Another eBookWholesaler Publication

Go behind the Schemes – Know the enemy!

By Ellis Wright

Proudly brought to you by

Lewis Philips signature books

Email

Recommended Resources

Web Site Hosting Service

Internet Marketing

Affiliate Program

Please Read this FIRST

Some advice in this ebook is from Government departments in the U.S.A. (such as the Federal Trade Commission, Secret Service and the Federal Bureau of Investigation) and equivalent organizations in other countries. Their advice may have been updated since this book was prepared and your situation may involve factors which require different actions.

If you live in the U.S.A., please check the web sites of the organizations mentioned above for current advice and addresses.

If you do not live in the U.S.A., please check the web sites of your country's Law Enforcement Organizations and/or contact them by phone or in person.

These sites and those of other appropriate organizations and individuals can usually be quickly reached through your country's central Government website. If that is difficult to search, use your local phone book or even the public library.

Always contact your local police. They have experienced officers on hand or easily accessible that may be able to help you and guide you to other appropriate services.

Disclaimer

This book is based on extensive experience and research.

The author and all associated with the distribution of "Scams Exposed" offer this book for entertainment only. They do not offer professional advice of any kind and all readers must accept full responsibility for their own actions, decisions and whatever use they make of the enclosed information.

We detail many schemes and methods but never, in any way, recommend that anyone use any of them, even 'for fun'. Because this is not intended as a User's Manual, some critical operating details may *not* be present.

YOU HAVE BEEN WARNED.

CONTENTS

Introduction

I can guarantee that, if it hasn't happened already, ***you will be scammed***!

I can't tell when, where or for how much but, after years of hands-on dealings with people that many of you would prefer not to meet, I would bet on that!

That's because it's inevitable that all of us will, at some time:

- Pay more than a fair price for a product or service; from 'miracle' cleaners and engine reconditioners to real estate
- Make an investment, from lottery tickets to company shares, which are over-valued or even worthless
- Donate money, products or other resources to someone or an organization which does not really have the desperate need which you are told that they have
- Or be a victim in some other way of the many schemes that people have developed over the centuries and continue to refine in the Internet Age to take advantage of our natural optimism and generosity.

That doesn't mean that we should seek a life without risk for ourselves before ever putting our trust in others. Most people are as honest as you or I. They will usually respond to us in the manner that we deal with them.

The best defense against the small, nasty minority that seek unfair advantage in their personal and business dealings is to be fair in our dealings with other people.

Also, be aware of the ways of people who walk the dark side - that's what I shoveled into 'Scams Exposed', my *behind-the-schemes* book.

You will learn:

- How to recognize warning signs that *may* indicate a scam (as in the sun *may* rise in the East tomorrow!)
- How to reduce the chance of being a victim
- What you must not do
- What you can do if you suspect that a scammer is targeting you
- What you can do if a scammer has already victimized you
- The classic scam methods and why they are still used

I will give all the details you should need about how the perpetrators work but strongly advise that you don't try any of it yourself. The consequences could seriously affect your health as well as your bank balance.

Do you feel insulted by the suggestion you might misuse the information that I give you? Why do I put that warning in this book?

Because, in the words of my pal, Sam, "The only difference between many 'honest' civilians and guys like me (Sam) is that they don't know how to do this stuff and are afraid of being caught!"

Sam should know because he's made thousands of dollars from simple, often-exposed but still successful scams. The fact that he might have made much more in almost any type of job without all the jail-time which takes up a large part of his life is something that doesn't occur to him.

About The Author

Ellis Wright knows far too many lurks and the people who use them.

Ellis says, "To be able to keep doing what I do would be more difficult and much riskier if I gave any more personal details or my picture for use in the book, sorry."

He hopes that this book will help reduce the amount scammed from you and many other people in the future but he says, "It probably won't because of human nature. P.T. Barnum did ***not*** say, 'There's a sucker born every minute!', but he should have!"

He does not have a website where he can help you with questions about the contents of this book or related matters, sorry. But he suggests that you tell the Ebookwholesaler Member who supplied this ebook to you whether you would like a follow-up to this, Ellis's first book under his own name. Be honest but nice, please – Ellis's feelings are easy to hurt.

The Scammer in The Mirror

There's a little larceny in everyone's psychological make-up. I think it's there to provide a base level of protection – to help us recognize when one or more of our fellow humans is trying to separate us from our cash (or worse).

But there's no need for you to worry – the person that 'forgets' to report finding that they've been given 40 cents too much change by the check-out operator at the supermarket still has a long way to fall to be at the level of the serial scammers that you'll meet here.

And no, I'm not condoning anyone ripping off the supermarket, (remember the poor checkout operator will almost certainly have to make good that 40 cents themselves, so that's who you're ripping off!)

The only way to help you to protect yourself against the offers and promises of the characters in this book and their brethren is to get down and dirty about how some of us treat each other. But, I'm not recommending that you use any of this except as 'a word to the wise', okay?

The person that looks back at you from your bathroom mirror probably doesn't look that much different from the 'average' scammer (or axe-murderer for that matter – but that's a different book).

The Real Scammer

What are the defining characteristics of a genuine scammer?

- ⇨ They live better, when they're not behind bars, than most of us
- ⇨ They pay more attention to their appearance than many of us
- ⇨ They will happily expend more energy than many of us do in our jobs, to get just a few quick dishonest dollars (or lots of them).

⇨ They will never let the chance go by to take even the smallest unfair advantage.

They will spare no-one – age, poverty or illness are no protection from their attentions. And they just view emotional or blood relationships as another way into your wallet more than anything else.

They know just how much you are worth to them within a very short time of meeting you because that's all that they are really interested in.

They actively seek rehabilitation programs when they are caught because they meet more of their own kind and can plan future schemes.

They 'know' they are smarter than us because we let them take our money. According to them, it's really all our fault – we 'ask' for it by being so trusting and we put temptation their way!

Gentlemen Thieves

The public perception of con-men or scammers as being intellectual and non-violent has never been completely accurate. In the past, scammers avoided violence more from a concern about the heavier prison sentences it would attract rather than the popular notion that they were gentlemen crooks.

Few, if any, of the fictional accounts dwell on the effects on the victims from losing their life savings or being found to have embezzled large sums from their employer. This often leads to loss of their home, job, family and reputation and may cause violence within the family or even suicide.

Consideration of those possible consequences would never have stopped the scammers from doing their schemes, so they were surely as responsible for that violence as they would be if they struck the blows or gave the poison themselves.

Modern scammers are quite likely to have a body (and loot) guard while, as a last resort, most would be prepared to protect themselves and the money with all the finesse of a mother grizzly bear protecting her young cubs!

The scammer's target may be a very large amount (like the money that *two* greedy French contractors pressed on Victor Lustig when he offered each of them the exclusive rights to demolish the Eiffel Tower for scrap) or it may just be a couple of dollars.

A scam may require time and expense in careful preparation, selection of confederates and the victim, or it may be almost off the cuff.

But the most important ingredient is a victim. That person has to have access to the money which is all the scammer is really concerned about. And, generally, the victim must be dishonest or desperate enough to grab any chance of sharing some shady money when the scammer offers it. Remember, the scammer doesn't care why you need or want the money, their focus is always just the money.

Off-line Scams

In this section, I'll detail some of the smaller swindles. Many of the 'classics', surprisingly, still flourish in various forms, continuing to reap thousands of dollars, pounds, and other currencies. Others have been rendered obsolete by advances in technology or the development of more lucrative scams that require less preparation, resources and risk.

I don't know of any scam which became less used because people's moral standards improved!

