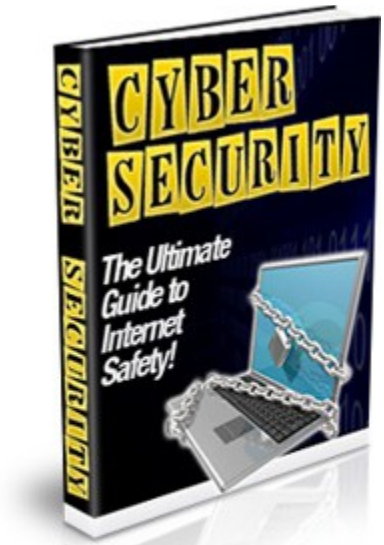

Cyber Security

The Ultimate Guide To Internet Safety!

By webbzo

http://www.webbzo.com

Table of Contents

Chapter 1 - Introduction

When I got my computer in the late 1990s, my kids were young and my primary concern was their safety. Most people, back then, were worried about computer safety back then and the fact that anyone could "come into their home" via computer and steal their children or money. I still know people who think this way, even today, and who will not have a computer in the house for this reason.

Computers are safe, but you have to learn about internet safety and you should be aware of some of the tricks, con games and scams that take place online. The internet is perfectly safe, as long as you know how to protect yourself. Although child exploitation and identity theft are feared online, there are ways to protect yourself against these problems.

During the years, I managed to learn quite a bit about internet safety. Much of what I reveal in this book has been learned through trial and error. I did get viruses in my computers. I did get my identity stolen. I did have problems with people who found out too much information about me. Fortunately, I was able to learn from past mistakes and prevent others from making the same mistakes that I did.

Internet safety is all about keeping yourself, your family and your personal information safe. Once you learn how to do this, you will feel much more secure in using the internet for a variety of different purposes. Despite the problems that happened to me, I still maintain a Facebook page. I do all my banking online and most of my shopping. I have had the same computer for a few years and it is virus free. I also managed to keep my children, who are now grown, from falling prey to any internet predators.

The internet technology has also allowed me to make my living as a writer - if it wasn't for computers and the internet, I would be out of work. I know quite a few people who met their spouses online and I have managed to make some nice cyber friends through this media.

Yes, there are dangers to the internet, but if you know what you are up against when you go online, you will not fear these dangers but be able to enjoy the convenience and fun of using the internet. The internet is here to stay. It is important for anyone who wants to keep up with current technology to learn how to not only use a computer and go online, but also to do it safely.

There are many advantages to using the internet when it comes to making purchases or even ordering services. Jobs are often found through the internet today and many companies insist that you apply for a job online. Airlines and other companies offer discounts to those who order tickets online as opposed to using an agent. Needless to say, the internet has tremendous advantages for everyone.

After reading this book, you will understand how to keep yourself safe when using the internet. This is not a book that uses technical language regarding cyber security, but a book that will teach the average person how to be safe, as well as keep their family members safe, when online.

Chapter 2 - Child Safety Online

Most parents are worried about child safety online and have every right to be. There have been incidents of young people, mostly young girls, who have fallen for an internet predator pretending to be a boy or girl their own age. These incidents have made the news. Needless to say that many parents are concerned with their child's safety when online. In addition, they also are worried about images and websites that are out there that they might not want their child exposed to. Fortunately, there are ways that a parent can make the internet safer for their children.

Young Children And Internet Safety

Parental controls will allow you to filter what your young child sees when they go online. There are sites that are created for children to use where they can play games. Children can also find out information that they need to do homework when using the computer. There are three things that a parent needs to do when it comes to letting children younger than 13 on the computer:

- Learn to use parental controls
- Teach their children about internet predators
- Supervise the use of the computer

Parental Controls

Just about every computer today is equipped with child safety features. These parental controls can block explicit sites and images from the computer when the child is using it. You simply set the parental controls to block these sites and images and they will not allow the child in. You should have a password that you can use to access the parental controls that the child does not know. While younger children will not usually want to explore things that are off limits, older children may be curious and want to go on sites that may not be for them.

Many websites today are featuring a safety feature that makes those who post images or text declare if it is explicit content. This feature is used on many sites, although not on all. As children get older, they want to go on MySpace, Facebook or Twitter. These sites do not screen out explicit content. Parental controls can prevent a child from visiting these sites and setting up an account. You can even manage parental controls so that you block certain sites from the computer. Children who are younger than 13 have no business using social networking sites that are created for older children. They are not yet mature enough to realize the implications of putting personal information out there for the world to see.

