Another eBookWholesaler Publication

Proudly brought to you by

Richard Tong

Email

Recommended Resources

- Web Site Hosting Service
- Internet Marketing
- Affiliate Program

Please Read This First

Terms of Use

No alteration by anyone to the appearance, format or content of this ebook as supplied by eBookwholesaler is allowed. This Electronic book is Copyright © 2013 eBookwholesaler. All rights are reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted by any means; electronic, mechanical, photocopying, recording, or otherwise, without written permission from the copyright holder(s).

You must not distribute any part of this eBook in any way. eBookwholesaler Members are the sole distributors and must abide by the eBookwholesaler page for Terms of Use. No-one may offer or distribute this book through eBay or any type of auction. This book is published by eBookwholesaler and no-one else may claim to be the publisher.

Disclaimer

The advice contained in this material might not be suitable for everyone. The author got information from sources believed to be reliable and from personal experience, but does not imply nor offer 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 act on the information here. All readers must accept full responsibility for their use of this material.

All pictures used in this book are for illustration only. No link or endorsement between the people pictured and the book, author or publisher is implied and should not be assumed. All pictures must not be used for anything else without the rights holder's prior written permission.

Images © 2013 Jupiterimages Corporation, a Getty Images company.

Contents

About the Author

Drew Gawler decided to write this book to help people learn to use the power of the Internet to enrich their lives and, at the same time, avoid the tricks and traps which are causing so much fear and loss.

Drew said, "The Internet has been described as the new "Wild West" – many wonderful opportunities and benefits and also lots of risks to avoid."

Drew's focus is to help you become a better judge of the offers and claims which you see so you avoid the traps in the future.

"A lot of the tricks used on the Internet to take people's money and other assets are variations of old schemes with updated technology."

"Many use the same psychological tricks that con artists used years before the Internet was even invented."

"Because of the new technology, the damage can be more devastating and harder to prevent than in earlier times."

"No-one is completely safe on the Internet. But, I'll help you to reduce the risks and worry which affect so many people when they or their family members use the Internet."

My book will help readers to protect themselves and their families from a lot of the potential harm and get better results from the Internet for years to come."

Introduction

The rapid advances in technology are providing new options for our business activities and entertainment at an incredible rate.

We can be amused, informed and debited more easily, faster and (sometimes) cheaper as well!

With all the advantages, there are also more risks.

We can be robbed, have our reputations ruined, our children bullied and our actual identity stolen.

The only sure way to minimize these dangers would be to close down our computers and opt-out of using the electronic highway for handling bills, buying goods and much more.

That's not an easy option. Some businesses and governments have moved a long way to abandoning paper forms and postal mail.

And, staying off the Internet will not be enough to protect you completely from theft of your money, reputation or even your identity.

My ebook will help you to become aware of many of the tricks and traps and show you what you can do.

It gives you unbiased information and resources which you can use to keep up with the latest news in this rapidly changing landscape.

I focus on those areas which affect families and individuals. These include scams, stalkers, I.D. theft, bullying and many more topics you need to know about.

The aim is to inform you and help you to advise and protect your family.

I've included information about some of the risks you face in everyday life, even when you are not connected to some electronic device.

Many of the scams were used in simpler forms before the Internet was available to the public. The scammers have just adapted to the new technology. They have plenty of stolen money to do that by acquiring the latest technology with. Law enforcement does a great job but they often have limited funding and other restrictions which don’t affect the scammers.

The potential risks have increased every year with the development of new devices.

My aim is to give you a better chance of dealing with current threats and be able to recognize new ones when they come along so that you and your families will be able to take full advantage of the new technology.

Drew Gawler

Family Fun and Fears

When families had only one computer, it was fairly easy to supervise the children's activities and minimize the risks.

It is much harder now because it is considered essential for children to have access to their own computer or other device so they can keep up with the workload in the modern curriculum and be on an equal level with their friends and other students.

Almost every child has their own computer or smart device. Those who don't usually have access to one at school at least.