The Feline Pig

Let's go back to the Middle Ages. Don't worry – this is a very quick trip to illustrate the most common features of a scam or con-game.

Good meat was rarely available to the average working family unless they came upon a generous traveler who offered to sell them his pig.

They wouldn't get to see the pig which was held in a tightly roped bag but their need was great and the price was always just about the most they could possibly afford.

They were all sworn to secrecy about the transaction because of the murky origin of the animal – possibly from a noble's estate which would mean death if the transaction was discovered.

This method of delaying the victim's discovery of the fraud is another tactic which is still present in many types of scams that reap the dollars today but some other powerful legal or illegal force is used as the threat instead of the Middle Ages nobleman's anger.

When the kind seller had made his escape, the ravenous family would rip the bag apart to find a huge, starving and ferocious cat instead of the expected docile and delicious porker.

That was what happened if they were lucky. Sometimes, the victims were confronted by a huge rat instead and, while the cat would do some damage as it tried to escape, those large, filthy rats always left disease as well as scars, whether or not the victims were hungry enough to eat it.

That scam, by the way, is believed to be where we get the sayings, "pig in a poke" and "letting the cat out of the bag".

Buried Wealth

Another scam from that period is still reaping scammers rewards today. Someone would hear about a 'wise person', usually a woman, who could be persuaded to change a few coins into real gold or coins of much greater value. The details, like every story scammers tell, could be changed to fit the assumed gullibility and possible assets of the intended victim.

The victim is looking for a quick rise in his fortunes and desperate enough to do whatever the scammer tells him to.

Usually, that would involve passing something of value to the scammer and also the money that was to be increased in value.

If they could transmute gold, why would they work for a couple of groats – because they're really nice, of course! The scammers mostly attract the foolish and the desperate, sometimes people who were both. But they also succeed with the educated and powerful, depending always on how greedy the potential victim was.

The Money Machine

This scam still operates but there was a variant which started with the beginning of the Industrial revolution. Instead of just wrapping the victim's money in a cloth, the scammers had little boxes made which seemed to be capable of producing fresh, untraceable currency.

The scammers would target wealthy businessmen whom they met at hotels, casinos and on cruises – places where there was a lot of money around but someone that always paid with fresh notes still would be noticed.

They would meet their victim, buy him a lavish meal and pay for drinks with new notes. then and let the victim see that they used the last note in their expensive leather wallet.

The scammer would excuse himself and return in about half an hour, letting the victim see that his wallet was refilled with more new notes.

After a couple of days where the scammer might shower some lavish gifts on his new friend, he would approach him with a very worried expression. He'd say, perhaps, that he'd received terrible news about his (non-existent) child and would like to talk to his friend privately.

Then he would say that there must be absolute secrecy about this matter. His child was either very ill or in a foreign country and facing a terrible prison sentence.

The scammer needed a significant amount of money in a great hurry.

He'd say, "I would never ask a friend for a loan." This would certainly relieve the victim's mind! " No, I have something to sell which you will never have another chance to find."

"Now, because of this imminent tragedy, I'll have to reveal my most important secret which has enabled me to live in this style for the last two years although I've not any money or job!"

"I know you don't need more money but this is a bargain even if you just play with it occasionally. You must have realized that I always pay with new notes?"

The victim would agree, already wishing that the scammer would quickly show him the secret and let him buy it!

The scammer would reveal the money machine and even demonstrate it by pushing through a small sheet of good quality but ordinary writing paper. Out popped a genuine bill, maybe $50!

The victim would ask why didn't he just sit up all night and produce the notes.

"Alas," the scammer would say, "the machine is limited to just $400 a day. I don't have that much time before my son/daughter goes to jail or dies."

The scammer would play the victim's greed for every cent that it was worth, all the time saying how generous his friend was. Most of the generous victims would drive a very hard bargain, despite the tragic circumstances.

Of course, the scammer didn't mind because the machine, however impressive with flashing lights and switches cost him probably about $20.

The victim had to hand over cash, of course, then the scammer would gratefully give him the machine and even some nice notepaper (provided by the hotel for free) to get him started.

He'd tell the victim that he, the scammer, had run every note from the machine because of his desperation and it would take about 20 hours to recharge fully.

Even in those days, the scammer with the help of the victim's donation, could put a lot of distance between himself and the victim in 20 hours!

3 Card Trick

With the popularity of magicians and their tricks, do you think that the old 3 card trick and other street scams, based on the methods which magicians use in their performances, would not still draw money from many people's pockets in the 21st Century?

Scammers still work their tricks and so many people greedily wager on their crooked schemes that, to the scammers' admittedly warped minds, they make enough money to consider the obvious risk of prison just another work hazard.

They always have several members of their gang among the spectators or handily nearby. Some of them are just there to protect the gang with whatever force is necessary. This is usually limited to 'settling' any aggressive victims but the heavies are as likely as other gang members to scurry away if police arrive.

Others act different parts to earn their share of the gang's loot. Everyone that wins is likely to be part of their group and the winnings are either never actually paid over or the 'winner' makes sure to return every cent before the share-out after the day's scamming.

Some gang members also watch for the appearance of police or anyone taking too much interest in the game without betting. **Don't** ever think that you can 'play' around with these sharks. They are focused on the money and their own safety – any hint that someone knows what they are up to is likely to put that person in real danger.

They also pretend to help the victims that bet on picking the winning card. They might even turn over the corner of what the victim is sure is the right card when the dealer is distracted by someone else in the crowd.

But the victim still loses because the dealer knows exactly what is going on, and how to secretly straighten that corner and then bend the corner of another card when a gang member distracts the victim.

The odds that the dealer offers seem generous. They would be if there was any fairness in the way the cards are handled. I'm not going to detail the moves which dealers use. They require years of practice to reach a suitable level of smoothness under pressure which is always present when the dealer is surrounded by a crowd that are mostly strangers.

And the risks to dealers are much greater than those faced by other members of the gang. That's because the dealer is most closely observed by the crowd and any lurking police. As a result, they are more often convicted and get longer prison sentences.

They also may be harassed and even beaten by angry victims and other members of the crowd. Often, protection that has been promised by the gang doesn't happen because the other gang members quickly melt away so they don't get attacked or imprisoned as well.

In the Name of Charity

Cars for Charity

This has been reined in by changes to the United States tax laws but, of course, someone in power might decide to help the poor profiteers whose businesses have been affected by the changes and reverse the changes sometime. They were not scammers because what they did was within the law. But, somehow, their dealings left you feeling robbed anyway.

For several years, there have been tax concessions available for people that donated cars which they had owned for at least a year to a recognized charity. The rules are much tighter now.

Sometimes, these cars were sold and the whole proceeds were passed to the nominated charity. Many of them were sold for more than was passed to the charity. How much more? Often, there was enough of a margin (for 'expenses') to provide a comfortable living for the car salesman.

One report that I read, by Jeff Schnepper on moneycentral.msn.com, said that a prominent and respected charity received a benefit from the sale of several hundred cars in a particular year and gave the amount received.

When Jeff Schnepper divided the amount by the number of cars, the average amount per car was just over $120. Now, I don't see many cars being sold from established car yards for $120, do you? And, since that was the average, the charity probably got even less for many of the cars.

Perhaps the charities were victims in this but I am sure the main victim was the average U.S.A. taxpayer! The people who donated the cars were able to claim a tax write-off for

their donation and many chose to claim the book value for the particular model that they donated. If the book value happened to be much higher than the price they might have got if they just sold the car (and probably had to pay tax on the sale price), then that was just a reward for their generosity to the less fortunate!

Again, this was not a scam, just a benefit from careful study of the tax rules.

Charity Related Offers.

