Another eBookWholesaler Publication

Your Ezy-Internet Safety Guide

by John Williams

Proudly brought to you by

Lewis Philips signature books

Email

Recommended Resources

- **Web Site Hosting Service**
- **Internet Marketing**
- **Affiliate Program**

Please Read This First

Terms of Use

Disclaimer

The advice contained in this material might not be suitable for everyone. The author obtained the information from sources believed to be reliable and from his own personal experience, but he neither implies nor intends any guarantee of accuracy.

The author, publisher and distributors never give legal, accounting, medical or any other type of professional advice. The reader must always seek those services from competent professionals that can review their own particular circumstances.

The author, publisher and distributors particularly disclaim any liability, loss, or risk taken by individuals who directly or indirectly act on the information contained herein. All readers must accept full responsibility for their use of this material.

All the web addresses listed in this book were checked for accuracy shortly before publication. But, their ownership and content may change at any time without our knowledge.

We cannot accept any responsibility for anyone visiting any of the listed sites.

Contents

Please Read This First 2

Terms of Use 2
Disclaimer 2

Contents 3

About the Author 6

The Truth about Web Safety 7

The Biggest Problem 8

Make Your Computer Safer! 10

Keep Your Programs Up to Date 11
It's Best to Back-up 12
Check EVERY File 12
Passwords 13
Tips for Better Passwords 14
No More Passwords Lists on Paper 15

Safer Surfing 17

Don't Expose Your Friend's Addresses to Other Friends. 17

Identity Theft 19

Quick Tips to Reduce the Risks 19
Click Here for Your Private Information 21
All Websites have Rules 22
Your Information will not be Distributed. 22

Using Other People's Material on Your Web Site 23

Security Software 24

Find Something Good and Stick to it! 24
Updates and Scans 25
Pep Up Your Computer 25
Suppliers of Security Programs 26
Web Browser Add-Ons 26
Anti-virus Programs 27

Firewall 28
Anti-spyware Programs 29
Anti-malware Programs 29
Anti-spam programs 30
More Ways to Reduce Spam. *30*
Your Email Program 31
Email Programs 32
PocoMail *32*
Pegasus Mail *32*

Protecting the Family 33

Protecting Your Original Work on the Internet 34

"Free" can be EXPENSIVE! 35

Seeking Just Friends and Fun 37

"Save Money and Live Longer" 39

The Enemy – Software 40

Viruses 40
Worms 40
Spyware 40
Trojans 41
Email Hazards 41
Attachments *41*
Links *41*

Web Site Dangers 44

Please Verify Your Account Details 45
Check Your Spelling 46
Check Their Spelling too! 46
Phishing Sites 47
Under New Ownership 48

Scams Exposed 49

Work at Home Offers 49
Forward Packages – High Pay – Even Higher Risk! *49*
Easy Money Straight into Your Account. *50*

Training for a Guaranteed Job *50*
Other Old Scams in New Clothes 51
The Nigerian Scam: *51*
Lotteries or Inheritance Scams *51*
Bargain Travel Scam *52*
Email Scams 52
You can Help, but ….! **54**
Resources **55**
Helpful Websites 55
Castle Cops *55*
Phishtank *56*
Bank Safe Online (U.K.) *56*
Keep Safe – Keep Informed **57**

About the Author

I have been using the Internet and writing about its benefits and perils for about four years.

I try to explain how to use computers and the Internet as clearly and simply as possible without special terms or too much detail..

I have concentrated on giving you, as far as possible the latest available information about the threats which we must be aware of on the Internet.

I hope this book will help to guide you through the hype and sensationalism which is written about this very important subject.

I will put new and updated information on the web site that I set up to help readers of this book, http://www.ezy-internet.com/

I would also be grateful for your feedback and will try to help you if you submit any questions related to Net safety through that website.

The Truth about Web Safety

The Internet is not much different from any other part of our world.

We all face risks every day from the moment we get out of bed in the morning.

We have to take what we consider reasonable precautions to protect ourselves, our family and our work or business from possible dangers that exist in every neighborhood.

But, most of us focus on the many positive aspects of our lives – alert but not worrying about what we can't foresee.

That's also the best attitude to have about using the Internet. There's too much to gain from wise use of it for us to let our inexperience, or the often sensational media coverage of Internet scams and other problems, keep us away.

I've written this book to help you reduce the risks and improve your whole Internet experience with minimum cost and no stress.

The book covers many areas and I give you the best information that I have.

But, new problems are unleashed almost every day. And, of course, the products and services to combat these problems are improving too.

With this guide next to your computer, you'll be better protected and able to understand the actual degree of risk when new threats appear, and judge which security products might be worth your time and money.

When you need more information, use the links to organizations in the book or visit the web site, http://www.ezy-internet.com/ that I've set up to provide updates and new information for readers of this book.

The Biggest Problem

All humans have a desire to improve their circumstances – that's the drive which has brought most of the benefits which many of us enjoy or hope to in the future.

Many people are very interested in finding ways to do that with minimum cost and effort.

That's what makes people, including many otherwise upright citizens, become victims of scams on and off the Internet.

The fact is that you can "cheat an honest man or woman". Quite a few people are only honest in proportion to the risk they think there is of being caught.

Some might not report finding fifty dollars in the street if they think no-one saw them pick it up. Even more might find the offer of hundreds of thousands of (apparently) untraceable dollars from some ex-Government official in a foreign country, as a commission for a "simple" transfer of funds, irresistible.

These people probably think that there is less chance of their involvement in something shady on the Internet being traced, or that they are "small fish" that will not attract the attention of law enforcement organizations.

Those can be very costly assumptions.

Of course, there are also many people who only grab these "offers" because of the almost unbearable pressure they are under financially, often through no fault of their own.

They feel so desperate that they risk everything when a minute of clear thought would suggest that "If it seems too good to be true, it usually is just that!"

That's just one common human trait that the scammers prey on.

Another is probably the most powerful gimmick, on or off the Internet – something for nothing! Most of us are going to read what the offer is, aren't we?

Well, just opening an email or visiting a web site can cost you plenty! You need to follow the steps I'll outline here.

And, I'll show you some of the other things you need to consider in the "Free" can be EXPENSIVE! Chapter.

Make Your Computer Safer!

My first tip is to consider turning off your computer if it is not going to be used for, say, a couple of hours. It probably should always be turned off if you will not be using it for a day or more. That will save power as well as reducing the possibility of an attack while you are not nearby.

Every Internet user should have security software and a firewall.

Connecting your computer to the Internet without up-to-date security software, is like walking blindfolded down the middle of a busy motorway and hoping you won't be hurt.

Your computer and, especially, the personal information on it, is a target for destructive software like trojans and viruses, as well as scammers and other villains, from the first moment you connect to the Internet.