They are also likely to use computers or powerful phones and other devices when they are with their friends at their homes or the local library.

Every parent needs to be aware of and try to understand the systems which their children have access to.

If you are not already comfortable with using at least one modern computer system, I suggest that you take lessons with a community college or some other organization so that you can understand the opportunities and risks which your family members are exposed to.

A "family digital usage policy" is a good idea.

Start the discussion as soon as possible.

You need to set rules before your children start using a smart device or computer.

You will have to:

Keep learning about new technology and sites. If you don't, your tech-savvy kids could get their information outside of your home and your inpuit would lose any value.

Make them aware of problems which could occur if they share information, pictures and opinions online. "Stranger danger" is a bigger problem online because anyone can pretend to be almost anybody else!

Keep your family's lines of communication open. Be prepared to discuss whatever they want to talk to you about without being too judgemental. If you are just giving commands all the time, they will tend to go elsewhere with their problems and may not get good advice.

Be aware that the only control you have over their internet usage when they are away from your home is the values you have demonstrated to them and the information you have given them.

Check or limit their access to sites, at least until you've reviewed them. Reading each sites Terms and Conditions could be a full-time job. A rule of thumb is that better sites usually have the easiest to understand T and C pages.

Keep up with information about changes in site policies. This can be hard because many sites don't publicize all significant changes.

Acknowledge their successes and support them when they need it. Nobody does everything perfectly all the time.

Kids are Prime Targets

Computers are becoming essential entertainment and learning equipment for even the youngest children as well as everyone else.

This generation is rightly called, "digital natives". They were born into a world where digital equipment is common-place. Even those who cannot get their own computer or smart phone are well aware of what they are and their capabilities.

Earlier generations had to adapt to the increasing flood of technology. It was made even harder because some devices which were released one week might be superceded the next!

Some parents use them as electronic pacifiers just like they have used cartoon programs on television for several years.

And, many professional educators are recommending that they use the devices to teach their kids much earlier than has been done in the past.

That sounds great. But, the growing flood of new material puts enormous responsibility on parents and everyone else that cares for children.

We need to protect and help them to deal with the risks as they take advantage of the opportunities which are becoming available.

Marketers have been quick to get into this area. The parents get advice and entertainment for their kids with small messages from the sponsors.

The risks are starting to multiply even faster.

Children, and many parents, often don't know the level of the danger which they might encounter when they share information and photos on the Net!

We must understand that any photos and other material which go online are no longer fully under our control!

Anything put on a website is subject to the Terms and Conditions which the site owner has put on it. Many sites try, in their Terms and Conditions, to claim ownership (usually described as "permission" or "license") to use the material in any way, anytime and anywhere they see fit.

Some just want to be covered against claims that they are misusing the material if they display it on their site. Others may misuse it.

Even if the site owner does their best to protect the material, it can usually be copied and misused in a number of ways without you knowing anything about it!

Personal photos may be used in ways you would not want to happen. Your family members' personal information, even their identity, may be grabbed by some scammer.

Some parents are very casual about sharing information on Internet forums and other sites where they connect with other parents to swap advice and support.

Remember that people may not always be who they say they are and their advice may be tainted by underhanded motives.

Risks for Older People

Scammers have no scruples. They will take what they want from anyone at all without a second thought.

Older people can be particularly vulnerable. They have less knowledge and experience of computers and the Internet.

The same benefits that we get from using computers attract older people who have even less knowledge of them than us.

They can gather information for hobbies, keep in touch with friends and distant family members, improve their skills or just use the computer for amusement.

You can help them a lot by sharing the basic safety information here and supporting them if they have difficulties at any time.

Many older people can be capable computer users if they get some patient help and support.

Many are concerned about the learning required and the potential risks.

But, the biggest problem is usually being unable to find the necessary support.

If you are helping someone to learn the basic steps of using their computer, find a program which relates to one of their hobbies or other special interest.

That can increase their enthusiasm and get them started.