Do you get advertising which includes the 'hook' where they promise that some of your money which you pay for their product or service will be donated to a charity or local service group?

"Buy from me and 10% of the price goes to XYY Charity Holdings Inc."

It's great that the charity or voluntary service benefits but the business may have adjusted its prices upward, say, **20%** before making the **10%** offer and the business will probably also claim a tax write-off on the amount of **your money** which they donate!

Why not look around to find the company which gives you the best all-round deal, which will probably be at least 10% better.

Then you can decide which charity that you want to support, how much you want to give and you can get any tax write-off yourself!

Pay Forward

This scam has a long history but it's become very popular and even easier to do since the Internet became available.

That's because the scammers have access to a far greater number of sellers with desirable, high-ticket items through on-line auctions and other sites which list items, such as expensive cars, for sale.

The scammer finds a suitable item and tells the delighted seller he want the item very much and thinks the asking price is very reasonable.

Then the scammer puts in the hook, "I am in another country and foreign exchange is difficult to arrange. But my colleague in your country owes me (an amount that's more than your asking price)."

"I can get him to send you a certified check for what I'm owed . Then you can deduct the sale price and freight charges and wire the balance to me, okay? But please wait until the proceeds are in your account"

That sounds pretty good, especially if you need the money and have found no-one else even remotely interested in paying your price for the item.

The clincher is when the cashier's check is delivered by a reputable courier firm within 24 hours of your acceptance of the deal.

You take it to your bank and ask the teller to examine it. They say that it seems to be genuine and start the processing.

If your bank account is well established, the amount of the check could appear in nice black ink within 24 hours. So, you wire the extra amount to the buyer's address.

You are jerked back to reality about a week later when your bank tells you the check is a fake and they demand that you pay the amount you spent, including the scammer's profit which you wired him when you saw the figure in your account.

Work At Home

These scams don't focus on the greedy, but anyone that wants to add to their current income or get paid for working at home instead of having to go to the employer's premises to do that work, perhaps because of family or health commitments.

But scammers don't spare anyone.

There are many traps in this area and scammers are continually refining their offers but here are simple explanations of some tricks which they use.

Simple Work for High payments.

A large number of people with few job skills, or only specialized skills that are less sought after with changes in technology are becoming unemployed. They are ready victims for the scammers who offer "Type at Home", "Envelope Stuffing" and "Home Assembly" scams.

Type at Home

Though you may not be a very good typist, the rate of return which the scammers offer is very attractive. So, you pay your fee and anxiously wait for the work to pour in.

But it's not a job, it's an opportunity; an opportunity to type out and distribute copies of the same sort of advertisement which caught you! The only payments you will ever see has to come from other people that you scam.

Maybe the offer will be to prepare courses and sell them but those courses may just be one page of simple instructions on how to prepare and distribute these scam offers.

Envelope Stuffing

This must read like a dream come true – fill envelopes with the material the company provides and get a few cents to a couple of dollars for each one!

Whether you sign up with someone offering the lower rates or the higher rates doesn't matter. You will usually have to pay a fee, then you get the secret instructions to copy the advert which lured you and send it to others – your payment will not come from the supplier but from other poor souls that you lure into their scam.

Home Assembly

The offer says something like, "We're desperately short of assemblers and will turn to you as our first source of supply." So, you don't have to do any market research – just

buy ("pay a security deposit") your first lot of parts and they'll buy all you produce, right?

Only if they meet their criteria, which won't be very clear until you go back to them with your first batch. That's when they tell you:

- Your carefully prepared items don't meet their strict quality control standards or
- They're currently over-stocked with that line or
- They had tomato soup for lunch – **any excuse will do**!

That is what they say if they even bother to acknowledge that they got the carefully wrapped package which you sent them. Did you figure the high, certified postage cost when working out how much profit you were going to make?

Some scammers simply close up their office, which is often just a Post Office box or other mailing address, and set up somewhere else.

Then you'll probably start to look at selling your products (they're definitely **your products** now – the supplier has your money which is what they were after!) and that's where more shocks start to pile up.

There's no market for them at a price which will repay you for your effort and set-up costs or there's no market at all for those items.

With the scammers' fees, inflated charges for the parts you had to assemble and other costs such as postage from the scammers' "factory", you paid more than the assembled items could ever be sold for. It may surprise you that people would not check this possibility out before sending off their money but the victims of this scam are *desperate*!

It's only when the bad news strikes that many victims sit down and read the offers and other paperwork for the first time.

Your Own Service Bureau

You've retired or, more likely, been retrenched from your job and you've got a little money, some clerical skills. You soon realize that you need to increase your income though jobs for people in your age group are rare and the number of qualified applicants large.

Then you see an advertisement:

"Run Your Own Service Bureau from home. We supply software, stationery and contact details of businesses in your area that need your services! Sign up today and start your business next week!"

The advertisement might mention specific services such as bill collection, book-keeping or casual secretarial services and transcription.

This sounds like something you can handle and the cost is within your reach; a few thousand dollars.

But the reality is a little less than the promise.

- The software will probably be freeware or obsolete commercial programs that have few instructions, no technical support and may not even run on your computer. **Note;** there's some great freeware programs out there but you should expect current, commercial software when you are charged more than a thousand dollars for it!

- The Forms are standard, cookie-cutter templates that almost anyone can turn out from any Word Processor program. There's little chance that the forms will be set up with any special fields, such as those that might be required for State licenses and tax information.

- The biggest disappointment will probably be the '*selected contact details of businesses in your area that need your services*' – that will just be information

scanned from telephone books and other standard directories that you either have in your home or could access for free at your local library.

Then you find that you'll have to invest a lot of time and more money to make anything out of the investment while competing with established, well-known service providers.

Model Scams

People who are attractive or whose children seem (to them) to be more attractive and brighter than those in the television commercials, are prime targets for scammers at all levels of the modeling business.

The traps may snap down on them right at the start of their career. Some scammers will set up studios or pose as agents, seek out hopeful, inexperienced models or proud parents of attractive children and suggest that they should have a portfolio of professional photos which can be used to seek modeling jobs.

Of course, the pictures and even the actual albums are provided at inflated prices by the scammer. Some will just take every cent they can get and disappear without ever providing any photos or albums.

The photos are not likely to be of a standard acceptable to legitimate agents, advertising companies and studios, so the victims face additional expense for proper photos if they decide to continue their quest after their unpleasant and expensive lesson.

There are other scammers that also call themselves agents. They may have real premises and all the trappings of a legitimate business. Of course, all that can be rented at fairly reasonable rates by the day or the week as a serviced office. Scammers don't mind signing a contract because they're never there when the bill arrives.

These agents advertise for new models to apply to register with their agency. They charge a fee, either for setting up the records or some other excuse.

Legitimate agencies do not charge that sort of fee. Their income is from a commission on the work of the models they accept. Of course, their standards are much higher than the scammers'.

Sometimes, they might say to some hopeful that they will waive their usual fee because they truly believe that person has a real future. Remember the first rule – legitimate agencies don't charge a fee, they don't make special deals with beginners, and agencies

that even sometimes charge fees should be viewed with caution and, preferably, from a considerable distance.

Agencies will suggest that some new models take classes or individual coaching to improve their chances of getting well-paid work. Beware any agent that pushes you or your kids to a specific coach or class. There's a possibility that a nice spotter's fee is the reason for the recommendation, which means that your best interests are not their focus.

At all stages of your career, if you work hard enough and have enough luck for repeat work to start coming in, take advice but make your own decisions.

If the models are your kids, I strongly urge you, right at the start, to discuss every aspect with your partner and also consult your kids. Ensure that both adults are equally confident that the children have everything they need to have a good chance of success and, most importantly, that it's something the children really ***want*** to do.