There are several ways that you can protect your computer and your information from being accessed or damaged.

But, please understand that no program can protect you from 100% of the risks 100% of the time.

There is always a period of time between the appearance of a new problem and the moment when security software can be updated so that it will provide efficient protection against the new threat.

That's why you have to be careful about what programs or other files you allow on to your computer.

It's also a very good idea to keep copies of your most important files in a secure location completely separate from where your computer is. You could use CD ROMs, DVDs or an external hard drive to store the back-ups.

A famous movie director was recently the target of a burglary. As well as his computer equipment and all the information it contained, the thieves also took his only back-up copy - twenty years' worth of work and memories which he'd regularly copied to another hard drive.

Unfortunately, he kept that hard drive in the same room as the computer he used every day!

Check the quality of your back-ups from time to time. I always make two copies of files that I'm using on two different brands of CD ROMs. That's probably a bit extreme, but those files can be worth a lot more than the cost of an extra box of disks to me.

Keep Your Programs Up to Date

You should ensure that you have the most current versions of all the software that you use.

This includes your operating system (Windows, Mac-OS or Linux) and web browser (Internet Explorer, Firefox, Opera etc).

It's your choice whether you permit the programs to update themselves automatically, or you only let them notify you when new updates are available so that you can decide which ones you will allow to be installed.

Some upgrades can take a length of time and may slow your use of other programs on your computer until they're finished. So, you might want to specify that the updates are done when your computer is not likely to be in use; maybe just before your turn it off and go to work or to bed.

The older versions of some programs and systems may have flaws which hackers had found and used to infect them with viruses and other malware (destructive or spying programs). That is a common reason for new versions of programs to be released.

Most updates which are responses to potential virus threats are usually free. But, even when you have to pay for an upgraded program, it's really cheap insurance and you will probably find that some other parts of the software have also been improved.

You may not be able to get assistance if you are using out of date versions of programs. Some companies do not offer any support at all for older versions after they release a major upgrade. Others phase out the amount of support

available over a period of time because it is an expense that no longer brings them any financial return.

Using current programs and keeping to a regular up-date schedule reduces the risk but it cannot ever be entirely eliminated.

I suggest that you always have your security programs check for updates or upgrades just before they start their regular scans of your computer system.

If your computer is continuously on and connected to the Internet most of the time, then I suggest that you check for updates to your security programs daily.

If you only use your computer to connect to the Internet much less frequently, then weekly updates may be sufficient.

Some suppliers routinely release their updates near the same time each week. When I see this is happening, then I make sure that I check on that day.

But, with new malware being released every day, you can never be sure that an extra, possibly vital update will be held back until the regular release.

It's Best to Back-up

It's important to back-up your files regularly and store the copies in a safe area away from where your computer is located. That provides for the possibility that if your computer and other equipment, such as external hard drives and boxes of CDs or DVDs are stolen or damaged by fire, you will be able to access your files for business or personal reasons from the off-site copies.

Check EVERY File

You should always check every file that comes on to your computer, even if you know that the supplier has a good reputation or your mother gave it to you (is she a computer expert?).

Passwords

You should have a password on your computer, preventing access by people that don't know it. That's a good start.

Many programs that you use on your computer and some sites that you visit also require you to have a password and a username.

But many people a bit lazy and they use the first things that come to mind for their passwords. That's not much better than leaving your front door unlocked, and just putting a piece of sticky tape on it.

It makes it too easy for scam artists and hackers when people skimp on this basic precaution.

If they think that your information is worth their personal attention, they can start by using any of the following:

- ✓ the name of a family member or a pet, which they might get from your website or a post on a forum
- ✓ The word password (perhaps followed by a number - 1 to 9 - which you use to make it "hard to guess"!)
- ✓ Open Sesame
- ✓ Your birthday
- ✓ ABCDE or abcde
- ✓ 1234 or onetwothree

... And that's likely to give them entry to the computers and information belonging to a surprising number of clever, but lazy, people.

This information might come to them when your wallet or a credit card receipt is stolen or copied, but most of it is probably available in the information stored on your computer. See the next section, "Click Here for Your Private Information".

Most attempts to grab passwords from websites are done with powerful, freely available software programs that make thousands of attempts automatically and rapidly.

These programs are, unfortunately, very easy to obtain.

Many viruses are produced using "virus kits" by inexperienced would-be hackers that are usually referred to as "script-kiddies". That's not a compliment. It indicates they are know-nothings that can only produce their malware from kits where someone else has already done most of the work.

Tips for Better Passwords

- ✓ With passwords, longer really is better. Microsoft recommends a minimum of fourteen characters. I would never use less than seven unless there were restrictions imposed by the security system used for a particular site.
- ✓ NEVER let your browser (or the browser of the computer you're using at work or somewhere else) store any username or password for you. Yes, people really do this even with computers that they don't own.
- ✓ Each extra letter you add could increase the possible combinations by twenty-five times. That's still not going to be much of a challenge for the hacker's brute-force programs that churn through combinations at very high rates unless you also do at least some of the following tips as well.
- ✓ Don't use common words, the name of a family member or your baseball team.
- ✓ Just using a mixture of upper and lower-case letters will improve the strength of your password, but not really enough.
- ✓ Put a couple of symbols, like "#" and ")" in there. Be a little more creative than just substituting "@" for "a".
- ✓ Use numbers and letters.
- ✓ Don't use the same password for any two sites or other access points.

Free On-line "Password Checker"

Microsoft provide a free Password Checker at this address;

https://www.microsoft.com/protect/yourself/password/checker.mspx which gives a value for the strength of the password that you enter.

I felt that the values might be a little on the high side for some simple passwords that I tried but they may be improving that software behind it, so you could find it more useful than it was when I tried it.

I appreciate that Microsoft have done this with no ulterior motive and deserve our appreciation. At the very least, everyone that tries it will be more aware of what is needed to improve their password security.

No More Passwords Lists on Paper

I have always used, and recommended, keeping a small tabbed notebook for all of your passwords and other computer information rather than storing it on your actual computer or even some other electronic device.

That's worked very well but I kept running out of space on the pages for certain sections which meant getting another book and transferring the still-current information from the old book to it. If you're prepared to do that when necessary, it's cheap and effective.

Then, I found a very powerful and low-cost computer program that is recommended by many whose experience in this area is much greater than mine.

It was a surprise when I read an unsolicited recommendation by a highly respected Internet marketing professional, who said, "I could not operate my business without Roboform." This endorsement was enough for me to get the program myself.

You can get a free copy of the program from this link:

http://www.ezy-internet.com/getroboform/.