Make them aware of potential problems. Be patient with their questions and recognize their progress.

Disposing of Your Old Computer

In past years, when we upgraded to a new computer, we may have tried to sell the old machine and, if that didn't work, give it away to a friend or some charity for free.

Few people gave much thought to the personal and even business information which might be still stored on the hard drive or disks which we got rid of at the same time.

Many people probably only did a basic delete of all their personal files and then handed it over.

Most businesses would be more careful.

All the disks would be destroyed.

Then, they would have everything on the hard drive over-written with meaningless symbols many times so that, theoretically, the new owner could not get any of the information about the business from it.

But, there were companies which offered to retrieve information which was on hard-drives which crashed. This was an expensive service but worthwhile to many businesses and even individuals.

If there were methods to do that, you can be sure that some people would use those systems to try to get commercial and personal information from discarded hard drives.

You cannot be sure that no-one can get any the information on the hard drive of any computer you give away, even when you have used some program to overwrite it several times!

With the sophisticated retrieval systems available now, the only way to remove that possibility is to make sure that the hard drive is physically destroyed!

Using a sledgehammer is better than trying to scratch all the surfaces.

It is a risky procedure, so I advise you to get someone with appropriate experience and all the necessary professional-quality safety gear to do it for you while you watch from a safe distance.

If you have old CDs and DVDs containing personal or business information, you can get shredders which will slice them into pieces. Scraping the recording surface off them might be another way to make them unusable.

Wear strong gloves and quality eye protection when doing anything like this.

Also make sure that no pets or children are anywhere near the area.

Keep an Eye on Your Credit

Your good name is important but, in the current economy, your credit rating is also a critical factor in how you are viewed and treated by others.

Your credit information is very valuable but many people treat it without due care.

Depending on your bank's or anyone else's system to protect your information and savings will not be sufficient unless you stay aware of the risks and act on any sign of potential trouble.

Don't click on any links in emails which appear to come from your bank or other financial business.

The best way to contact them is through a phone number which you already have on file or by going to their office.

Scammers can make very clever imitations of Business sites which are designed to load malware on your computer and extract your most valuable private information.

If you think your computer or your information has been infected, call your Bank or other service immediately.

Credit Bureaus

The three main Credit Bureaus in the U.S.A. are **Equifax** (http://www.equifax.com), **Experian** http://www.experian.com and **TransUnion** http://www.tuc.com.

If you are in the U.S.A., any application you make for credit will be checked through one of them.

You will realize that the accuracy of their reports can be significant to you. The rating you have in those reports can affect many parts of your life.

Credit and insurance providers, as well as employers, real estate companies and even landlords can access all of the information to use when making a decision about an application you make to them.

Under current legislation, you are allowed to get a copy of the report on you from each company once every twelve months without charge.

You will find their web addresses in the resources chapter of this ebook. You can apply there or through the phone numbers on their websites for a copy of each report and review other information they want you to know.

They each have their own procedures but they are not difficult to understand or use.

Always apply directly to each of the Credit Bureaus for your copy of their reports on you. There are companies which will do this for you but its easy enough for you to do yourself.

After all, you don't want more people than necessary having your permission to access it.

These third-party companies could not stay in business if all they did was offer a free credit report to anyone that contacted them. They have to have some way of paying for their staff and advertising. Many of the free reports are attached to expensive and unnecessary services which you may not realize you signed up for!

Instead of getting the three reports at the same time each year, you might prefer to apply to a different company every four months.

This will give you access to updated information every four months instead of once every year. That gives you a better chance of seeing any potential problem more quickly.

If you are preparing to make a major investment, such as buying a house, you should get the most up-to-date credit report you can a few months before starting the process.

The credit reports are a prime target for Identity thieves. They would be a gold-mine of information to them!

Always carefully check the section of each report which lists who has enquired about your report.

If there are many enquiries from organizations you don't recognize, they might be trying to get your information for criminal purposes.