I used parental controls on the computer until my kids were 13. They used the computer for homework and had sites that they liked to visit. After they were 13, I gave them a little bit more freedom on the computer, but still kept the adult websites off. When my kids were 16, I took off all parental blocking. My son promptly downloaded "free music

files" online and got a virus on the computer from these files. I will talk about viruses in a later chapter.

The parental controls worked well for me, but I certainly didn't rely on them to protect my children when they were online. After all, there were many sites that they visited that were for children and featured chat features that were perfectly acceptable, according to the parental controls. These controls are a great tool when it comes to keeping a child safe online. But they should not be the only tool that a parent uses.

Education

Teach your children about internet predators. It is still amazing to me that parents do not teach their children about 'stranger danger" on the outside. From the time my kids were old enough to understand, I was constantly telling them about stranger danger. My husband said I was making them "paranoid," but I wanted to be sure that they were safe. It was the best that I could do.

I did the same thing when they went on the internet. I always made it clear to my kids that they didn't really know who they were talking to when they were online. I gave them concrete examples of how predators would behave. That they would pretend to be a person of their own age and post information that a young person wants to hear.

Education is necessary for all young people who go online. The same education should also be used for adults. Those who prey on children online do not seem like child molesters or worse online. They do not hang out in adult chat rooms looking for kids. They go where children go - in their chat rooms and websites. And they pretend to be children.

This is why it is important for parents to also educate their children when they are online as well as use parental controls. Parental controls may stop a child from entering an adult site, but there are plenty of sites online where kids can interact with one another. These are supposed to be for children only, and those who are adults and pose as children are violating internet safety laws. However, it doesn't stop adults from violating those laws.

Educate your children about the fact that it is very easy for anyone to develop a false persona online. They can use fake photos of themselves and pretend to be whoever they want.

Small children should not be chatting at all when they are online. They cannot understand the concept of someone pretending to be another person. Only allow your children to chat online when they understand the following:

- That anyone can pretend to be anyone they like online
- That fake photos and names are often used online
- Never to reveal any information about themselves
- Never agree to send a photo of themselves to someone

•Never agree to meet someone online

This still does not protect your child totally from online predators. As anyone with children knows, they do not always do what you ask. It is important for parents to not only use parental controls and education to keep their children safe, but also supervision.

Supervision

Do not let your kids use the computer unsupervised until they are mature enough to understand how to stay safe online. Children under the age of 13 should not have computers in their rooms and should not be using them unsupervised. This does not mean that you have to be looking over your child's shoulder the entire time they are online, but that the computer stays in the family living space of the home.

Many parents feel that because they have told their children about predators and have installed parental controls on their computers that their children are free to roam around online. They can enter chat rooms and go on forums where there are "moderators" for these sites. This is not true. Let me tell you how easy it is to be a "monitor."

A website monitor often works for free or for a free service. When AOL first came out, it cost $23 a month to get online (this was with a dial-up connection) and they looked for monitors for their chat rooms. In exchange for being a monitor, you received a free membership. I signed up to be a monitor. I only had to give them my name and email address and I was in. No background check. No authenticity required. If someone tries hard enough, despite more controls that websites are using, they can become a monitor for a forum or chat room. There is no formal interview and all is done over the computer. Parents should not entrust their children to website "monitors" who may or may not be who they say they are.

After children are old enough to have computers in their rooms and have a bit more freedom online, parents should still know what is going on. As they get older and prove to be more trustworthy when it comes to using the internet, as well as personal choices that they make in their lives, then you can loosen up a bit. But you should still watch their internet usage.

Many of the young people who fall prey to internet predators do so because they are lonely and have few friends. They spend an inordinate amount of time in their rooms on the computer where they meet "friends." It is important for parents not only to be supervisory of their children's internet activities, but also to watch how much time they are spending with their internet "friends." Internet friends should not take the place of the real world. If a child is spending all of their time on the computer and not participating in real world activities, something is wrong.

Parents should also remind their children, even older children, of the fact that anyone can be watching what they are doing online. While they may think that it's fun to post pictures of themselves drinking at a party on their Facebook page when they are 17, it

may end up coming back to haunt them. Remind kids that the internet is public domain. Anyone can see what they are up to on such sites. Including college administrators and prospective employers. Kids do not often understand the repercussions that can occur from simply posting a picture of themselves online.

Internet security is crucial for any parent. Make sure that you have adequate software that supports parental controls and that you also use education and supervision in order to make sure your kids are safe online.

Chapter 3 - Secure Payment Sites

Many of the people I know today are amazed that I have done my Christmas shopping for four years entirely on the computer. I have been purchasing items from sites like Amazon, eBay and others for years using the internet. I have never had a problem with having my credit card or identity stolen when using secure payment sites.