If you only want to keep up to ten passwords in the program, then you can continue to use it without any cost. But, you will have to buy the program

for about thirty dollars after the trial finishes if you want to store more than ten passwords.

Safer Surfing

When you meet someone on the Internet, you only get the information about them that they want you to have. That may be genuine, incomplete or completely false.

For your own safety and peace of mind, you should be miserly about what personal information you give out anywhere.

It's nice to be able to tell people that you come to know through their posts on your favorite web sites about your new job, husband or baby. But, any information you put into a Forum, chatroom or other social or business site is likely to be seen by many more people than the relatively few that post – there is often a much larger group that "lurk" without posting except when they feel it is to their advantage.

Also, remember that the information that you have freely given will float around the Net for years!

Don't Expose Your Friend's Addresses to Other Friends.

Don't accidentally share addresses from your address book. Many people send copies of the same email to a number of friends at the same time.

The correct way to do this is to put one email address in the **To:** box and then put the email addresses of all the other people in the **Bcc:** box.

I have seen many emails with a dozen to a hundred private email addresses clearly displayed either in the **To:** box or in the **Cc:** box.

If any of the people that get the email indulge in spam (and there are many "amateur" spammers trying to make a few quick dollars), then your friends will start getting some unwelcome advertising mail.

The addresses will all be in all of your friends' email accounts, probably for months. If any of those accounts are breached by a spammer with a Trojan or virus, then all those addresses will be added to his spam list.

It may even appear to come from your email address if the spammer fakes the sending address!

Even if that doesn't happen, your friends will all see everybody's addresses clearly displayed on your email and know that you shared their addresses without asking. That's not good for your reputation.

Identity Theft

Like most of the tricks and traps mentioned in this book, Identity Theft is not confined to the Internet. Your information may be obtained through a bogus web site or email, but it is probably more common for the scammers to get the information from someone copying your credit card details when you use it in a restaurant or from a carelessly discarded receipt at your bank branch or retrieved from your rubbish bin!

Identity theft is devastating for the victims and their families. The money they lose is just part of the damage they suffer.

They may have all credit stopped, their cash savings, if any, disappear, and they have to prove the crime or be liable for all debts that the scammers created with their stolen information.

This may take years. It also often has serious effect on your health, business associations and personal relationships.

Almost anyone can be a target, not just people with significant assets.

Teenagers are popular targets for the scammers, because many are fairly casual about security of their information and their credit is usually unblemished.

The profits from these scams can be huge but, perhaps because of a lack of knowledge about their effects on the part of legislators and judges, legislation is not a great deterrent at this time.

It seems like some trials take longer than the sentences imposed on those found guilty.

Quick Tips to Reduce the Risks

Do not to give out your personal information just because someone asks, especially your Social Security Number or other sensitive information.

Carefully check your financial statements and all accounts each month as soon as possible after you get them. Query anything you cannot confirm. Some people find small, fairly regular amounts being charged to their credit card every month by some organization that they can't remember ever

contacting. Even $5 a month becomes worthwhile to the scammer when it's not costing them anything – and they are probably doing the same thing to many other people too!

Don't store passwords on your computer unless you use some purpose-made software that you trust.

Your web browser should not be used to store any passwords.

Never use a password for more than one web site.

Never click on a link in an email. If it is from someone you don't know and trust, be extra careful.

If it seems to be from your Bank or other financial institution, call them on the phone or visit their office to discuss the matter and check the validity of the email.

If you decide to visit the web site, open a new window in your web browser and type the address in. Check it carefully before you click the button to go to the web site.

When you finish making your transactions at your Bank's web site, wait for a message that you have been logged out and then close the window completely. Do NOT use that browser window to visit any other site or even log back into the same one.

Take the extra few seconds, close the browser window and open a fresh one.

Click Here for Your Private Information

A convenient feature of all web browsers is the ability to store any passwords that you use for the websites you visit.

Having read this far, you'll realize that storing the passwords of sensitive sites, such as your bank, anywhere on your computer is not a good idea. It's up to you whether you want to use this feature to store other passwords.

But, either way, your browser probably stores much more information about your Internet activities than you may realize. If your computer was examined by someone that knew what they were doing, it could reveal many secrets, including:

- copies of pages that you visited
- details of files that you viewed and downloaded, and even
- information about files that you deleted and thought were gone forever

There are many software programs available which you can use to remove most of this information. The one that I have, and am most comfortable recommending, is free to use. It is called CCleaner and you can get it from http://www.ccleaner.com/.

Another program worth checking out is Privacy Eraser from http://www.privacyeraser.com/

Of course, removing your usage history information and cookies from your computer will not be completely comfortable for you at first. You will have to type in your username and password for each site that you visit in the future, instead of the browser inserting them into the form instantly when you open the web page.

Your choice will depend on how much that convenience is worth for you compared to the potential risk.

All Websites have Rules

All web sites belong to someone or a business. You need to know their Terms for your use of their web site.

Most well-organized sites have a link to their "Terms of Use" at the bottom of the main (home) page of the site.

For instance, they probably require that you confirm that you own all material that you post on their site.

They may require that you give them a perpetual license to use anything that you post on their website in any way they see fit forever.

Most web sites have requirements like this but do not abuse your trust – they are just covering themselves against any possibility of action for copyright infringement.

Other sites, however, may use some material that visitors post on their sites for advertising or other commercial purposes.

You are still subject to the terms even if you didn't red the fine print. Anyway, the time and expense of fighting them later could be very high.

It's much better to check all terms and disclaimers before you decide to post anything on any particular website for the first time.

Your Information will not be Distributed.

That sounds good, but some people interpret that as meaning it's okay for the site owner to use the information you provided when you signed up for access to their web site as a way of targeting the advertisements you see on their site to your particular interests.

Using Other People's Material on Your Web Site

If you have a web site, you probably want it to be attractive and full of interesting information.

You should only put material on it which you have specific rights to use on it. That is, your own original work and any material where you have got specific permission from the person that produced it to put it on your web site.

I mention this because there are several places on the Internet where you may be offered pictures, for example, on any subject you are interested in.

Most pictures are subject to someone's copyright and many producers or rights holders will go to great lengths to protect their rights. The major companies digitally mark their pictures and can trace them anywhere on the Internet, even if they have been edited!

Always read the Terms of Use on any site where you are offered pictures or other material. I saw one site recently that said that visitors could use any pictures from that site in any way that they saw fit without attribution or fee. However, the Terms of Use required that the visitor that used a picture accept all responsibility and protect the site owner from any claim for mis-use!

Another case of "always read the fine print"!

The same caution should be used with pictures supplied in collections on CD Rom or DVD. Always keep the Terms of Use that came with the disc.

Security Software

This Chapter is an overview based largely on my own experience with programs as well as the experiences of colleagues and clients.