Many parents try to live their own lost dreams through their children and that is usually a pathway to tears, not stars.

Pet Scams

After ourselves and our immediate family, if we have one, we are most attached to our pets.

There's many ways that scammers can exploit that attachment for their profit. Sometimes, they never even need to see the pet!

Second Time Lucky

When you advertise that you've lost your pet, expect quite a few calls. Most people are good-hearted and many take the trouble to phone if they see a loose animal that resembles the description you gave.

Among the calls though, you may get one from a person that says they've found an animal similar to the one you lost but they need a better description. When you give them

the best information you can, they tell you that it is not your pet and will probably even apologize for wasting your time.

Not very much later, you'll get a call from someone else who gives you a detailed description of your pet. You'll naturally be excited and may even agree to their demand to get the reward money up front. They may say that they had to pay for a veterinarian to attend to your pet or they're some distance away, even in another State – having just returned from a trip to your city, and need the money to bring your pet back.

But it's a scam – the two callers are working together. They have no real information about your pet except what you told that first caller (who fed it to the second caller) and that it's still missing.

Steal and Recover

Some petty, cruel scammers will steal your pet in the expectation that you will offer a reward. If you advertise but don't offer a reward, this type of low-life may phone you and threaten to hurt your pet if you don't pay up.

You Find the Scammer's Pet!

If you find a lost pet, be very careful about who you return it to. Scammers have responded to "found" advertisements for valuable animals with a view to selling them for profit. Some will even try to get almost any animal and then sell them to laboratories, where that is still allowed.

You Have Won

Every day, someone somewhere wins a lottery prize that changes their life, usually for the better. It could happen to anyone, even you – if you buy a ticket.

Some people get that sort of good news even without buying a ticket! It might be a lottery win or even an inheritance.

The news comes in a large envelope bearing some interesting foreign stamps and all the information they need to claim their prize or confirm their interest in being a beneficiary of some relative that they had long forgotten or, more likely, never heard of before.

There's always one important matter that is highlighted in the official-looking correspondence.

You must send an amount to cover processing of their claim. That's really the whole point!

There's usually no prize or inheritance – if there is, it's very unlikely to rightfully be the victim's. Sometimes the scammer goes to the trouble of linking the victim to the name of someone that actually existed but, knowing that greed and optimism are present in us all, they mostly don't worry about providing that level of spurious detail.

And, these days, there's an extra burden for the victim. The scammers are very likely to sell their personal information to other scammers, who will make use of their bank account information and their email addresses.

Little Fish – Small Wins.

As well as the huge but imaginary lottery wins and inheritances, there's some other 'free' prizes that it pays to be wary of.

Travel Certificates.

You might get a certificate awarding you a heavily discounted trip to a popular vacation area. All of us need and probably most of us deserve a vacation and areas that are most popular with tourists always have higher prices than other places.

So, let's go… NO! Before you accept any of those offers, check the fine print ***twice***. Find out what is not covered by your certificate and what fees or other charges you are required to pay.

The Terms and Conditions (which you might have to search for or even contact the company making the offer and ask for a copy) should be read before you start on the colorful brochures.

Otherwise, the only color you'll see after your trip will be **red** – all through your bank and credit card statements.

Trip Deferred.

This one is surprisingly common. There's legislation in most countries where you can seek reimbursement but that can be difficult and, if the promoters of the offers are not registered in your jurisdiction, you might spend more than the cost of your next vacation and get back no more than enough to cover a couple of aspirin.

You get a ***special limited offer*** and are told that you only have to pay a (substantial) deposit for the trip of a lifetime.

But your trip never happens – there are unfortunate delays, after which the promoter offers you free upgrades or other concessions – anything but a refund of your cash.

Then, when you are finally packing to start your holiday, you find that he has taken a quick trip himself and you've paid for it!

Investment Opportunity and Free Holiday

You are approached to look at a time-share investment and the promoters are so confident about what they're offering they'll fly you to the resort and accommodate you at their expense.

It can't hurt to look, can it?

It will – your eardrums will be constantly assaulted and every technique in the high pressure sales handbook will be used on you repeatedly while you 'enjoy' your holiday.

Unless you have the hide and the temper of a crocodile, the only course to relief is to buy or die.

The latter is cheaper.

The Classic Scams

The Ponzi – Fools' Money.

A Ponzi scheme is the classic pyramid scheme. I know you've heard of them – everyone has. Despite their notoriety and frequent warnings through all the media, and severe penalties for promoters that are caught, they still are one of the most common and successful get-rich-quick schemes. They reap rich rewards for their operators if they manage to get away with the proceeds.

It can be dressed in many different disguises, always has copious claims that is genuine, 'unlike those terrible Ponzi schemes', but the operators concentrate on explaining how quickly and simply the Investors, Members or Associates will double their money.

Then they say, "That, of course, is just the start!" and the **GREED** button is pressed in many of their prospective victims.

The operators usually return significant amounts to those who first sign up, confident that those happy players are not only likely to plough more of their savings into the scheme but will also promote the scheme to their friends, relations – everyone they know.

That will quickly bring in much more than the operators have given back and increase the rate that money comes in.

That is very important because the 'dividends' all come from the investors' own contributions. There is no real income from investments or sales and the operators will clean out the company's accounts and quietly steal away one day, not very long after that first, and probably last, dividend payout.

The Big Store

Here are the main parts of the classic big-time scam – the 'Big Store' or 'Long Con' type that is most often represented on the movie or television screen with varying degrees of authenticity.

With the large scams, involving very large sums, there's a **team of scammers**.

A **Spotter** will often locate the potential victim, lure them to meet the scammers and then withdraw, because they have to maintain their reputation and appearance as an honest member of the community. If the victim comes back to them later, they will help them drown their sorrows, if the victim has enough money to pay for the drinks.

The people that had most contact with the victim would be pleasant, attractive and helpful.

One key person, sometimes called the **inside man**, was the scammer that the **Spotter** brought the victim to. They could be male or female, always charming and ready to make the victim feel they had found a true friend.

Another scammer, **the Fixer**, managed the group, making sure each person was in place at the right time, all the equipment and any 'bait' money was available where needed. They also were usually responsible for 'fixing' the local police where this was possible and trying to ensure that none of the local criminals would interfere with the scam or try to get the proceeds from the scammers afterward.

There also could be casuals, either unemployed people hired for a day or a few hours who might be totally unaware of the scam or, more usually, small time crooks that were known directly to the scammers or recommended by their contacts inside or outside of prison.

Even in the 'good old days', few scams operated without a **Heavy**, someone that was ready to apply physical pressure to make sure the victim came up with the money and, more often, to quieten them if they tried to get their money back or threaten to go to the police.

There might also be bribed employees of a firm where the scammers took the victim such as a stock-broking firm.

Using a genuine company's premises entailed a lot of risk and most scammers set up their own fake stock-broking floor, betting shop or whatever and staffed it temporarily with crooks they could depend on.

"Money Laundering"

Real money laundering involves converting money that is the proceeds or robberies and other crimes into legitimate funds by feeding the cash through casinos, other gambling venues or even regular Main Street businesses.

But the scammers' version is the classic which is commonly called "The Nigerian Scam" because many of the addresses and people involved in promoting the offers were based in Nigeria.

For the scammer(s), this has always been just about perfect for their needs. The set-up requires very little investment or time but the return can be huge.

It's sad that the reputation of a whole country is scarred by these crimes and this causes much heart-ache to many honest and hard-working Nigerian people. But the name is etched in place because of the history of the scam. The related violence and the deaths of some of the victims who foolishly followed their money to Africa in vain attempts to get some back have ensured that the country's name is deeply stained.