The trick is secure payment sites. Not all websites that accept payments offer security. Some offer minimal security while others offer the same type of security that banks use online. Large sites like Amazon and eBay are safe to use. Paypal is safe to use. They employ the same type of cyber security systems that are employed by my bank online. I have also ordered many things from online retailers such as golfing equipment, perfume, food, flowers and other things from secure sites.

But it can be easy for someone who is used to all sites being secure when making payments to fall into a trap where they purchase from a site that is not secure. I almost fell into such a trap not too long ago.

I found a website that offered VHS tapes that are not found anywhere else. It seemed like a great site for me and I bookmarked it to place an order. Then I started thinking about the site and how I found it.

I found the site through an email that was sent to me from an online group that I belong to that is devoted to classic films. I went on the site to see if they offered a secure payment system and they did not. I was used to seeing the secure symbol, which is a gold lock, on the sites where I shopped. This site did not have this symbol.

I looked into the site and saw that they did not have any information posted about them. No information on where they were located and no customer service number. While this does not guarantee security when you are shopping online, it does help you think that the site is more legitimate.

There was also no security information about the site. Retailers that are in compliance with Internet Safety Standards have to post security and privacy information about their site. This site did not post this information. As I looked further into the site, it appeared as if there was no security at all. Needless to say, I didn't place an order. But had I not stopped and thought about it, I might have placed an order. Whether or not the website was a sham or whether they are actually just trying to sell VHS tapes is up for grabs. The important thing is that by giving them my credit card information over the internet, it would not be protected.

Anyone who is interested in shopping online needs to look at the security offered by the site. Although the site may be legitimate and make good on purchases, they need to offer customers who are using electronic payments some type of security that their information they provide will be private. If a site does not have such a privacy statement and a safe checkout, it is not a good idea to shop there.

I am happy to say that I have never been cheated when ordering something online. I also never had my information stolen when using my credit card or Paypal online. However, to be safe when shopping online, you should use either Paypal or a credit card to insure your purchases and not a debit card.

A debit card offers no security if you do not get the items you receive. Paypal offers customers a guarantee and is an easy way to pay for something online. Credit cards also offer their customers a guarantee. I have credit cards and my Paypal account on file at several of the sites that I frequent the most and also pay my bills in this manner. Many people are worried about their credit card information being stored at some site and it being used for other purchases. I have never had this happen to me. You do, however, have the option of storing your information on the site, such as your password and payment information, or not. If you feel uneasy about this, you can elect not to have the information stored.

I have found that it is actually safer to shop online than in a store. My debit card was compromised by a false front that was put on the ATM machine at the bank. Fortunately, I did not lose any money but I had to get a new card. A friend of mine had his entire bank account wiped out after he was shopping with his debit card at a major discount store in his own town. The cashier swiped his card into a device that copied all of the information, a new card was produced with a PIN number and the card was sold to someone who used it in another state.

Whether you shop online or off line, you need to watch out for identity theft. However, it is often easier for these thieves to get you off line than online, as long as you are using secure payment sites in which to do your shopping.

A good online website will offer secure sockets layer (SSL) cyber security systems to protect your internet transactions as well as password controlled entry. You should be directed to a secure area on any website to make a purchase that is safeguarded against intruders.

Chapter 4 - Online Banking

Is online banking safe? Yes. I have been doing my banking online for years. It is not only safe, but convenient as well. There are many online banks that offer good interest rates on their accounts. I have an off line bank but make most of my transactions with them online. I also use Paypal quite a bit like a checking account as many sites will now accept Paypal payments.

Banks offer state of the art internet security that employs the following state of the art security technology:

- Secure Sockets Layer (SSL) protocol
- Password controlled entry to the site
- Firewalls
- Data encryption
- Filtering routers
- Public private key pair

All of these systems combined makes for very tight security. If you are planning on doing online banking, you should make sure that your banking site offers this type of security. You will need to log into the site using your password each time. You do not store your password in these sites and will have to enter your user name and password each time you can get into the system. You can write down this information somewhere private. Some people put this information on a flash drive so that they have it.

After you have logged into your online banking site, you should then be directed to a secure environment where you can conduct transactions. The SSL will secure the session for you with your browser. The data that goes between your bank and you will be encrypted and can only be decrypted with the private key.

Your browser should be 128 bit encrypted in order to support the security of an online banking site. Three browsers that support this type of encryption are the following:

- Internet Explorer
- Mozilla Firefox
- Netscape

If you are using another browser, you will not be able to do your online banking. For your own protection, you should use one of these secure browsers. You can download the latest version of these browsers by going to the websites and getting a free download.

Online banking sites also have firewalls that will reject any traffic to the site that is unauthorized. There are also filtering routers that will verify the source of any requests that travel in through the information packets on the site.