Most programs for which you have to pay are available in trial downloadable versions which will run with all or their most important features fully working for a period of up to thirty days so that you can test the program thoroughly before buying.

While you are using the trial version, you may not be able to access the full support options that paid-up clients get.

But, you should submit a genuine question to their support department during the evaluation period. I found that one significant difference between some of the best programs that I tried was the prompt (one to two business days during the evaluation period is fair) and understandable responses which were easy to use that I got from only a small number of suppliers.

Find Something Good and Stick to it!

Testing different programs was something I felt that I should do so that I could give you a wider range of information.

But, I advise against chopping and changing between security programs of the same type, but from different suppliers, just because one announces that it has a new, and currently exclusive, feature in the new version of its program.

Every program that you use will require some time for you to learn how to get the best from it. When you set up a different program of the same type, you're more or less back to square one and the virus threats, spam or other malware won't wait for you to catch up!

I have always run two anti-spyware programs and not had any noticeable difficulty. But, that may not work for you.

Updates and Scans.

I advise that you schedule your various security programs to check for updates and perform their system scans at different times to the other programs.

This will reduce the amount of resources which they take away from other programs that you may be using at the time these procedures are running.

Pep Up Your Computer

If you find that your computer is running more slowly than you are comfortable with, the main things for you to check would be:

- Have you cleared any unused or obsolete files from your computer system and defragged it. This may take some hours if you have not done it for a significant period, so arrange time to do it as soon as possible.
- Are there programs installed that you aren't likely to use? Just having them on the system is reducing the resources available to you and also increasing the time that the security programs require to check your computer system.
- Can you add more ram (not a larger hard drive which would just encourage you to store extra files on your computer) at a reasonable cost.

A free program that will help you to find the information which you need to answer those questions is **Belarc Advisor** which you can download from http://www.belarc.com/

Some suppliers will just quote you for the maximum amount of extra ram that your system will accept. I was very pleased when the salesman at my favorite computer store said that, while my computer had space for two more gigabytes of ram, he recommended that I only buy one because the applications that I use are unlikely to need any more.

That saved me about $120 which I was prepared to pay right then. Of course, it's likely that he'll see that money and quite a bit more because I'll

be buying most of my future computer needs from the salesman that took the long view on a fairly small sale.

Suppliers of Security Programs

Here are some of the many quality suppliers of anti-virus programs.

Avira.com Supply a free version of their anti-virus program with limited features (no email scan, for example) and two paid versions.

Comodo.com Supplies a range of free security programs and also full-powered commercial programs for medium to large businesses.

Grisoft.com Supplies a wide range of security software individually or as a suite under the AVG label. There are both free and paid versions of most of the programs.

Kaspersky.com Supplies well-respected security products.

Lavasoftusa.com Supplier of the highly respected Ad-Aware anti-spyware program. Free and paid versions available.

Safer networking.org This is the home of one of the most highly regarded anti-spyware programs, Spybot S&D (Search and Destroy). It has always been free though, of course, the developer will accept donations at his site. Available in several languages and regularly updated.

Sophos.com Powerful anti-virus program

Spyware Terminator Another highly regarded Anti-spyware program – completely free. They also offer two commercial programs; "Web Security Guard" and "Crawler Parental Control".

Trend Micro PC-cillin Internet Security 2008: Excellent suite of security programs which seems to affect computer resources less than some others.

Web Browser Add-Ons

The current version of the **Opera** web browser has a "fraud detection" feature which uses the database at http://www.phishtank.com to check sites that you visit.

McAfee Site Advisor is a free add-in for the **Internet Explorer** and **Firefox** browsers which uses their own database to check whether the sites you surf to are known to have spyware, adware, spam etc.

Anti-virus Programs

An anti-virus program searches your computer for virus programs which it has information about and also for programs it may not recognize but which show characteristics similar to programs that have already been added to its knowledge base.

Your anti-virus program will also monitor important files on your computer and check any that are changed in size at any time (a possible indication that a virus or some other malware has affected the file).

It's very important that you always have the most recent version of the program and its reference files. I schedule my program to check for updates every day, just before it starts the full daily scan.

But, if you are not using your computer on the Internet every day, then a weekly check for updates may be enough for you.

It's not a good idea to try to run two anti-virus programs on the same computer.

Some will clash and your computer may even crash. It's even more likely that the two programs could claim the other is (or contains) a virus simply because of the reference files that accompany each program.

Another problem is that having the two programs constantly scanning your machine, even just on a low priority basis in the background, can reduce the resources available to other programs you are using and slow down your work or leisure activities.

Most anti-virus programs will scan your emails as they are received or sent. This may require you to specify the path to the main file of your anti-virus program or its email-scanning sub-program when you set up your email program.

Not all anti-virus programs will do this. If yours does not, I suggest you think about upgrading it or getting a different program which is more fully featured.

Firewall

Your firewall may be a software program installed on your computer or it might be part a hardware device called a router, which you use to connect to the Internet.

A hardware firewall is probably stronger than a software program but hardware firewalls require a power outlet and may also need to be switched at times so that authorized people (technicians or employees from other areas) that do not normally use that system can get access.

This makes the system vulnerable, so you should keep them to a minimum and always run a full scan with the current version of your anti-virus program as soon as possible after the firewall is restored.

Windows has a firewall as part of the package but many people, including me, use a firewall program from a different supplier.

I was impressed with the Microsoft program and would still be using it except that I decided to try a variety of security programs of each type while preparing for this book.

I was very impressed with another program that I use, so I got the firewall program from that supplier.

You should not try to run two firewall programs on the same computer. In fact, most will check when you are installing them and ask you to switch off or uninstall any other firewall program they find before their installation can be completed.

There is no valid reason to want to have two firewalls.

The firewall program that you select will probably have in it a reference file containing details of programs of all kinds that the firewall's producers know are safe.

Your program will scan your computer when you first run it to log the programs that it recognizes are okay.

But, you will probably also have some programs on your computer that you trust that are not in the safe list. The first time that each of those programs starts up after your firewall is installed, you will be asked what action you want the firewall to take about that program.

You've got to train your watchdog and sometimes you will see similar messages where the program is asking you about may be interacting with different programs on your computer. Bear with it.

This is another indicator of the clarity of messages that you will get from the program in other circumstances.

It may also help to make you aware that there are some things going on within your computer that you are glad to know about.

Anti-spyware Programs

Spyware is a term that covers a range of programs which may produce spam or harvest your personal information including financial transactions, passwords, sites that you visit and the type of files that you download or view.

Anti-spyware programs seem to be almost as numerous as the malware they try to protect us against. Some are free but most of the others are low-cost for the important job they do for us.

These programs also need to be kept up to date.