The information which is used to update the reports comes from businesses which you deal with.

Each agency has its own system for evaluating the information and preparing their reports, so there can be variations between the rating you get from the different companies.

These reports are available to many more people than you might expect. The reports you get should list everyone who has applied for your report in the previous twelve months.

Mistakes and Omissions

If you find that there are mistakes in the report or believe there is important information omitted, contact the agency which issued the report as soon as possible.

You may feel upset if you see some information you believe is incorrect and become worried that it might hurt your credit and reputation. But, take a few breaths and always be polite and professional when you contact the Bureau to seek a correction.

Each of the Bureaus have details of how to ask for corrections listed on their websites. Make sure that you follow them closely so that your request can be processed promptly.

They are allowed about seven weeks to evaluate your input and respond.

Keep copies of all emails and make notes of any conversations with them.

Children's S.S.N's at Risk

In North America, our Social Security numbers are rightly treated as very important.

They are very attractive to all sorts of scammers. But, possibly the most valuable are those belonging to children.

Most Americans apply for their child's S.S.N. before they leave the hospital where they are born.

They either tick a box on the Birth Registration Form at the hospital or apply through the local office as soon as they are settled back at home.

This is important for many reasons, including being able to include the baby as a dependant on their next tax return.

But, many parents are completely unaware that their children's Social Security number is the type which is most attractive to scammers.

The child's record is bare and, if the crooks get the number, they can get very creative.

The crook can misuse the information to set up accounts with a few businesses, paying cash for everything and using the child's S.S.N. with a false name and birth date.

They will set up more accounts with this information, paying cash each time.

At some point, they will use that good reputation to get as much in the way of goods, cash or a significant loan against the false account and then disappear.

The money cannot be recovered unless the crook is caught with the information about the S.S.N.

The child probably won't know about the defaults logged against their S.S.N. until they apply for a job, loan or some other important occasion many years after the scam happened.

Because years have passed since the scam was done, it can take months to sort out the mess. This may mean the child is unable to take up the opportunity which was available to them.

There are moves being considered by the Federal Government to ease the requirements for children up to the age of 13 (and possibly 18) to get new S.S.N.'s where fraud had occurred without their knowledge.

Sometimes, the fraudster is someone close to the family. The child's parents may even be the culprits in many cases!

Parents can check their child's credit reports with each of the three major credit bureaus (listed in the resources section) in a similar way to checking their own.

Each Bureau has its own requirements about how to apply and there may be a small fee involved for each one. But, it is worth taking the trouble now so that you reduce the chance of your child getting a big, damaging shock when they reach fifteen or eighteen and make that first important application!

Not so Smart Phones and Users

The popularity of smart phones is still rising as more features are added and prices become more attractive.

The risks are obviously comparable to those when using computers but the majority of users seem to be more careless about protecting their devices and the information which they have on them.

Protecting your phone and your information is much less trouble than trying to repair the damage which its loss could cause you.

Review the available systems and software for protecting your phone and get whatever fits your needs and your budget.

Remember that your device needs to be protected from people being able to access the data and messages which you share with other people. That is often done without having physical access to your phone.

If you use a publicly available Wi-Fi system in a coffee-shop, library or other place, you need to stop anyone being able to copy your information or install malware on your device.

Ask your supplier for information about the latest software or the devices' inbuilt protection.

Bluetooth Blues

Bluetooth connections are very popular with data thieves. Make sure that you set your device to be "not discoverable".

Turn off Bluetooth when you don't need to use it.

Be very wary about installing Apps in your device. Get them only from the confirmed reliable source, such as your Bank or the Apple App store.

Many third-party sites offer apps for free. The problem is they may have malware which can extract your information and photos from your computer or device and send it anywhere on the Net.

Protecting Your Accounts

Don't Share Your Access Information

People are either too trusting or unaware of the potential losses when they share their account information too widely.

You and your partner probably have joint access to some accounts. That's obviously a good idea.

But, many people have been hit heavily by charges to their accounts made by their children.