Over recent years, I've seen this sort of appeal with addresses in other countries, including the U.S.A so it may be that the Nigerian link may loosen from the public mind and be replaced by the term "4-1-9" schemes. But that will still link the scam to its Nigerian roots because the term "4-1-9" refers to the section of the Nigerian penal code that covers fraud!

It begins with a letter or, in recent years, an email which is supposedly from a minor bureaucrat, ex-military man of high rank or the widow of a senior bureaucrat who had been involved with his country's finances. These people or their deceased partners were all removed from office in a coup.

They offer the victim a small commission to help with the secret transfer of a sum, in the millions of dollars, to the victim's country. Because of the large amount which the scammer is supposed to be offering to share, the small rate of commission means the victim looks to be in line for a very attractive total amount if he or she is prepared to be dishonest 'just this once'.

The scammers always stress that their enemies in their country's new administration desperately wants the money back and may be prepared to kill the scammer, so everyone involved has to keep all the details secret. This ploy is really there to stop the victim from contacting the Police or Secret Service or asking their family or even their hair-dresser about the proposed deal.

It may be a surprise to you how effective that these simple lies are time after time, year after year. But the victim is often overcome by greed at this point.

I saw one victim interviewed who said, "I was going to ask the Police but, if they told me it wasn't true, then I would never get the money!" Of course, it wasn't true, he didn't get the money and he also lost his entire savings!

The first thing that the scammer requires of the victim is to arrange for receipt of the money at his bank. To do that always involves sending all of his bank account and credit card details to the sender of the letter. As soon as they do that, their accounts are sucked dry! It's simple, quick, but far from painless.

That's the simplest version of this type of scam. There are many variations and extensions which are sometimes used. If the scammers discover that the victim has considerable assets, they may not just grab the contents of his Bank accounts, and use every available cent of credit from his credit cards (that takes an amazing short time – isn't technology wonderful?!) They can delay that final blow by delaying the deal with 'unexpected' fictional charges or the need to pay bribes to fictional public servants or even police to ensure the smooth transfer of the money from their country.

The victim usually accepts that he will have to pay these charges but will, he is constantly assured, be reimbursed many times over as well as getting the full commission which he was originally offered.

You might expect that the victim will quickly realize that he is just throwing away more of his own money but, like many gamblers who are consistently losing, these victims often feel that they must see it through so they can get back all the money which they have already 'invested'! Even worse, they may be desperate to get a pay-off because they embezzled money from the firm they work for or stole it from family or friends.

A report in the British press a couple of years ago said that British police estimated that, at varied times in each week, up to 100 people would spend an hour or much more waiting in the lobbies of London hotels ready to hand over money as a result of getting these scammers' offerings!

That's despite frequent, repeated exposures and warnings by all media and the police in just about all countries, of every grimy detail of their operations.

Why? G-R-E-E-D on the part of the victims.

Internet Scams

Almost all the 'classic scams' have been migrated to the Internet with appropriate improvements. Many of the classic small-time scams were instant successes when the scammers took them to the Internet. Little change was needed except the scammers could now put their offers in front of thousands instead of just a few people, usually at much lower cost and often with less chance of detection and being caught.

Fortunately, the authorities are catching up with more as police and other groups get the necessary resources for training and equipment. Even the governments and the Courts are starting to realize that, because of the reach of the scammers' offers and the volume of transactions, these crimes are ripping off huge amounts and causing untold hardship, even where the amount of money in individual cases may be small when compared to the latest bank robbery.

The scammers have access to all the best technology because scams are low-cost and high profit – thanks to the generous contributions from their victims.

Sometimes, the scammers keep their costs even lower by obtaining their high-tech hardware and software with worthless drafts and checks or just sign contracts, then skip when they run out of tactics to delay payment of the bills they incur.

Malware

Scammers that use the Internet have new weapons at their disposal – spyware and other programs that are deposited on your computer when you visit some sites, download some 'free' programs, pictures or music files or use chat rooms or file-sharing systems.

A technician showed me a list of more than 400 viruses and similar 'mal-ware' that were specifically designed to infect the computer systems of people using chat services. That was more than a year ago so there are probably many more improved versions lurking there now.

My Computer was Invaded

I got a personal demonstration of the sneaky methods they sometimes employ when I visited a site that offered some free programs (definitely not a porn site!) Suddenly, my computer system was being drowned in a flood of viruses and Trojans which tripped my anti-virus resident protection.

I immediately turned off the modem connecting my system to the Net; hardly a high-tech response but at least it stopped more attacks while I dealt with the stuff already degrading my system.

After some time, I got most of the viruses out. Then I saw that there was a search program in my Start menu which I had never installed! A very professional looking application but I never found out what it was designed to do because I immediately removed all visible parts of it, of course.

All my efforts were not enough though. When I tried to make a Restore point on my 'clean' system (as I thought it was), I could not do so. The viruses had changed some of the most basic settings in my system and the operating system had to be re-installed.

Key-logger Spy Programs

There is another type of program that helps scammers – a key-logger which records all the activity on your computer, what you type (yes, including passwords) and what sites you visit. Then it sends the information to whoever secretly had the key-logger installed on your system.

Programs like Ad-Aware from http://www.lavasoft.de/ and Spybot Search and Destroy from http://www.spybot.info/ are essential to alert you to any of these sorts of programs that might get in to your system and help you to remove them. But, remember, the crooks are updating their spyware all the time so it's essential to always have the most current versions of the programs which protect your computer.

I use both programs which I named. Be wary because there are some anti-spyware programs which come with spyware installed in them! Check for independent and current testimonials. Lavasoft have a forum where you can find out about these issues.

You should also realize that scammers do not need to have this technical knowledge. Not only can they afford to buy whatever technical help they want, there are actually do-it-yourself kits available for those twisted souls who want to wreak havoc by creating and distributing the sort of viruses I encountered or try to make their fortune with their very own spyware!

Old Time Scammers on the Internet

The Internet is even usable for the old-school scammers who are too set in their ways to bother with advanced software.

Some just set up a site which offers people products or opportunities to make money. They either pay a college student a few dollars to make the site and load it to their web domain or they hire a professional to do that, then run up an account before skipping without paying it.

With the site in place they offer tremendous bargain prices, free delivery and whatever it takes to get the victim's money. Other scammers will promote themselves as successful entrepreneurs offering their secrets to a few (thousand) specially selected (from a mailing list) lucky customers.

Their sweat is applied to transferring the sort of offers they've been using for years (to offer shares or used cars) into the proper format of web pages offering Internet-age opportunities and products.

It doesn't take much effort to present yourself on the Net as someone you're not with a string of fake accomplishments. Any legitimate off-line business can save money by putting their brochures and catalogs, with as many pages and colors as they need online. But this also helps the scammer. He can be 'Robert Reputable' on one site and 'Tricia Tantalizing' on another at the same time. Amazingly, it can be hard to discover the truth

but I've put some tips in a later section, 'How YOU should Protect Yourself', on how to spot and avoid these scammers.

The e-Nigerian Scam

The classic 'Nigerian' scam which I detailed under "**Money Laundering**" in the ***Classic Scams – Big time*** section was quickly flooding the Internet as soon as access was available to the general public.

But there are other Internet scams:

Phishing.

Phishing is sending of emails which appear to be from banks, credit card services and other organizations such as your Internet service provider (ISP) or government agencies which you deal with.

These emails have identifying logos which are identical to or closely resemble the organization's real logos. The ever-increasing power and features available in office equipment make it easy for the scammers to prepare virtually identical copies of genuine logos and other identifying marks. And, of course, many people don't look too hard at those symbols when they have just read that their bank account or credit facility may be at risk!