Chances are that your bank, like mine, has a website that you can use. You can

comfortably do your banking from home without worrying about someone getting your information. As I mentioned earlier, my recent problem with my bank was due to me using the ATM, at the bank, that had a false plate on it that picked up the numbers. Fortunately, the bank spotted this in time and before my card information was printed on another card and my account wiped out.

Those who bank online or use a merchant site like Paypal should also know that these sites do offer protection in case you do lose money due to nefarious activity from a predator. My friend had to complete an affidavit about his card and received his money back. Paypal offers the same service for anyone who is unfortunate enough to have their account compromised. It is important to realize, however, that most accounts that are compromised are done so because of a mistake on your part rather than someone hacking into the system. I will talk about phishing and pharming, two common practices, in a later chapter.

Banking online is easy and safe. I do, however, make it a point to check my balances on a regular basis so that I can catch anything unusual with my account right away. As long as you protect your password and information, there is no reason why you should worry about your online banking being compromised.

Chapter 5 - How To Keep Your Password Safe

Your password that you use for your internet access as well as online banking and on different sites should be something that you will remember and is not easy for someone else to figure out. For your own safety, you should use different passwords for different sites. For example, if you sell on eBay, you should have a different password for your eBay account than you do your Paypal account. You should also have a different password for your banking accounts and anywhere else that you need security online.

The reason to have different passwords is for internet security. If someone does manage to get your password for one account, they cannot use the same password to travel to all of your sites and get into your bank account, Paypal account and other accounts. You should have different passwords for all different accounts.

You should put your passwords, along with the accounts that they are used for, in a special place. Some people put them on a flash drive, which is a handy device that plugs right into your USB port and will allow you to store data. You can also put your information in a safe place such as a safe or safety deposit box. If something should happen to you, you should have someone who you can trust be able to retrieve your passwords for you, especially if you are banking online.

You should never give out your password to anyone who sends you an email. If you have a Paypal account, for example, you should know that Paypal will never contact you by email and ask you to give them your password. Nor will banks. Often, such emails are sent with a sense of urgency to an individual in the hope that the person will act quickly without thinking. A friend of mine nearly had his Paypal account compromised not too long ago.

He received an email from Paypal that said that his account was frozen due to suspicious activity on his account. They requested that he verify his password and send it back to them. This is known as phishing. Needless to say, my friend did not fall for this scam.

Never give your password out to anyone online unless you have logged into the site yourself. Never give your password to anyone for verification through an email. Your internet security is hinged on the security of your password. Keep all of your passwords in a safe place and do not share them with anyone unless they are a friend or family member who you know and trust. And above all, do not use the same password for all of your accounts online. Many accounts use an email as a username. If one account is compromised, such as your email account, the predator can easily go through all of your account and gain access.

Use a browser that is secure such as Internet Explorer, Netscape or Mozilla Firefox. These browsers have firewalls so that no one can get into your computer and gain access to any of your information on your hard drive.

Chapter 6 - Common Scams

If I had just a dollar for each time I was sent a scam e-mail, I would no longer need to work. There are many scams around online that compromise internet security. Many of them are just new versions of old scams that have been used for many years, even before the internet came around. They usually prey upon your greed and desire to get something for nothing. It is best to know about these scams to protect yourself. Never think that you are "above being conned." Con artists say that the easiest person in the world to con is those who think they cannot be conned.

Many people are afraid of going online because of "hackers." Every once in a while, we hear about a computer hacker who managed to get into a bank or other secure online environment. These instances are rare. Most people who become internet victims fall prey to one of three common scams:

- A con game
- Phishing
- Pharming

A Con Game

A con game is short for confidence game. This sort of activity has been around since the beginning of time, but the internet gives it new legs. If you are reading this and are concerned about internet security, you have most likely heard about the Nigerian Bank scam. This is probably the biggest con game going online and it has many variations. The reason that about one billion dollars per year is lost due to the Nigerian Bank Scam is because people continue to fall for it, despite repeated warnings, and that the internet security laws in Nigeria are non-existent.

The way this scam works is as follows: You get an email from someone in Nigeria who has a great deal of money but cannot leave the country. They promise to send you a check for $50,000 (this amount changes) if you will just send them $1,000 (this amount changes, too) so that they can get out of the country. The check is drawn on a US bank and they cannot cash it in Nigeria. They ask for your help so that they can get out of Nigeria and say that they will be willing to then split the money with you when they get to the United States.