Anti-malware Programs

Of course, the different types of programs that I've already mentioned are anti-malware programs too. But, I've seen some new programs which are called by this specific title.

The main difference that I've noticed is that they don't find and remove any sort of malware that is already on your computer when you install them. They monitor all new programs and files coming from the Internet which try to install themselves on your computer.

There's likely to be some cross-over in functions between some of these programs and, say, anti-virus programs but they are worth checking out.

Anti-spam programs

I've been happy just using the spam-reducing features of my email program but there are a number of programs that try to reduce it before it gets to you.

1. Only messages from "friends" (whose addresses you have already approved) get through with some programs. They block all messages and tell the sender that the message will be submitted for approval to you. The sender may be given an opportunity to send a brief message that you see before you decide whether to open the email.

   Some of these programs advertise the service they provide to each sender when they offer them the opportunity to send that short message to you and also when they notify the senders of messages that you approve.

2. Other programs have on-line databases of user-notified spam messages which they will remove from your incoming emails.
3. There are also programs which have definitions which they test your incoming messages against.

More Ways to Reduce Spam.

- Use the spam-reducing features of your email program.
- Don't sign up to an email newsletter unless you are sure that it will be useful to you and the supplier will not share your information. Carefully read the forms you subscribe through.
- Review all subscriptions at least every month and unsubscribe from any you don't need or read.
- One way to check whether your information is being passed around is to use different variation on your name in the subscription form;
  - Mr J Williams

- J Williams
- J (A to Z) Williams
- John Williams
- John WIlliams (yes, that upper-case "I" is deliberate)

If you start getting email from people or organizations that you never heard of, to a particular version of your address, you can be fairly sure that the person you gave that address either shared it with the spammers or that their email account has been breached, possibly by a trojan or virus.

Your Email Program

Your email program is a vital part of your equipment but many people, possibly because they get it for free, take it for granted unless there's a problem. And, they never try to use any protective or time-saving features that the developers may have spent months building in to it.

Some email programs contain functions that feature in anti-spam programs that you have to pay for but they're often ignored by many users of the email program.

One thing your email program cannot do is stop you from subscribing from lots of email lists. You may need to check your inbox every so often and unsubscribe from those newsletters which you don't need or read any more.

If it's no longer important for your personal or business interests, or you just can't spare the time to read it, save some bandwidth and disk space – unsubscribe today.

The less clutter in your email account, the easier it is to spot and remove the spam and possibly malicious emails.

Fortunately, you can see enough information in the header of the message to be confident that you can delete it without opening it.

In fact, many email programs will let you examine the headline of each message before you even download it from your email service provider. So,

you can delete it right there and it never has a chance to clutter or infect your computer!

That sort of feature is worth paying for.

If your anti-virus program is able to scan your emails, make sure that you set up the link between the email program and anti-virus programs.

Email Programs

PocoMail

http://www.pocosystems.com/ A robust, self-contained, multi-featured email program.

Pegasus Mail

http://www.pmail.com/ One of the earliest email programs, regularly updated, with a huge, dedicated user base - and it's completely free!

Protecting the Family

The Internet is a boundless and ever-growing resource of information and entertainment for people of all ages.

Most parents who have the financial resources, give their children a computer of their own, to make use of that information for their school-work and also to provide high quality entertainment.

But, they also know, from press reports and government warnings, that there are potentially serious risks in doing that.

It is unrealistic to think that you can isolate your children from the Internet unless your whole community has no access. They will get online through their school or other government facility, or with the help of friends whose parents have allowed them access.

How do you protect them from harm or bad influences?

The first requirement is to set an example that they can follow. Children will copy your actions more than your words. If you tell them what they should do but show that you don't abide by those standards yourself, you can expect disappointment or worse as they follow your example.

You should try to ensure that there is mutual trust and respect but you also should maintain a watching brief on your children's Net activities.

Put the computer in a fairly public part of your home, with enough screening that it does not interfere with other family members' activities nearby and that they don't reduce your children's Net experience.

Don't intrude or supervise but be alert for any negative signs that seem to arise from their computer activities.

You might want to install software that restricts access to sites that might be inappropriate for young children. I believe that most of those software packages are a waste of money – many children can beat the restrictions in just a few minutes and the presence of the censorious software may act as a goad for your child to do just that.

Discuss with your children media reports about the risks of Net surfing and how you and they can protect yourselves from them as far as possible.

One rule is probably the only one that is absolutely essential – they should never put any personal information on any website or in an email without discussing that with you first.

Be ready to discuss any topic or incident that your child wants to talk about. Just as you would if it had nothing to do with the Internet.

Protecting Your Original Work on the Internet

The best advice is, "Don't put anything on the Internet that you can't afford to lose."

Many people have a personal web site, and they may also have one which is related to their business.

You should realize that anything you put on that web site may be mis-used, often without your knowledge.

Some people will re-publish your words, pictures or even your whole web site as their work.

Someone might publish some of your material in another country and not on the Internet.

Your photos may be used for many purposes you never even thought of. If you're good-looking, someone may use your image as their own on social web sites!

This is illegal but laws differ in various countries. It may not be possible to get any action taken or penalties imposed. But, I've found that most hosting providers, provided you approach them in a reasonable manner and supply documentation, will act to have any suspect material removed. That could take weeks, of course.

But, you may never even know the material has been mis-used.!

Even if you find out, getting the matter put right can cost money, time and be very stressful.

"Free" can be EXPENSIVE!

There are many great bargains that you can get from the Internet but there's usually some sort of cost.

It might be money, or that you have to subscribe to the supplier's email newsletter.

Sometimes, as happens with many software programs, there is no charge but a request to donate some amount to help with further development of the program if you can.

Many things are really a gift, just like the sign says.

But, there are also many offers which don't have a price tag but will cost you plenty.

An extreme example that was reported recently happened in the real world, but demonstrated the perils of using equipment that you don't know the origin of.

Several employees of a large American corporation found small USB sticks, a storage device which plugs into almost any computer and has enough Ram to store, for example, hours of music.

Most of them did not report their lucky finds but rushed inside the building to their desk where they plugged the devices into their work computers.

I don't know what they found on their new storage devices but a hidden load – a virus – was instantly injected directly into the highly protected corporate computer system.

The company's own employees had carried in the modern equivalent of several Trojan horses and whoever planted the sticks in the area around the building was probably downloading the confidential information he wanted within an hour at a cost of a couple of hundred dollars for the almost untraceable devices.

You may not have highly sensitive corporate information on your computer at work or at home but please take this story with you and always check any

new disk or device, whatever its source, with the best security software that you can.

If you do use a corporate network, never put any program or other file on the system without explicit approval from your system administrator.