This can easily happen when you let them use your device to access sites where you have accounts that have some form of "Instant Payment". Before giving your children access, make sure that Instant Pay is blocked or removed entirely.

Use Strong Passwords

Keep in mind that your passwords are a vital factor in protecting your finances as well as your personal and professional reputation.

People know they must use passwords but seem to believe any passwords will do. Surveys confirm that "password" is one of the most commonly used!

Some basic steps are to:

- **Use long passwords:** Eight characters should be your minimum, fifteen is better.
- Use a combination of letters, symbols and numbers.
- Never use the same password for different things.
- Make major changes to all your passwords regularly.
- If you think you can't remember them, use a program like Roboform. You might also have a paper notebook or a file on a USB stick (password protect it!) and make sure no-one gets access to it.
- Ensure that whoever will administer your Will knows how to find it.

They don’t need a personal copy. That would be awkward because you will be updating the passwords often, won’t you?

Facebook and other Friends

Your ability to protect your details from being shared or harvested online is becoming less almost every day.

The time to decide what you will share regarding information or opinion is before you put it anywhere online. Once it is on a website somewhere, you have started to lose control of it.

Facebook is a hugely popular social network platform where you can interact with old friends, new possible friends and a lot of people who you would not want to become friends with such as scammers, identity thieves and other low-lifes.

Facebook claims to make serious efforts to protect your privacy by shielding important details, but their business model is based in part on collating information about their users for advertisers and others who pay them!

They provide ways for us to select what may be shared with which defined groups (friends, your network and possibly other categories).

Access to some of the most personal information can be restricted through a simple update. But, you also need to change or remove access to your information if your relationship with someone who was already a friend of you on Facebook should change significantly.

You may want to use a contraction of your real name or even a different one and a photo which cannot be used to clearly identify you because those two items are available to anyone that searches for you on Facebook – anyone at all.

Those entertaining and useful apps which you get may also have access to some of your information. You should carefully select the options you are comfortable with in the screen which each app must display before it is installed.

You can change the setting for who can see the information your app collects at any time after you start to use it but, people who had access will not lose the information you have already shared with them through the app.

Most importantly, there are frequent changes to their privacy-related rules and settings. It is up to you to check regularly and ensure that any information you provided at some time has not been compromised.

Useful: You might want to check out the free search engine **Duck Duck Go** http://www/duckduckgo.com/ I use this service as well as the more well-known search engines because it does not track your information.

Privacy Support Programs and Services

The sites listed below offer programs they claim will help you maintain your privacy online. I have not evaluated the sites, offer no endorsement of them and have no commercial connection with any of them.

Abine.com http://www.abine.com/

They offer DNTMe (Do Not Track Me) which blocks many trackers.

This free program is compatible with both Mac and PC on Internet Explorer, Firefox, Chrome, and Safari browsers. The company also offers paid programs with more features.

AdBlock Plus http://www.adblockplus.org/

This free product blocks banners, pop-ups and video ads on most sites including Facebook and YouTube. Used widely to help protect web surfers' online privacy.

Privacy Fix http://privacyfix.com/start A free privacy dashboard which you can use to limit your exposure on Facebook, LinkedIn and Google.

Caution - Before you download or install any program which claims to assist protecting your Privacy and/or security:

- Invest some time in checking its reputation and credibility.
- Start with the provider's own web site.
- Check their Privacy policy.
- Do a search for feedback, both good and bad.

Don't go to sites which you do not know and trust. Stick with major news organizations and those recommended by experienced people you know have visited them.

Paid endorsements: Many sites which offer reviews of any kind of products depend for their income on commissions they earn from sales of those same products which are made through links on their sites. Reputable sites will tell you about any such relationship they have in their Privacy Policy.

Check whether any program you decide to download or install on your computer will work with your preferred web browser. Some websites will recognize the browser you are using and immediately offer you the correct version.

Ask questions and resolve any doubts you have before downloading or installing anything from the Net.