In "good faith" they send you the check first and ask for you to send them money so that they can leave Nigeria. You get the check, deposit it into your account and send them the check so they can get out of that country. Or, perhaps, you are a dishonest person and keep the check and do not send them the money. It doesn't matter because the check is a phony. It looks like a real check, is often a money order or cashier's check, and is drawn off of a bank in the United States.

By the time you realize that the check is a phony (after it bounces and is returned to your bank - often bouncing all of your checks) you are out $1,000. Or $10,000. Or even more. Some people have lost hundreds of thousands of dollars in this scam.

There are many variations to this scam. They usually involve you cashing a check for someone and giving them part of the money. In some cases, the Nigerian Bank scam will ask for half of the money to be sent to Nigeria.

Because it is so well known, this scam has taken a twist and is often the UK Lottery Scam. You won the UK Lottery, they are sending you a check but you need to send back half for taxes.

In order for you to practice internet security online, do not fall for any request that asks for money. No matter how good the offer seems to be, no matter how it looks as though you cannot lose, you will end up being parted with your money.

Other confidence games that make it tough on those on the internet prey on lonely people. Lonely hearts scams are also very old but have gained a new life online. Women or men will write to you, usually through a dating site, and fall madly in love with you. But there will be one problem - they cannot leave their country. They ask for plane fare or money that they owe someone so they can be with you. This game is often called the "Russian Bride Scam" as it is often used by Russian women on American men.

My friend who had his debit card compromised at the discount store almost fell prey to this. He was about to send $1,000 to a woman in Russia who he had been flirting with online. Because he was lonely and looking for a girlfriend. The worst thing about these confidence games is that they prey upon those who are lonely. My friend is a college educated person with a successful business. You would think that someone of his intelligence would not fall for such a trick. But he almost did. Remember - the easiest person to con is someone who thinks they are above being conned.

Never send money to anyone online. Period.

Phishing

Confidence games are old, but the internet has made it possible not only for the old con games to flourish, but for new, more technically challenging, games to begin. Phishing is when you receive a request for information through an e-mail or other sort of online contact.

In addition to preying on greed and loneliness, con artists also prey on fear. Phishing is successful because the person doing it creates a sense of urgency in the "mark." In the world of scams, the "mark" is the victim who will soon, if he or she is not careful about internet security , will soon be parted from their money.

Those who are phished often do not even know that anything has happened because it all

occurs so suddenly. As I discussed in the previous chapter, it usually starts with an e-mail that is very urgent. Your bank account has been frozen. All your checks have bounced. They believe that someone is using your account. Can you verify your password?

In some cases, the phishing can be for other information instead of a password. They may look for your social security number and birthday. With this information, they can open up accounts in your name. I saw one email that said that you can get 10 percent interest on your Paypal balance if you just filled out a form. Of course, the first three things that they asked for is name, birthday and social security number.

Never give out information to anyone who contacts you by email. Even if it is someone you know, you should never give out this information. You never know if their account has been compromised and someone is using it to phish for information from others on their email list.

If you get a request that you believe is phishing from your bank or other secure site, you should forward the request to the site as long as you have virus protection on your computer. You should never open up an email from someone you do not know if you do not have virus protection on your computer. Virus protection as part of your internet security, will be discussed in a later chapter.

Never give out any information to anyone who contacts you by email. Period.

Pharming

Pharming is another term that is used in the internet con game world. Unlike the regular con games that are older than the hills and phishing, pharming is very sophisticated and not only takes a black heart, but also some technological skills.

Like most common internet scams, pharming starts with an email. The email is supposedly from a company that you know and trust. They send you a link for a special offer and you are directed to their "site." Only it is not their site. It looks just like their site, but is a phony site that has been created to look like their site. Here you will enter your username and PIN number or password and fill out bogus information. It will seem fine, except you have just compromised your account. The phony site will have your information and use it accordingly. The one time that I had trouble online was with this scam.

Chapter 7 - How I Got Pharmed

A few years ago, I was selling merchandise on eBay. I had a Paypal account and was doing pretty well with my little eBay home business. Then I got pharmed.

The scam preyed on my greed and desire to get something for nothing. I wanted very much to be a Power Seller at eBay, but did not have enough sales to make this goal. The email I received seemed to come from eBay. It stated that I could, if I acted right away, become a Power Seller. They had a special promotion and I could earn this status.

I was not anywhere close to being a power seller. I had auctions that ended every few days and watched them a few times a week. I had not earned the number of sales to get this goal. But I wanted it, so I was excited to jump on the link that they provided and go to the eBay site.

Had I looked carefully, such as at the address bar, I would have seen that although where I was looked just like the eBay site, it was not the eBay site but a very clever duplicate of the site. I put in my username and my password and then filled out the request to be a Power Seller. I was pretty excited that I was going to be a Power Seller on eBay.