The consequences for your employer and your future employment could be serious.

Seeking Just Friends and Fun

The current boom in online socializing sites, from chat rooms to the likes of YouTube, MySpace and whatever new concept has burst on to the scene since Saturday, is an extension of something that has been a very popular part of the Internet from its first public incarnation.

People want to meet other people, many want to show off themselves, their accomplishments or something outrageous that they do and many more people enjoy watching them do that.

But, all these places harbor risks for the unwary or the over-excited.

When you first sign up and log in to the wildly popular site, you may be flattered to get invitations from many other Members to join their lists of "Friends".

It's not because they like" you, it's to increase the number of people that link to their information pages. Some, of course, could be very helpful and great fun to interact with on the site. Some may have darker motives.

Chat rooms have been the beginning of a lot of relationships. Many of them have been extended to off-line meetings with a wider range of results, good and especially, bad.

One reason for that is that people can assume any persona and almost any form on the Net. It's naturally highly attractive to social misfits and those who have little success, for various reasons, in establishing successful offline relationships.

It's common for people to use other people's pictures and even false names and other details when they meet new people on the social sites.

Some will even pretend to be younger, a different sex or whatever it takes to attract the type of person that they desire.

This is one of the real dangers for young children venturing into the Net while still forming their own values.

Experienced predators know what to say and they can, if necessary, change the voice they use to say it with freely available software.

But, these same techniques are successful with more experienced and older people too. The enticements might change but the tested tactics still work.

And, if the intended victim realizes something is going badly and backs away, the predator may try to reach them off-line and get some revenge for being "let down".

"Save Money and Live Longer"

With the ever increasing costs of medicines, many people are tempted to try the offers which flood into the e-mail box or can be found around the Internet.

But there are many risks when you take this path just to try saving a few dollars.

You may never receive any product. That can be better than some of the rubbish which some people have received and even risked their lives by taking.

Your use of the product will be entirely at your own risk. Do you know the potential side effects?

Even if you're medicine is accompanied by some directions, the person that wrote them has no idea at all of your physical state or medical history. Even if the product supplied is legitimate, you may face significant risk of a negative reaction between that product and whatever other medications that you are taking.

Of course, there is no guarantee that the product you get will have the correct strength of the active ingredients or, in fact, have any active or useful ingredients in it. That's another way that some producers increase their profits at your expense.

The source of the product that you receive is not guaranteed. Some producers have been discovered using sub-standard ingredients and very unhygienic equipment to produce products that give them the highest possible financial return.

If it's starting to sound like the cost of consulting your doctor is probably good insurance, I'd have to agree.

The Enemy – Software

Viruses

A computer virus is a program that arrives uninvited and unknown with another file that you deliberately put on to your computer.

Some viruses are not destructive but there have been some which were only intended to, for instance, put a message onto the screen, which were badly written and caused damage as great as other intentionally damaging ones!

Computer viruses can destroy or damage files on your computer even ones that are essential for your computer's ability to operate.

They are called viruses because the reproduce themselves and spread to other computers by attaching to files that you send from your computer; emails, business documents and other files.

Worms

Worms can reproduce themselves and spread through a computer network without piggy-backing onto other files. They may damage files like viruses or just seriously reduce the efficiency of a network because the rapidly growing number of copies absorbs most of the resources that are available to the network.

Even very large networks can be brought down in a short time.

Spyware

These programs capture information that is on your computer and some may record the actual keystrokes that you type, including passwords and other sensitive information.

This is then sent through your Internet connection to the hacker that released the malicious program. The effects, like theft from your bank accounts, can be short-term or long term. Some operators will set up small, regular withdrawals from your account, taking advantage of people who don't always check the details of their financial statements.

Other criminals will try to get everything that they can out of your account in short order.

Sometimes, spyware is used to gather data about the types of sites which you visit so that you can be targeted with appropriate advertising.

Trojans

These programs come on to your computer when you get a file that has been infected or produced with the trojan aboard.

They may do any of the things I listed for viruses and worms. Other trojans are designed to:

- install or exploit access points on your computer
- send spam emails through your system for which you could be blamed
- make your computer act as a relay for a "denial of service attack" where the hacker uses the resources of maybe thousands of infected computers to flood a large network with the aim of making it crash
- gathering email addresses from your system for the hacker to send infected emails to

…. The possibilities are endless and all bad!

Email Hazards

Attachments

Email attachments are a classic way of introducing viruses and other nasties to your computer.

Always scan all emails that you get and be very careful with ALL attachments even if they appear to come from people you know well and trust.

One possible problem is that your friend's computer may have been infected with a virus or trojan that is sending emails with infected attachments to everyone in your friend's email address book without them knowing anything about it!

Links

Never click on any link in an email. Someone told me the other day that he'd done that regularly for two years without any problems. I hope he never does have a problem because I've heard from technicians about serious

consequences they've been asked to try, often unsuccessfully, to repair after just one bad link was clicked.

If you get an email that seems to be genuine and urgent, grab the phone book and contact the company or person by phone or by opening a new browser window and typing in their website address (no surprise to me if that is just slightly different to the address in that unexpected email!)

Emails may be in plain text or HTML (web page) format. The text format is less likely to hold any dangers.

But, sometimes you get an email where the whole email is actually a picture. That's a technique that spammers use to avoid their words being detected by anti-spam filters that would then trash the email.

I am told that those pictures may also carry malicious code.

Web Site Dangers

One of the security program producers reported that their figures indicated that about 14% of all web sites on the Internet contained malicious software, ready to infect or harm in some other way, the computer of anyone that came there.

That's astonishing - but possible, I suppose.

There's not much chance that anybody will dispute the figure because the growth of the Internet is so rapid that the number of websites has changed dramatically since that figure was announced a few weeks ago.

And, of course, other companies will have no reason to dispute the figure – it will probably help to increase the take-up of their security products as well!

But, even if the figure was wildly exaggerated, it is an acknowledgment of the presence of a danger which few people were probably aware of – a significant number of web sites that exist only to trap and steal from visitors.

Some bogus sites are much more basic. When someone lands on them, they get a barrage of pop-up windows with advertising that can slow their computer or even stop it.

I don't know that anyone would ever buy anything that was advertised in that way but, from my own experience of an incident like that a couple of years ago, I know that there can be other reasons for the overwhelming barrage.

I went to a site that was listed in a book where I read a list of web sites that offered free or very low-cost web hosting. In those days, web hosting was much more expensive than it is now.

But the site offered nothing but garbage advertising banners. The only way I could stop them was to turn off my modem.

After a few minutes, I turned everything back on. Among the icons on my computer screen, I noticed one that had not been there before.

Most people would not have noticed it but I was a proof reader and the change in that familiar desktop jumped out at me.

