Another eBookWholesaler Publication

Your Ezy-Internet Safety Guide

by John Williams

Please Read This First

Terms of Use

You must not distribute any part of this ebook in any way at all. Members of eBookwholesaler are the sole distributors and must abide by all the terms at http://www.ebookwholesaler.net/terms.php

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

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!