A day or so later, I went to look at my status and saw that I was not a Power Seller. I wondered about this - after all, I filled out the form. For some reason, I took a look at my auctions. None of them were close to ending, but I noticed that the address to where the money was to be sent was somewhere in Italy. This bothered me as I live in the United States and have never been to Italy.

I called eBay and got in touch with someone there. They told me that I had been "phished" because the term "pharm" had not yet been coined. They promptly froze my account and stopped my auctions. Luckily, nothing bad happened. As none of my auctions ended, no money was exchanged and none of the customers who were bidding on my products were cheated. Had I been a real "Power Seller" I would have been in trouble. I had to close out my eBay account and start all over on another account.

When I told the person at eBay what happened, they also advised me to check my Paypal account. As it happened, my Paypal account had been emptied. This was because I used the same password for my eBay account as I did my Paypal account. There was not much money in that account (as I was not a Power Seller) but the little money that was in there was gone. I had to call Paypal, close the account and fill out an affidavit. I did get my money back from Paypal.

Had I been more of a mover and shaker on eBay, I could have lost quite a bit more money, and those bidding on items would have lost money as well. I never knew that a false site could be created. I learned this lesson well and, although I get pharming emails regularly, I never feel prey to it again. Because now I know the following:

•Never click on a link that the site sends you - go to the actual site

•Never use your same password for everything
•Never expect to get something for nothing

People who are concerned about internet security need to be aware of the techniques that are used in the scams that run online. They prey on the greedy, the needy and the easily frightened. If you get an email from any site that states something urgent, **do not click on the link**. Go to the site to find out what is what.

Pharming attempts for Paypal and eBay are very common. If, however, you get a pharming attempt from your bank, contact your bank and forward the email to them.

Chapter 8 - Virus Protection

If your computer does not have virus protection, you should make sure that you get it. You can get Norton Virus Protection, that often comes with computer programs, which will protect your computer against viruses that are often found online.

When it comes to internet security, most people worry about computer viruses that can get into a computer and wipe out the hard drive or do harm to the computer. Virus protection is one way that you can prevent this from happening to your computer. You can get virus protection software for about $75 at a computer store. Norton is usually installed on most computers and you can pay a monthly fee or annual fee to keep this software updated so that you are protected against the latest viruses.

A computer virus is like a bug that will infect a computer. It can be something that is just created for malicious purposes or one that is created to look for information. Some computer viruses will cause pop up ads to appear and your system to shut down.

While it is essential to have virus protection, there are always geniuses out there creating new viruses. This is why you need to use a little common sense when it comes to your internet security and virus protection.

I mentioned earlier that our first computer was ruined by my son, who downloaded some "free" music online. I would like to say that this was the only computer ruined by my son from downloading free music files, but I would be lying. He actually ruined 3 computers in this way - the original family computer and two of his own. His third computer was purchased with his own money - I assume he does not want to ruin that, so he is now downloading any files from "free" music sites.

Music and video files are often contaminated with viruses. Often, the creator of the file does not even know the virus is there - they often get the material from another infected file. Downloading free music from certain sites where others put on their own files is a sure way to get a virus in your computer. If you have protection, you will be notified if the file has virus.

Free things that you send to people online often have viruses. Most of the time, these are viruses that cause pop up ads to appear. I sent a card from a free card site to a friend and he wrote to me, thanked me for the thought, but said that his computer detected a virus in the card so he did not open it.

To protect yourself against viruses, you should do the following:

- Have virus protection on your computer
- Do not open up emails from people you do not know
- Do not click on links in emails that you receive from others unless you ask for them
- Do not download free music from music sharing sites
- Do not download free videos from video sharing sites

•Stay away from adult content sites

If you start getting pop-ups that you cannot control, your computer starts to crash all of the time or you cannot get into programs, chances are that you have acquired a virus in your computer.

You can take your computer in to have it cleaned or you can uninstall everything on the computer and install all of the software again. Many computers today are sold with discs that will bring the computer back to the state where it was before you put anything on the computer. You can often use these discs to wipe out everything that was installed on your computer after you took it home from the store. If the virus has not infected your hard drive, this will often do the trick. If not, you need a new hard drive.

You can also try going online with another browser. If, for example, you think you contacted a virus that is affecting your Internet Explorer browser, you can download a Mozilla Firefox browser and use that to go online. This can help if you have a small virus on your computer.

Those who have Mac computers do not have the same problems that those with PCs experience when it comes to viruses. While there are some viruses that transcend between the two operating systems, most of the computer viruses out there are created to affect the Windows operating system.