It was the icon for a search program of some kind and I was sure that I had not seen it before. I deleted it through the Control Panel and ran my anti-virus program though the whole system.

It didn't find anything but, just to be sure, I reformatted the hard drive and re-installed the operating system. Considering the potential of damage from any hidden malicious software, I don't think that was an over-reaction.

Some of the malicious software in use today is very sophisticated. Of course, I am glad to report that the protective software that we now have is also much more powerful.

If you are ever caught, be sure that you check everything with a clean copy of your antivirus and other security software before doing anything else on your computer.

Please Verify Your Account Details

eBay, like almost every other large cash-handling business, is popular with scammers who send emails that ask you to go to a special, secure page and confirm your account details because of a periodic review of random accounts or some other lie.

The email is in HTML format, like a web page, and the logo and other pictures may be copied from authentic eBay web pages. I've read that some scammers may even include links to eBay's actual Privacy Policy or other relevant documents!

But, the link that they want you to use to visit the web page and confirm your details only looks like an eBay address – the one you see conceals the scammer's website address.

You should never click through any link in any email. This one could cause you to have your linked credit card maxed out very rapidly with false charges.

Your computer may be infected with a Trojan that could send details of everything you type to the scammer.

Just by visiting the site, other malware could be planted on your computer that the scammer could use to take complete control of your computer!

Check Your Spelling

After you've typed the Web address that you want to surf to in your Web browser, and before you click the button, please check that you got the address spelled correctly.

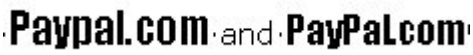
Scammers have been known to register web sites where the domain name is almost identical to a well-known web site or company. When you visit the "fake" web site, you might get spyware or worse planted on your computer, directly or through something free that you download from the site!

Or, your computer might be blasted with dozens of pop-up advertisements. I mentioned in another section that my computer was hit like this a couple of years ago. When I rebooted the computer, there was a program there which I had never installed!

Check Their Spelling too!

For the same reason, if someone provides you with a link, it could be worthwhile to carefully check it before going to the site.

For instance, these two website names;



probably look the same?

If you entered your personal details on the second site, you would be on a domain called Paypal.com instead of the well-known credit card service Paypal.com. The letter that you probably thought was an "l" in that address is an uppercase "I"!

This shows how carefully you need to check web site addresses.

Phishing Sites

Phishing sites are designed to look like they are genuine commercial sites; well-known banks and other institutions. Scammers use these sites to extract personal financial information from unsuspecting victims that are lured to the phishing site by bogus emails that also closely resemble those from the genuine companies they imitate.

I've seen a few of the bogus emails and they are sometimes almost better than the real emails. Some, however contain small errors which are a complete give-away.

Of course, people that get these emails are usually upset or excited by the content and probably don't look closely at every small detail of the design or the company information.

This type of scam is featured in the media lately but it is not new. The first reference to the practice under that name was in about 1996!

The aim is to get people to visit a web site that closely resembles that of a well-known and trusted company, and then enter sensitive personal information such as Bank account, or credit card, details and passwords.

Sometimes, the victims' accounts are cleaned out in a short time but some scammers apparently on-sell the information and there is sometimes no suspect activity for months.

The victim may not know anything about the often crippling loss until they get an account from their bank or have a credit card transaction refused because of insufficient funds.

Some sites have special code that prevents the visitor from using the back button on their browser to leave the false site.

This technique was developed by scammers to stop people from closing a browser window that was sending lots of pop-up advertisements to the visitor's computer.

Apparently, many phishing victims who encounter this trick eventually enter their information. They'd probably be better off closing the web browser completely.

Under New Ownership

When we register a web domain address, like http://www.mysite.com/ (not a real link), we have to pay an annual fee to use it.

If we do not, for any reason, pay the fee when it is due, then the domain name is available for anyone else to register and use.

Sometimes, that's a scammer who refits the web site with some malware, phishing software or maybe just lots of advertisements.

That's why should always be careful when you visit a web site that you haven't been to for a long time or have never seen before.

The site may have new owners and other surprises.

Scams Exposed

This Chapter shows just a few of the scams which plague the Internet. Many are very old but the scammers use them because they work very well.

Work at Home Offers

There are many variations on this particularly cruel scam which targets desperate, unskilled people who may really need the work.

Many of the schemes involve payments of fees and payment for stock – whatever the scammer thinks they can get away with.

Forward Packages – High Pay – Even Higher Risk!

This sort of offer may come by email, through a discussion group set up just to recruit victims or on a respectable-looking business web site. They want people to accept delivery of goods by post and forward them to overseas addresses.

They reasons vary. All are carefully rehearsed and scripted to sound convincing. They may, for instance, say that the suppliers of the goods will not post directly to their country.

You have to provide Bank account details and other personal information.

The pay probably seems generous. It needs to be large enough to hook people so hard that they don't even think, "Why are they willing to pay anyone that much? Why me?"

One reason is that the goods are stolen, so their potential profit is very high.

There is real danger here – the operations I've read about were believed to be linked to criminal organizations.

But, there is also a strong possibility that you will be arrested on multiple serious charges – you may be the only part of the racket that can be located easily and, of course, the parcels can be traced, within your country at least.

The addresses and any other information about your overseas contacts will probably be useless. They'll quickly move and set up somewhere else at the first indication of trouble.

That's likely to be when you are arrested or interviewed by the police.

You would find it difficult to convince anyone that you thought the whole deal was legitimate.

As if the charges about stolen property and mis-using the mail service weren't serious enough, you will probably also attract attention from the Tax Department if you don't declare the payments.

Easy Money Straight into Your Account.

A variation of this scam is to get people to receive cash payments into their own bank account and then send the funds, minus a generous commission, to the scammers overseas.

It's called money laundering.

People that do this high-risk activity are called "money mules".

That's not actually fair. Real mules are fairly smart.

You don't really think that someone who has a legitimate need to frequently send large sums of money overseas cannot do it except by contacting someone like you after stumbling on to your name on a Forum or elsewhere on the Internet?

Of course not! Neither will the police.

Training for a Guaranteed Job

They want you to pay for a course of training with work guaranteed after you complete your course.

You may never get a pass mark in your course or they may just disappear after you pay them for the course.

No-one can guarantee work on this basis and the amount that they say you can earn is probably much above the rate which is being paid in your area for the type of work.

Check with local sources what people doing similar work are paid, what training they need to do and, especially, whether the course you are pressured to buy is a recognized form of training by employers.

You may also have to buy equipment or materials for use with the course.

The price that they will charge you will be much higher than you can probably get the materials locally.

2] Assemble craft or other items and the supplier will guarantee to buy them back so you make a generous profit. However well you make the items, they won't pass the supplier's "quality inspection" or any other excuse they want.

