

AOL Instant Messenger (AIM)

A free online chat service for instant messaging.

<http://www.aim.com/>

Social Networking Sites

[A list of Social Networking Websites](#)

Supplied by Wikipedia, the free encyclopedia, this is a list of the major social networking websites. Please note that the list is non-exhaustive, but is limited to notable, well known sites.

[Unit Structures](#)

You are probably familiar with the major social networking sites: MySpace, Facebook, Classmates.com, and Friendster. There are hundreds of emergent SNS players, but what are sites you need to pay attention to? Here's a list of five social networking sites you need to know about.

[350+ Social Networking Sites](#)

Over the past several years, some social networking sites have thrived, some vanished, while hundreds of new ones have appeared. It has become a huge area to follow, and this article illustrates this well: a collection of over 350 social networking sites, all of which were covered in one way or another here at Mashable.

Video Sharing Sites

[Light Reading's Top Video Sharing Websites](#)

A list of 45 top video sites with comments included and the marks awarded for the top ten classification.

[PC World's Top Ten Video Sharing Websites](#)

These websites allow you to upload your videos for sharing with other connected users, through either the site or your blog, and some even share income with you.

A List Of 40 Useful Websites

- <http://en.wikipedia.org/>
- <http://findarticles.com/>
- <http://home.efax.com/>
- <http://onguardonline.gov/>
- <http://selfpromotion.com/>
- <http://sitelevel.whatuseek.com/>
- <http://tinyurl.com/>
- <http://www.anybrowser.com/>
- <http://www.archive.org/>
- <http://www.articlebanks.com/>
- <http://www.boogiejack.com/>
- <http://www.bookmarklets.com/>
- <http://www.botspot.com/>
- <http://www.changedetection.com/>
- <http://www.coolarchive.com/>
- <http://www.coursesuseek.com/>
- <http://www.dynamicdrive.com/>
- <http://www.ezineadauction.com/>

- <http://www.filext.com/>
 - <http://www.freeadvice.com/>
 - <http://www.freeautobot.com/>
 - <http://www.freesticky.com/>
 - <http://www.freewebtools.com/>
 - <http://www.freshdevices.com/>
 - <http://www.jansfreeware.com/>
 - <http://www.plinko.net/>
 - <http://www.publicityinsider.com/>
 - <http://www.queryserver.com/>
 - <http://www.refdesk.com/>
 - <http://www.roboform.com/>
 - <http://www.scambusters.org/>
 - <http://www.soyouwanna.com/>
 - <http://www.speedcolor.com/>
 - <http://www.talkbiznews.com/>
 - <http://www.techguy.org/>
 - <http://www.techspot.com/>
 - <http://www.tracerlock.com/>
 - <http://www.turbonotes.com/>
 - <http://www.vistaprint.com.au>
 - <http://www.warriorforum.com/>
-
-