Most computer viruses do not wipe out your entire data base or cause serious harm to your computer, contrary to what you think. What they will do is cause frequent computer crashes, freezing of the computer, pop ups that seem to be out of control and the computer to move very slowly. It is best to get this problem addressed by a computer expert. It is even better to take precautions against getting a computer virus by having protection on your computer and following the above tips.

Chapter 9 - Self Maintenance

In order to keep your internet security up to date and keep your computer in the best shape, you should do some maintenance on a regular basis:

•Delete cookies
•Delete history
•Re-configure the computer

Delete Cookies

On your internet toolbar, you will find an icon for internet tools. When you press on this icon, you will be given options on what you would like to do. You can delete cookies. Cookies are placed on some sites that you visit that will hold your password or other information. They are supposed to make things easier for you when you go online, especially if you frequent a certain site all of the time. Sometimes, cookies are placed on your system by sites without you knowing it for data purposes and usually to send you ads. You should delete cookies once a week from your browser.

Delete History

You can also delete the past history of where you have gone online. This can help protect your internet security in case you do happen to have a virus that infects your computer and travels to where you last were online. You can delete your history on a daily basis. You use the same icon on the toolbar to delete your history as you do cookies. This does not affect sites that you have bookmarked as favorites on your browser. It takes a bit longer to delete history than it does to delete cookies. In addition to helping you with internet security, it will also make your computer run faster.

Re-Configure The Computer

There should be a reconfiguring tool for your computer. This will reconfigure all of your files and compress them. You should refer to your computer manual on how to accomplish this. It normally takes several hours the first time you reconfigure your computer, although if you do this regularly, it will not take hardly any time at all. In addition to getting rid of corrupted files, it will also make your computer run faster by keeping all of the files together.

You should also run a scan on your computer periodically to see if there are any problems with your system. If you have Norton Anti-Virus, you will be asked to run a scan for corrupted files on a regular basis. This can correct any problems with the computer, such as viruses, and also eliminate them. By understanding how to maintain your computer, you can keep it working properly and also keep it free from viruses that can cause it to crash.

Chapter 10 - Personal Information Online

Be careful what you put online, unless you want the whole world to know what you are doing. I discovered blogging in 2006. I began to write my daily occurrences online, as many people today also do. I used my real name and had my real town on the computer.

I met a lot of cyber friends from my blog and began to get a lot of followers. It was fun to write on this blog on a daily basis and keep an online diary. I frequently used my camera phone to add pictures to this blog. At one time, I was getting 1000 visitors a day to my blog. It was a lot of fun.

Unfortunately, I was soon to learn that not everyone online is friendly. As a matter of fact, some of the biggest weirdoes I ever met I met on this blog. I was the victim of cyber stalking on more than one occasion.

What Is Cyber Stalking?

Stalking is a term that was coined in the 1990s to describe someone following someone else incessantly, despite being told to stay away from them. Years ago, there were no anti-stalking laws to prevent this type of behavior from occurring. It took a few deaths to change the laws to where we now have anti-stalking laws. Most of the stalking that we hear about are those who are prosecuted for stalking celebrities. Most stalkers, however, are stalking someone they know personally. It is usually someone who has what they feel is unrequited love for another person who does the stalking. This often escalates into violence, which is why there are the laws to prevent this type of behavior which is, at best, very creepy.

Cyber stalking is when someone stalks you online. They watch wherever you are going and end up there, too. They follow what you are doing on your blog or Facebook or Twitter page and take casual contact as something much more serious than you mean it. Fortunately, most cyber stalkers do not physically confront their victims.

Of the two people who stalked me, one of whom I actually had to file a police report against, one came on like a friend and the other like a real jerk. The real jerk saw my blog and it antagonized him. I did not know this man at all and later found out that he lived in another state. For some reason, he used all of my personal information and use it against me. Every day, he would write nasty comments about me and my family. When I didn't respond, he actually looked my name up and found my phone number. Because I had my real name and town, and was listed in the telephone book, he was able to obtain my telephone number and began harassing me by phone.

I had to dial *57 and trace his call through the telephone company. I then filed a report with the police department who gave me his name and telephone number. I was able to go online and find out his address by using a reverse directory. I let him know that I

knew who he was and fortunately, the stalking stopped.

The other person came on as a friend and we chatted for quite some time online before exchanging phone numbers. When I didn't call him back immediately after he left a message, he went on a tangent that was over the top.

Other people who I met on this blog also didn't appear to have both oars in the water, so to speak, and finally, after nearly two years on this site, I closed it down. I learned the hard way not to put too much information about myself online for the world to see.

I have known people who have lost their jobs due to blogging about companies where they work. What very few people realize is that anyone can see what you are putting on your blogs. And some people take a casual cyber friendship as something more than it is. Unless you want trouble, you need to limit the information that you put online.