The fraudulent messages say that you need to urgently confirm your username and password of your account by clicking through one or more links in the email.

When the victim does this, they will see a web page that closely resembles the organization's own - but everything they type in, including their confidential information, will be stolen by the scammers!

Beating the Phishers

There is only one way to beat the phisher menace – constant vigilance and NEVER clicking on any link in this sort of email. Where possible, get clarification about any

email communication by making contact on the phone or by a personal visit to the local office of the organization.

Your bank, credit card service or auction site will **never** ask for critical information to be supplied this way.

Every time you go to the organization's site, always start by opening a fresh window in your browser and always type in the specific web address that the organization originally provided to you when you set up your account.

As soon as you complete your transactions, log out and close that window! Many organizations' sites will prompt you about this when you click the button to log out from their site.

I'd also advise that you do not record your usernames and passwords on your computer. Use an electronic diary or, even better, a small paper one which you always keep with you.

Using the history feature of your browser or a software program to keep your passwords ready to hand may save you minutes every week and lose thousands of your dollars just as quickly!

If you are in the U.S.A. and get a suspicious email, send the whole email including the headers to spam@uce.gov. You may need to read the instructions for your particular email program to make sure that you send the email complete with headers. That said, many scammers use varied methods to disguise themselves and keep their real information out of the headers. They may even forge the information of an innocent individual or company. So, it is wise to not make any accusations of bad conduct by someone just because you get a 'spam' or spoof' email from them.

Visit www.ftc.gov/spam to learn other ways to avoid email scams and deal with deceptive spam.

If you live in a different country, check your phone book or search engines for the relevant addresses of organizations to contact.

Qualify On-line.

There are many legitimate organizations offering quality training through the Internet. That's true and, also, my lawyer will be a bit happier if I emphasize that point before telling you about the other sort of qualifications you might be offered.

While the legitimate businesses offer quality training and support their students, there are other people who offer training which needs less of your time (about the same time it takes your check to clear) and their offerings focus on areas which are most likely to have strong appeal for people such as travel agency work, private detective, religious and other qualifications.

What you will get from the scammers' offers are some articles that have some relevance to the subject though they may be years old, a colorful certificate, and lots more advertising from the scammers and spammers that they sell your email, and other contact details to.

Among the offers you get, there may even be one from your supplier, asking if you want to offer their courses to your friends in return for a small commission.

The certificate or diploma will not entitle you to discounts from travel providers, access to a private detective's license or recognition as a priest or holder of a legitimate Doctorate of any kind.

In effect, you pay a lot of money for not very much.

These offers appeal most to people that don't have the time, money or talent to qualify for the regular qualifications. They like short-cuts.

One guy I know got a Certificate this way that declared he was a Bishop! He performed at least one marriage that I know of.

The groom knew my pal very well and set up the wedding soon after meeting his lady when they were both touring.

There was no lasting bad effect. When the happy couple returned to the USA, he suggested that they have another wedding so that their parents could attend!

Whether by design or accident , the Bishop could not make the second event though he did get an invitation.

And that couple are still together more than 20 years later.

I asked the Bishop if that was the only wedding he ever officiated at but he apparently did not hear my question.

Foreign Brides

If you are a lonely male, and decide to look abroad for a wife, there's lots of wonderful ladies that would make a great life companion for you to pick from.

There are also many helpful people and organizations that are experienced, careful and very considerate when dealing with their clients – men like you – and the ladies.

There are also scammers among the women and the intermediary organizations. That should be no surprise because this is an area where a lot of money changes hands, people are tense and susceptible to making rash decisions under pressure of their most basic physical and emotional drives.

Realize that considerable time, energy and money will be needed to bring your quest to a successful conclusion.

You need to be sure of all the legal requirements in your country and the country where your future bride is living. It's almost essential to check this for yourself.

While the reputable organizations will guide you through the paper maze, you might approach a scammer - intermediary person or organization - first and their information would be designed to only benefit them.

When you are looking for someone to share your life, it's natural to want to put your best foot forward. But some scammers will put someone else's foot forward by providing other people's photos instead of the women's own. Many of the photos are simply ripped off sites of legitimate model directories, from magazines or even casual photos taken in the street or at the beach.

It's also important that you don't gild the lily too much. You owe it to the woman and yourself to be strictly honest.

Don't give too much information about your assets, income and investments. What's the point? This will only give more encouragement to the wrong kind of person.

Trust has to be a two-way street. So, if you find it difficult to get direct contact information after exchanging a few letters, you should be more wary.

You will have to visit your potential bride's country before she comes to yours. That will obviously be a stressful time for all concerned so watch everything but realize that she, as well as all her relatives and friends, will be as nervous as you probably are.

The possibility of scams does not end when you bring your bride to start your new life together. A few, among the thousands that arrive each year to start a new life, will have an agenda that you may not become aware of for months.

Some will want to bring their relatives to live in your country and you could find that was the most important reason for them agreeing to your proposal – more important than your life together.

You might, if you have made a rare bad choice, bring someone that is not really interested in you at all, just the privileges of citizenship in your country. This is fortunately rare, but these individuals may be prepared to take any steps to get their freedom from you – even to alleging that you abuse her!

These are the exceptions but you could meet one or two during your quest..

Please also keep in mind that your potential bride is probably under even more pressure than you are – she will leave everyone and almost everything that is familiar to her to join someone that is still largely a stranger in a country that might seem something like a totally different planet.

Try to put yourself in her situation and let that guide you for at least the first few weeks.

It might be worthwhile to check if there are any local people or even groups that have gone through this experience. Personal experience is the best teacher and you will be extremely fortunate if you can get information in advance from people that have made the journey which you are starting.

Identity Theft

Identity theft is someone using your personal information such as your name, social security number, credit card number or other identifying information, without your permission, to withdraw money from your accounts, use your credit card numbers for on-line, mail or phone purchases or other crimes.

You may believe that your reputation, your careful handling of personal documentation; credit cards, receipts and the like, will make it very hard or even impossible for ***your*** identity to be stolen.

The truth is that this type of offense is spreading rapidly. It happens to people, probably people just like you, every day.

Identity Theft scammers don't just mess with the good name and credit record of their victims. The effects of their scam can be devastating for the victim and their family. The victim may:

- Lose their current job and future employment prospects
- Be unable to get new loans or repay current ones
- Be unable to get, or keep, education opportunities, their home or cars for their children or themselves, and
- Be arrested for crimes which the scammers committed while using the victim's identifying documents and information.

The effect on the victims' health, their families and their personal and business relationships can be very hard to deal with. That's apart from the stress, resources and effort they need to repair the damage. That task can take years.

The scammers may target anyone that does any banking, buying or other financial transactions through the Internet. But, while that means of unlawful access gets most of

the media's focus, the scammers can strike anywhere that your credit card details are transferred from you to someone else!

Be aware of where your credit card is at all times – watch while it is 'swiped' through the machine at your favorite restaurant. These days, that's not lack of trust, just common sense, unfortunately.

If your purse or wallet is lost or stolen, contact your credit card providers and your bank immediately after contacting the police. Although women's purses are the butt of jokes about the amount of extra items they carry, both men and women tend to carry far to much personal information; receipts, cards, passwords – that concession to convenience can have dire consequences if the wrong people get hold of the purse or wallet.

It should be obvious that you don't pre-sign checks or put your social security number on them but many people do. Lots suffer for that lapse.

Call the credit card company if your statement doesn't arrive at the usual time each month – scammers have been known to use stolen information to contact the companies and ask them to change the address where their victim's statements and replacement cards are sent!