They're in the business of selling kits to people like you.

You can probably find similar items, professionally finished, on sale in local stores for less than you pay for each of the items in your kit!

Other Old Scams in New Clothes

Many of the classic confidence tricks have been transported on to the Internet where they work just as well.

The scammers may run less risk operating through the Internet. The different laws in various countries and the failure of some countries to adapt their laws to deal with Internet crime in any meaningful way may make successful prosecution much more difficult and costly.

The scammers are also able to attack a rapidly-growing number of potential victims, already numbering in the millions, at very low cost.

The most common on-line scams would all be familiar to law enforcement people of-line. They include;

The Nigerian Scam:

Somebody you've never heard of wants you to help them transfer a very large sum of money from their country to yours. They are willing to pay you a small fortune for your generous help and the details of your bank account.

Lotteries or Inheritance Scams

You are notified that a relative you never heard of before or a lottery that you never entered has produced a significant financial windfall for you. You need only to provide either a few hundred dollars "search fee" or details of your bank account, or both, and you'll be in line for a great surprise!

Bargain Travel Scam

The scammer offers a highly sought after trip at a bargain rate.

You are charged add-on fees for almost everything that would make the trip worthwhile and may be subject to conditions in the fine print that means you decide not to take the trip.

However, if you have signed up and any Government enforced "cooling-off" period is over, then you'll still have to pay and that's all profit for the operator who doesn't even have to provide the basic trip!

Email Scams.

All the old mail scams are still used, but on-line scammers don't pay anything like the cost of posting a letter, if they pay anything at all, for each message they send.

Many scammers send thousands of spam emails each week and only need a very small percentage to respond for them to be in profit.

Some people think that spam is a nuisance but not a problem.

The truth is that spam is a major problem. The amount of spam circulating now is choking the Internet and reducing the resources available to legitimate users. And legitimate users pay for ALL of it through our hosting and Internet access fees.

It also re-enforces the negative impression that many people have about almost all Internet businesses.

Governments sometimes try to deal with the spam by placing restrictions on our use of the Internet and some have even suggested that every email should have to be paid for.

A lot of spam is sent through security holes on computers that belong to innocent people. They may have their accounts closed. Their reputations will suffer too. Proving to the satisfaction of their Internet Service Provider that they are innocent of any deliberate wrong-doing will be time-consuming and possibly expensive.

That's why I recommend that you get good security software, keep it up to date and make sure that you set it to scan your system regularly. It might be inconvenient but it's much better than having to explain a flood of spam that appears to have originated from your computer and email account.

Spammers would probably close their email accounts when the bills were due to be paid.

You can Help, but ….!

…. this is no job for Don Quixote!

When we hear of someone that has had their identity or their life savings stolen through Internet fraud, many of us feel a surge of rage and, perhaps, disgust.

If you have any idea of righting wrongs on the Internet through direct action, think twice and then think again, please.

The danger, and also the costs in time and disruption of your business activities and personal life that could happen, make it a high-risk route with little chance of success.

Leave it to the professionals, many of whom are also under-resourced and heavily pressured - but at least they get paid.

By all means provide financial or whatever other assistance you can to the organizations I mention in this book, send any information about online fraud or other illegal activity to your local or federal authorities and perhaps try to vote for politicians that know and care about those of us who work and play in the Internet beyond YouTube!

If you have verifiable evidence of scamming or are concerned that you or a close family member may be a potential victim, contact your local law enforcement, your Bank or other financial institution or consider asking for information from the Helpful web sites that I've listed in this book.

Resources

Virus Bulletin: (From their web site) "Virus Bulletin online magazine and website provides users with all the information they need to stay current with the latest developments in the anti-malware and anti-spam field."

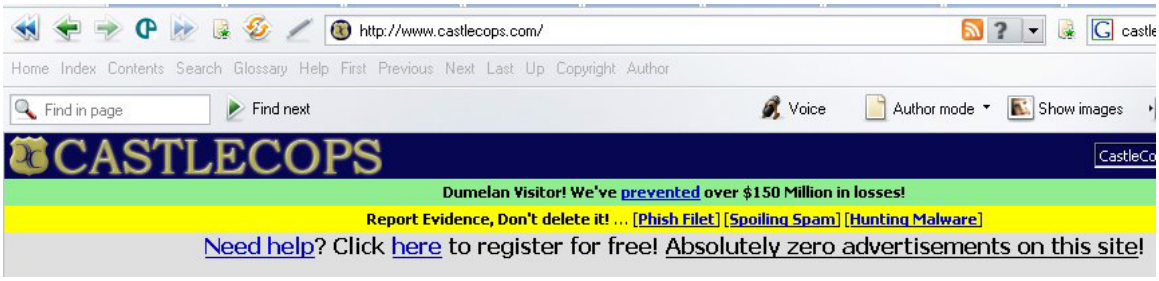
It provides annual reviews and ratings for security software and a newsletter, which could be useful for the casual visitor and also much that would be valuable to people involved with their company's computer system.

You need to register and subscribe to the free newsletter if you want to access a lot of the material which is, I think, fair enough.

Helpful Websites

Castle Cops

http://www.castlecops.com.



(From their website) CastleCops® is a volunteer security community focused on making the Internet a safer place. All services to the public are free, including malware and rootkit cleanup of infected computers, malware and phish investigations and terminations, and searchable database lists of malware and file hashes.

Education and collaborative information sharing are among CastleCops highest priorities. They are achieved by training our volunteer staff in our

anti-malware, phishing, and rootkit academies and through additional services including CastleCops forums, news, reviews, and continuing education.

CastleCops consistently works with industry experts and law enforcement to reach our ultimate goal in securing a safe and smart computing experience for everyone online.

US-Cert

http://www.us-cert.gov

This USA Government site has reliable and timely information about recent security alerts and tips for protecting your computer.

Among the newsletters which anyone can subscribe to for free is one specially focused on non-technical users.

Phishtank

http://www.phishtank.com/

This site was launched in 2006 so that people could report phishing web sites, set up by scammers to look like the official sites of companies such as eBay, PayPal or various banks.

Bank Safe Online (U.K.)

http://www.banksafeonline.org.uk/ was set up by Banks in the UK as a web site where customers could get and submit reliable information about Internet scams that might affect them.

Keep Safe – Keep Informed.

Almost every day, a new virus is unleashed on the Internet and several new or revamped scams are exposed.

I hope this book helps you and your family to be aware of the types of risks that are around you when you use the Internet.

The benefits are so great for education, business and increasing understanding between people around the World that we can't let the scammers ruin it for us or, especially, our children.

John Williams

http://www.ezy-internet.com/

Another eBookWholesaler Publication