Although my cyber stalker/bully did not do me any real harm, such people have done harm to people across the country, many of whom have committed suicide over cyber bullying.

What Is Cyber Bullying?

Cyber bullying is just like real bullying that a person, usually a kid, endures at school. Only this is on the internet. There have been TV movies made about the dangers of cyber bullying as well as newspaper reports about extreme cases in which a young person killed themselves over cyber bullying.

Cyber bullying is even more damaging than real bullying. In real bullying, people have to actually show their faces. With cyber bullying, they can hide behind their computer screens. One grown woman actually pretended to be a teenaged boy so that she could torment one of her daughter's enemies at school. She cruelly broke up with the girl (pretending to be the false boyfriend) and suggested that she kill herself. The girl did. The woman was sentenced to jail time, but not enough.

If you have kids who are going online, they should understand about cyber bullying. This can be damaging to an adult - I remember how creepy it was when that one guy was bullying me, and I'm and adult. I can imagine how horrible it can be for a young person.

The way to avoid bullying online is to keep your online contacts to your friends. Sites that lure the young people, like Facebook, are offering extra internet security because they limit access to a person's page to only their friends. However, your teens should know that friends can quickly become enemies.

Unlike bullying in school, there is little to be done about cyber bullying, unless it is an extreme case. As these events are taking place outside of school, the school has very little authority over what goes on when students are not under their control. Because of freedom of speech, the police also have little control, unless actual threats are made.

In order to avoid problems with cyber stalkers and cyber bullies online, you need to do the following:

- Limit the amount of information that you put about yourself online
- Limit your contacts to those people who you actually know
- Do not put down the name of your town where you live
- Never use your real name online
- Learn to use block systems to keep those who may be stalking or bullying you away from you
- Report any threat to you or your family to the police

Putting too much information out there for the world to see may seem like a "liberating" idea for some people. It did for me. Until I realized that the world is full of kooks and that some of them can be downright scary.

Talk to older kids about cyber stalking and cyber bullying. They should know what is a healthy form of communication and what is not. Tell them these stories and teach them to report to you anything that goes on that makes them feel threatened or uncomfortable online. Trust your instincts and, if you happen to meet someone online who you would like to talk to by phone, use a cell phone number that cannot be traced to your home.

Chapter 11 - Is The Internet Safe?

With all that I have written so far about the internet - the scams, the viruses, the nut jobs - you may be worried that the internet is not a safe place to be at all. It is, however, if you learn from my mistakes and find the internet enjoyable.
The information that I provided to you is not meant to scare you or put you off the internet. To the contrary, it is meant to give you the ammunition that you need to make sure that you are well aware of internet security and how you can make sure that you and your family are safe online.

Despite the pharming incident and the cyber stalkers, I have had a lot of pleasant experiences online. Let me tell you a few of them:

- I was able to meet a very good friend
- I was able to find a job
- I was able to get discounts on many different items that I would have paid a lot more for in the store
- I was able to purchase items that I couldn't buy in the store
- I was able to find out information about things I wanted to know
- I was able to reconnect with old friends
- I was able to listen to videos that are no longer on TV
- I was able to find movies that I never knew existed
- I was able to save time and money by doing my banking and bill paying online

The internet is a safe place to be if you understand how it works. The primary rules you need to know are the following:

- People can make up fake names and be anyone they want online - take what they say with a grain of salt
- Have virus protection for your computer
- Do not fall for internet scams - remember, you never get something for nothing
- Update your computer with self maintenance regularly
- Never reveal personal information such as your real name or where you live
- Teach your kids about internet safety and follow the tips in Chapter 1
- Beware of whatever you put online - unless you don't mind the whole world seeing
- When you shop online, use a credit card or Paypal account
- Keep your passwords in a safe place and never use the same password for everything
- Never give out information through an email
- Never follow a link to a site and then put in personal information
- Don't open emails from people you do not know

There is one thing that I did not mention earlier and should mention right now. That is the value of a secure connection. A secure connection is one that you use from your home and has firewall to keep others from getting into your system.

A non-secure connection is one that you have at a coffee shop or internet café. It is okay

for doing some things, but in order to do banking or make purchases, use a secure connection.

If you do not have a secure connection at home, use a wireless secure card for your computer when you do banking, make purchases or do anything with finances online. You can purchase these security cards that will protect your computer by purchasing them online or in computer stores. Always try to use a secure connection when you are doing anything with money online.

Hopefully, this book has helped you understand how internet security can help you. Remember, the more you know about what is going on in the online world, the better protected you will be. You can enjoy your time online when you are well versed in what you need to do to have internet security.