Within a very short time of ripping off the victim's financial and other personal details, the scammers can drain their accounts while running up their credit cards to, and often beyond their limits.

That is only the beginning because the victim has to prove that they did not have anything at all to do with the transactions and prove their innocence rather than be given the common presumption in law of 'innocent unless proven guilty'.

And, of course, they have to do this while their own finances are almost zero.

If you think that these precautions are only for the paranoid, remember that the effect of this scam can be devastating.

Sometimes the scammers activity may not show up until more than a month after the documents were stolen. Despite the warnings and publicity that this scam and its effects have received, some people have taken more than a year to find out that scammers have been accessing their funds and credit!

How YOU Should Protect Yourself:

1] Only carry those documents which are absolutely necessary

2] Monitor the cycle of your bills. Contact the billing companies if your bills do not come at the usual time.

3] Never click on links in emails which appear to come from your bank or credit provider which ask you to check, update, change or confirm your personal information such as passwords.

No legitimate financial organization will ask you for that information by email.

What VICTIMS Should Do:

As well as the specific advice in this book's various sections, here are some general points from the experience of the author, his friends with practical experience and the government authorities who compile their advisories from the results of victims complaints and subsequent court cases.

1] Ask the fraud department of any one of the three major credit bureaus to place a fraud alert on your credit file. The fraud alert asks creditors to contact you before opening any new accounts or making any changes to your existing accounts. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will be automatically notified to place fraud alerts, and a credit report will be sent to you from each of the three bureaus free of charge.

2] Close the accounts that you think may have been tampered with or which were opened by the scammers. Use the Federal Trade Commission's ID Theft Affidavit when disputing new unauthorized accounts.

3] File a police report locally. Then, get a copy of the report and prepare extra copies that you can supply to creditors and anyone else that may reasonably require proof of the crime.

4] File your complaint with the Federal Trade Commission through their website. The FTC maintains a database of identity theft cases which law enforcement agencies use for investigations. Filing a complaint also helps them keep their own knowledge of identity theft and the problems victims are having more current so that they may give you and future victims better assistance.

5] If you believe you've been scammed, file your complaint at www.ftc.gov, and then visit the FTC's Identity Theft Web site at www.consumer.gov/idtheft to learn how to minimize your risk of damage from ID theft.

Hoaxes Harm Everyone

All human beings are born with a sense of humor that develops under the influence of our environment – what we read, hear and how we are told to behave. So, by the time our bodies mature, our individual sense of what's funny and even what's acceptable will vary widely.

But, we all like jokes and stunts, like those we pull on our friends and colleagues on April 1st in many countries, or when a male friend is due to be married – or just about any time we are in the mood.

What's the Harm in a Hoax?

When someone sends an email with false information to a few friends, that might be okay.

But most people that start and deliberately spread hoax information which they know is false, try to have it spread to as many people, computers and countries as possible. The Internet is an almost ideal communication medium - for good or bad information!

We may intend no harm, but starting or passing on a hoax to everyone in our address book with a request that they do the same can cause undue pressure on the systems which transfer all those messages.

That, plus the cost of wasted work time while people read and the forward the message can, within just a couple of days, cost businesses and individuals a considerable amount of valuable time and computer system resources.

This is a highly effective method of spreading any message which costs the originator a minimal amount but that cost dramatically increases as the message is copied and forwarded.

The message can have other costs too.

Many hoaxes have asked for people to send greeting cards, business cards or other small, low-value items to sick people they name in the email. Many of the sick people may never have existed or, if they ever made a request of anybody for such items, have probably reached the stage where they are stressed out by the massive amount s of physical items or extra emails they get.

This is a totally nasty way to treat any sick person and also a stupid interference with the lives of the thousands of generous, ordinary people that respond to the request.

Sometimes, the message invokes the name of a respected beneficial organization. For instance, the well-known Make A Wish Foundation keeps a page on their site at http://www.wish.org/ detailing just some of the hoaxes where their good name has been misused.

Some hoaxes tell of non-existent viruses and other mal-ware which causes panic, more unnecessary and expensive forwarding of emails with the added risk that these make desensitize some people so that they may ignore genuine warnings.

Of course, the genuine warnings are ***never*** sent by email!

But, it's not unknown for people that create or distribute viruses through emails to use fake warnings as the message on the email which carries their virus, Trojan or other malware. Companies that sell anti-virus software usually have information about viruses and also virus hoaxes on their websites.

There are probably other sites with this sort of information. They may be reliable but some are probably hoaxes themselves.

More genuine information on this topic can be found at:

- **http://hoax**busters.ciac.org/ general information
- http://www.cdc.gov/doc.do/id/0900f3ec80226b9c (health related hoaxes)

- ⇨ http://www.pcworld.com/howto/article/0,aid,102396,00.asp Steve Bass at PC World magazine

What You Should Do

Be prepared and never, ever drop your guard.

That said, remember that the vast majority of people who you will have dealings with, on or off-line, are as honest as you or I.

Viruses and Other Nasties

It's obvious that you should have the most current version of a reliable anti-virus program and run it through your entire system regularly. But you also should have anti-spyware programs – the better ones will alert you to any potential problems on your system which your anti-virus program is not designed to detect.

Grisoft provide a free version of their AVG Antivirus software (for home, not business, use) at http://www.grisoft.com/doc/1

For spyware and the other nasties, I use and recommend SpyBot Search and Destroy from http://www.spybot.info/ which is "donationware" – pay what you can afford and think it's worth. There are versions available in various languages.

I also use the paid version of Ad-Aware from http://www.lavasoft.de/

Both these sites provide extra information and ***reliable links*** to more information and programs that can help keep the nasties out or remove ones that are already in your computer. I emphasize *reliable links* because, as well as some worthy and reliable competing programs in this area, there are other programs which try to plant spyware on your computer while pretending to check for and remove it.

One type of offer that I've seen in this area and would never accept is where you can have your computer checked for spyware or other mal-ware but must pay before the program will remove it. I am not commenting on the usefulness of the software which is sold by this tactic – I would never even download it!

Email Warning

Never, ever give out your personal information on-line directly or through emails. Emails are not a reliable method for secure transfer of sensitive information.

- Your information and comments may be intercepted during the transfer.
- The person/company which you send it to may pass it on to others without your knowledge.
- The person you send email to may not actually be the person that you think you are dealing with.

Keep Your Knowledge Up-to-date

If you want more information, your first source should be sites that you pay for with your taxes – those of the official Government watchdogs in your country.

Some of the private watchdog sites may not offer unbiased advice. This book gives you enough pointers to help evaluate whether they might be trustworthy.

There is another development which is worth being aware of. I visited a well-respected private watchdog site last night. Lots of good advice and the links seemed all to be legitimate but, among the little boxed advertisements down the side of one page was an offer to make money through joining and promoting a Multi-level marketing matrix.

There are many good Forums online but always be careful to independently verify any information or offers that people give you there.

Remember that, online, people may not be who they say they are. They may not tell the truth about their age, gender, religion, location or reason for recommending something.

Whether you are approached to launder a few million dollars or just look after a few electronic parts for an overloaded delivery man, my best advice is to say, "No" and leave.

Simple On-line Checks Save YOU $$$'s

The simple scam of offering bargain prices and vanishing with the victims' money but never supplying the products or services was quickly operating on the Internet soon after access became publicly available.

Yes, behind the impressively decorated web pages, 'sincere' testimonials and bargain prices could well be a veteran fly-by-night who has simply taken his line of chat to the whole wide (but not very wise) world, courtesy of the Internet.

There are some simple tests which you can use to help decide who is an authentic and probably reliable Internet merchant or service provider and who is, possibly, not.