Always scan anything you download with your Internet Security and anti-malware programs.

Also, check whether the browser you use has its own Do Not Track option. Internet Explorer version 9 had it. If Microsoft has it in later versions, you can be sure that most other web browsers will offer it in their new versions to stay competitive.

Even when your browser has that option, look at whether it gives you a comparable level of protection to those offered by the programs from other companies.

Always make sure that you have your antivirus and anti-malware programs up-to-date and operating.

Phishers are Mean

Phishing is one of the most common ways which crooks use to get valuable personal financial information from us.

They send emails with messages supposedly from Government or financial services asking the receiver to access a web site and update their information.

The sites are fake versions of the real organization's site but putting your details on it delivers the data to the crooks.

Most of these sites also infect our computers and other devices with malware of various kinds.

Some malware records everything we type into the computer from that point onward and transmit the keystrokes to the phishers.

Other malware gives the crooks access to data on our computer or lets them control our computer for use with thousands of other enslaved machines when they try to overwhelm the defenses of major companies or government department sites in "Denial of Service" attacks.

But, phishing is focused on collecting our information so they can drain our bank account, run up bills on our credit and take our identity.

Don't Get Hooked

You cannot eliminate all misleading emails from your inbox but these suggestions will help you reduce their number.

Don't share your main email address with more people than absolutely necessary.

Use temporary addresses for casual emails to people and businesses which you may not contact again. Then, stop using that address and start a new one.

Don't use your full name in your emails. Keep some details private as your full name is commonly used as an identifier with your bank and other important organizations.

Only give your date of birth to the most important organizations and people in your life. This is another identifier used by financial and other major companies.

But people frequently share it with every forum, chat-room or other web-based group they join. Most only need it if they offer material which may not be appropriate for children (a legal requirement in most countries).

So, you might use the correct month and year but choose a different day (1^{st} instead of the 11^{th} or whatever).

Don't ever click on an email address conveniently included in any email you get. The actual link may be disguised and the links may go to somewhere other than the site of the organization which apparently sent the email.

Most responsible organizations don't include emails which are linked in their emails. Some still do because they say it increases the number of replies they get!

But, you take a risk which could cause you great harm.

The sites will look similar to the real one.

Some pointers to it being a fake may be:

- It may not have https: in the link, just the less secure http:
- It may not have the small picture of a lock which indicates the site uses S.S.L. (Secure Socket Layer)
- Spelling mistakes and poor grammar are warning signs too.

If you go to a site which you realize is fake, you could already have malware deposited on your computer.

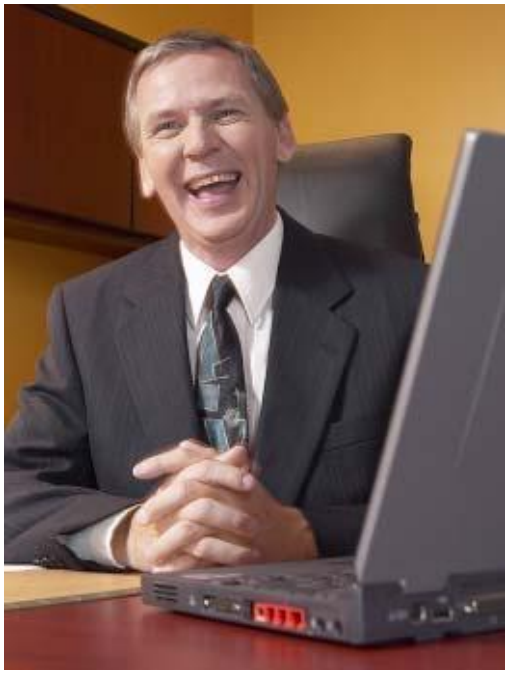
You should shut down your computer and do a thorough scan with our anti-virus and malware detection programs.

When you do visit financial and other sites where you use important personal or business information, always log out when you have finished using that site.

Then, close that browser window and open a new one before connecting to any other site.