Net Basics.

Run your spyware program(s) before you visit the website where you want to spend or transfer money or may have to enter any confidential information.

Always open a new browser window to visit such sites and type (by hand) the full address, which you were originally given by the organization, into the browser.

When you have finished your business, log out and close the browser window. Do NOT do anything else with the computer linked to the Internet until you have closed that window.

Never conduct any financial transfers or offer any sensitive information if you are not sure that the site is secure. One basic indicator is to see if there is a small symbol resembling a padlock in the task bar at the bottom of your web browser when you look at the supposedly secure page.

If you do not have confidence in the security of the page, ***go away***.

Search Engines

Go to the search engines, especially those which have sections that cater to your specific country - like Google. Type in the names of people, companies and products which you have seen on the sites and are considering doing business with.

Some of the links which you see will be useless for your purpose but you also will get much that will be interesting and even valuable, including perhaps snippets which the search engine bots have harvested from little known forums which focus on the sort of product, service or opportunity that the site provides. These comments may be from employees of the site, dissatisfied customers, competitors or happy repeat customers. Of course, the people posting the comments may not be telling the truth about the site, themselves or their connection with the site.

Despite these potential hazards, I suggest that you find and join Forums which relate to your business and personal interests. Keep in mind the points that I've already mentioned.

With the multitude of responses you get on each page of results from the search engine query, you will have a lot of information of varying quality to help make up your mind.

If you see the same products listed by other, perhaps better known organizations at much higher prices, the site may be offering genuine bargains but it might be worth checking further instead of just pulling out your credit card. The site's prices may only be for vaporware – products that you never actually get.

Are the products offered the current commercial versions? With software, this is especially important. As well as verifying that the program(s) will actually work, you need to confirm in writing that they will work with your computer equipment because most software cannot be returned.

Import and Other Costs

You also need to check on delivery charges to your location. These may be inflated compared to those charged by other businesses. You want to be sure of any liability you

may face for Customs and other import charges if you buy from outside your own country.

Ask your Customs Department, don't just rely on what the overseas merchant "thinks" you might be liable for. Be very cautious if the seller suggests that they have ways that will help you avoid import charges. You might save some money, but failing to declare dutiable goods and being caught will mean that you pay penalties that are often designed to not just punish offenders but deter others who might think of trying the same means of avoiding lawful charges.

Also, Customs and other Departments seem to have long memories. If you have one misdeed on your record, you won't be victimized but will probably find that all your parcels for years to come will be subject to search which means delays in receiving and using the products.

On the Net for Four Generations

If the site claims to have been around for several years, you may be able to find old copies of the company's web pages in the Wayback Machine at http://www.archive.org/

This is not infallible – it doesn't have every site through the relatively short history of the Net but you could waste hours there – it's a trove of trivia as well as important historical material.

Whois really on that Site?

Another very useful tool which is free to use is a whois database. This gives you the registration information and contact details (in most cases) for web sites all over the Net. They can also indicate if a domain name that you want to register already belongs to someone else.

Two well-known whois databases are http://www.whois.net/ and www.networksolutions.com/en_US/**whois**/index.jhtml

I prefer to have a small utility program on my computer which accesses online whois databases when I just open the program and type in the domain name I want to find out about. The one I use is Karen's Whois, just one of the free, useful and highly recommended programs (for PC's running Windows) from Karen Kenworthy at http://www.karenware.com/

Fighting Back

Some of you won't want to just walk away when you find something that seems to you to be suspicious – because of your own ethics, you'll want to hasten the scammers next appointment with the Courts, right?

Great, I'm proud of you. I'll be even more proud of you if you can keep to that course when you're threatened, accused of trying to extort money from the scammers(!) and see the cost in terms of time and resources that you will have to dedicate to your quest.

You should just keep any emails, including the headers, and pass them to the authorities, report off-line scams to the police station.

Trying to handle things yourself is just another path to grief. Leave these battles to the professionals who have the experience and resources.

Arm yourself with knowledge by visiting the Government websites but remember that having the theory is not enough to prepare you to handle matters yourself.

Scam Slang

I wasn't going to put a 'dictionary' section here because:

- ⇨ The ebook is sold World-wide through the Internet and there's distinct variations in the terms used in various countries.
- ⇨ I have no idea of the terms that are used by non-English speaking scammers.
- ⇨ I've noticed that many terms beloved of fiction writers are used less these days or the current meaning bears little resemblance to the crook's usage. One thing really surprised me – the term 'confidence trick' traditionally used for scams is now often being used when referring to tips that help you to boost your self-confidence. I'm no grammarian but I'd join the fight to stop changing a term for crooked behavior to something good, except it's already too late!

But, for completeness, I'll list many of the terms that have been used. If nothing else, they will help you to understand what the scammers and con-men in movies are talking about – most screenwriters and novelists still use the same terms from the era when 'Count' Victor Lustig pulled his classic scam and sold the Eiffel Tower.

'**The mark**' - the victim.

'**short con**' **-** a quick rip-off with no set-up or follow-up (if the scammers are successful).

'**long con**' **-** a scam where the scammers pre-plan, may involve a team of scammers and some casual help as well. This sort of scam can take days or even longer and the rewards and risks are obviously greater as well.

'**Putting him on the send -** can be part of an involved or 'long con'. The victim is sent to collect the money or other valuables which are the main target of the scam. The success of the whole scam rests on how well the victim has been fooled and/or pressured at this point. Some sheep never return to the fold.

Then, the scammers have to decide whether they believe that the victim has been so well taken in that it's safe and financially worthwhile to follow up with them or maybe the victim has not been properly hooked – they might find the police waiting if they try to contact the victim again!

'The Spotter' - befriends the victim and steers him to the scammer(s) for a reward! They're like some of those kind friends that recommend a particular used-car yard to you. Sometimes it's genuine desire to help us get a good deal and sometimes there's more of a desire to get a spotter's fee!

'Insiders' - the main members of the scam.

'Heavy' – muscle to make sure the victim comes up with the money or to quieten them if they try to get their money back or threaten to go to the police.

'Playing the con' - when the victim's new 'friend' spells out the opportunity to the victim.

'Roping the Mark' - convincing the victim to put his money or other valuables into the scheme. Sometimes the victim's new friend will take him to another scammer who is more skilled at the delicate art of roping.

'The convincer' - letting their victim make a small initial profit which the scammers are willing to risk to get his trust so that the victim is more willing to produce the much larger amount which the scammers were after.

'Pigeon' - often used by old-time con-men when referring to the victim. That's really a slur on all pigeons – they do what they do because they're hungry and probably have a family to feed but, as I've said before, the scammers' victims are almost always driven by greed and the chance of quick, often illegal, profits.

'Blow him off' - does not mean killing the victim (that's 'blowing him away'). The scammers won't risk the heavier prison sentences unless they're cornered – this means

pushing the victim away from them after they get the money – the more distance, the safer they feel.

'The Fix' - buying protection. This may be bribing some law enforcement officer(s) but can also involve meeting and paying the local criminals who could otherwise take action for running a scam in their territory.

'The Score' - the total amount which the scammers get, less expenses. From my knowledge and research, some do make a very good, though precarious living, but most would do better in a regular job if you cost in their time behind bars. The most common response about that point, for those that bother to answer, is that prison is the scammers' equivalent of college where they study hard to keep abreast of the latest techniques and make new alliances that plan more scams for when they are all released.

'Beef' – trouble, either violence or argument. The scammers try to maintain a low profile and a pleasant manner – it's good for business – but they are always prepared for physical action – much better prepared than their victims are likely to be.

Another eBookWholesaler Publication