Use the navigation on the site while you are there instead of your keyboard arrows or touchpad, etc.

Computer Tips.



Using security software whenever you visit the Internet is essential.

But, there are a huge variety of programs and apps offered.

I cannot give definitive recommendations which will suit every reader.

So, I will share my most important tips for reviewing and selecting the programs you need while reducing the risks of selecting and paying for products which might not deliver the results you want.

Keep your Computer Clean

Don't let old files clutter up your computer.

They can slow down the computer to the point where it becomes inefficient.

They increase the time needed for essential maintenance and security scanning. This is bad enough with the regular scans but is a major problem if you need to do a speedy full scan because you think you might have a virus or malware on your computer.

Keep your Programs Up-to-date.

Make sure you use the current versions of your programs, especially those related to safety and security, including your web browsers.

Older versions may have security flaws which could let hackers and other crooks put malware or viruses on your computer.

You might try **CCleaner**, a free program for Windows computers from http://www.piriform.com which will remove some of the clutter.

X Free Scans of Your Computer or Device

Many websites offer to scan your computer for viruses and other nasties without charge.

These offers usually *do not* include fixing any problems which they report the scan found.

They just provide you with a list of risks which they say were found and ask you to buy the product they sell to fix the problems.

This can appear highly misleading and a waste of time if you did not intend to buy the program.

The biggest risk is that you have to install their program on your computer just to do the "free" scan. This might allow the supplier to install malware, which could include viruses or key-loggers, at the same time.

Family Safe Browser

AVG is a long-established supplier of Internet security programs.

They offer a family-friendly browser with safety and parental control features.

There are free and paid options. Carefully review the details which may change from time to time before deciding whether this might be suitable for you.

The version for Mac computers is supplied through Apple's iTunes store.

https://www.avg.com.au/products/avg-family-safety/

There is also a version for Windows phones:

https://www.avg.com.au/products/avg-for-windows-phones/

Password Storage

Roboform Password Protector: http://www.roboform.com/

Roboform is a well-established program which you can store your passwords in.

It provides a password generator and other features. Versions for Mac and Windows are available. You can get portable versions which can share your passwords between different type of devices.

I used their support desk a couple of times and was impressed at their patience and quality of advice.

Their free version is really free and allows you to store up to ten passwords.

Be Safer on Social Networks

Social Networks have been available in some form since the Internet became available to the general public.

They initially required some level of computer savvy buut they are now accessible to just about everybody.

That fact has good and bad aspects.

If you want to be as safe as possible when using the networks which are most useful and appealing to you, you need to protect yourself at all times.

There are some useful links in the Resources section of this ebook.

Checking Your Online History

Almost everything you have ever put on the Internet is still there. Some people may be using it without your knowledge.

You might want to use http://www.duckduckgo.com for these searches because it provides you with some protection for the personal information you enter when starting your searches. I have more information about duckduckgo.com in the Resources section near the end of this ebook.

Search for Your Name: For the sake of your reputation, do a search for your name every few weeks.

You may be amazed (or worse) at what turns up!

Search for Your Photo: If you have ever posted a photograph, someone may now be using it to represent themselves or even to endorse some service or product they sell!

Search for pictures you own: People load pictures of themselves, their family and possessions to the Internet every day. Some people may take copies of your pictures and use them for purposes you would not like without your knowledge.

So, it is worthwhile to check if this has happened. Google provide a simple, free service which you can use for this:

Google Image Search

Google provide a simple way to check if there any images of you online and show you where they are.

Load a clear copy of your photo on your computer. A small version is preferable because the upload of a large picture will probably slow the process.

Navigate to the Google Image Search page.

Click on the small image of a camera in the right bottom corner of the Search Box.

Follow the prompts to either provide the link to an online copy of your picture or to transfer a copy of your picture from your computer to Google.

Google will display details of similar pictures it locates.

Checking through the images found in the Image Search may take some time but it may help you to stop mis-use of your images.

Record the details of any site where you see your picture in use and you didn't authorize its use there.

Check available information about the site and then approach them to remove the picture.

The Wayback Machine

http://archive.org/web/web.php

This site holds copies of over 240 billion web pages dating back to 1996. It's where you can find what particular sites looked like at an earlier time and what people wrote or posted on their sites as well as forums etc., years ago.

Although not everything from each of the pages is viewable, it is a valuable record of web history and also useful for finding sites which may not exist anymore and what they used to look like.

It also proves that you cannot expect to be able to erase everything which you did on the Internet in the past.

Important Terms

This section explains several important terms which will help you understand people who offer you programs or services for protecting or improving your computer security.

If someone uses a term which you don't understand, ask them to explain it right then so you know what they mean and how exactly it affects you.

Home Page: The page of any website which appears when you type in the web address without any extensions. For instance, http://www.example.com/ is the home page of example.com

Firewall: Software which checks incoming and/or outgoing traffic on your computer for malware and other potential risks.

Phishing: Luring someone to click into a fake web site where they disclose private personal financial information. The sites also deliver malware to their computer which copies and transmits what they type to the crooks.

Protocol: This term is used by many people in technical areas instead of "method". "**Secure Socket Layer"** is a protocol.

S.S.L. Secure Socket Layer: A method used to transfer data securely over the Internet.

Resources

Search Engine with Focus on Privacy

Duck Duck Go http://www/duckduckgo.com/

I use this service as well as the more well-known search engines.

This service takes your search query and searches several search engines, including Google. But, they prevent the services they use for your query from adding your information to their databases unless you make a direct connection with those services.

Social Security Sites

Twitter Help Center

http://support.twitter.com/articles/76036-keeping-your-account-secure#

Twitter's advice about keeping your account more secure.

This information should be considered when you are signing up with any Social or other network on the Internet.

Facebook Security Center (International)

https://www.facebook.com/help/131719720300233/

This is the Security section of Facebook's Help Center. Use this site to report concerns including when your Facebook page has been hacked, your name has been used to set up a false Facebook page or perhaps you think that a friend's site may have been compromised.

U.S.A

F.T.C. Consumer protection.

A variety of warnings and information from the Federal Trade Commission about protecting yourself and family members online.

NetCetera http://www.onguardonline.gov/articles/pdf-0001.pdf

A downloadable guide to helping children stay safe online.

Credit Bureaus

Links for the three main Credit Bureaus:

Equifax: http://www.equifax.com

Experian: http://www.experian.com

TransUnion: http://www.tuc.com

Applying for Your baby's Social Security Number.

You can get details about these procedures in this article:

http://www.nolo.com/legal-encyclopedia/social-security-number-for-babies-29528.html

Nolo.com is a reputable publisher of books on legal matters.

Electronic Frontier Foundation

https://www.eff.org/

From their Site: "EFF was founded in 1990 and continues to confront cutting-edge issues defending free speech, privacy, innovation, and consumer rights today."

United Kingdom

Education Department

Report on child safety on the Internet and relevant links.

https://www.education.gov.uk/childrenandyoungpeople/safeguardingchildren/b00222029/child-internet-safety

Australia

Australian Federal Police Cybercrime information

http://www.afp.gov.au/policing/cybercrime.aspx

The A.F.P. give information about cybercrime, its effects on the community and links to resources here.

This link gives resources and information for particular groi\oups such as parents and other carers and teens, etc:

http://www.afp.gov.au/policing/cybercrime/crime-prevention.aspx Cybersmart website. http://cybersmart.gov.au/

From the website: "Support and encourage participation in the digital economy by providing information and education which empowers children to be safe online."

Keep Safe out There!

Thank you for reading my book.

It was designed to continue to help you keep yourself and your family safer when interacting with people and businesses in your daily life, on and off the Internet.

The opportunities and risks are constantly changing and increasing, so please keep this ebook close as a reminder and guide.

Drew Gawler

Another eBookWholesaler Publication

