Below The Radar

Written By

Stephen Sindoni

Table of Contents

1. **Introduction**
2. **Wi-Fi Connectivity**
3. **Bluetooth Connectivity**
4. **Computer Basics**
5. **Securing Your Computer**
6. **Passwords**
7. **Internet Freedom**
8. **External Hard Drive**
9. **Below The Radar**
10. **References**

Introduction

In the early 1990's, I was working as a Video Sales Counselor for a large well known electronics company. My area of expertise was Television, VCR, and Video Camcorders. At that time, televisions were analog and using rabbit ears antennas for broadcast reception. This was at a point in time when we as a nation was still relying on analog technology to watch television programs from local affiliates such as CBS, NBC, & ABC. In total we had a little over a dozen channels to choose. All the channels were being broadcast to our living rooms from within a fifty mile radius. For those individuals who were living further away from the city, these individuals needed to have a high powered roof antenna to be able to receive television signals to watch television at home. There was no digital television. This was at a time when we didn't even have cable television. But that was all about to soon change.

Our store manager held a meeting with all of the men who worked in the Video, Audio and Computer Departments to inform all of the employees that we would soon be getting a visit from Sales Representatives who worked for electronics manufacturing companies such as Sony, Mitsubishi, RCA, Sharp, JV, Toshiba & many others. The purpose for this visit was to inform us that digital television would soon be replacing the analog television sets that we had all had so become accustomed too. The Sales Representatives would be spreading the gospel that digital television would soon be replacing analog television sets. The Sales Representatives would be coming to all of our stores throughout the country. As a recall, our company had well over a hundred stores. This in my mind was huge!

Within a matter of days, the first Sales Representatives from RCA. arrived with their product lines of digital televisions and went over all of the feature, functions and benefits of each specific model. We were informed that all of our stores within the next sixty days would be soon receiving digital televisions.

They would no longer be shipping the analog models. All of their television sets would now be obsolete. The Sales Representative went on to say that the US. government in agreement with the Federal Communications Commission were mandating this change to be in full effect by the year 2000.

Being curious by nature, I pondering the thought, “Why would the government get involved with the FCC in this matter?” After our store received the first shipment of digital television sets, I asked one of my friends who worked in the Electronics Return Department to open up the back of one the digital televisions.
What my friend and I discovered revealed a hidden built in microphone that could be used to eavesdrop on personal conversations and a web-cam that could be used to watch unsuspecting US. citizens in their own home.

Once the television set was connected to the cable box these features could be turned on and used to spy on all of us. Big Brother now had the capability to spy on 67 million households. Does this sound like the book written by George Orwell 1984? It was then I became highly suspicious.

What I knew about a television sets ability to use 525 scanning lines to transmit an image call ed an aspect ratio, triggered an alarming question. What if someone decided to reduce the 525 scanning lines to create a smaller image example a letterbox smaller and wider screen similar to what you would see when you went to the movie theater would appear and the unused portion of the television screen could be used to send a higher EMF signal to the set that was designed to send harmful EMF waves to the unsuspecting viewer? Has anyone ever fell asleep and left the television set on only to find the television screen size has been reduced similar to the letterbox theater image and as a direct result of changing the aspect ratio on your set and using the television set as a weapon of destruction against you, woke up with an extreme headache? It does make you wonder doesn't it!

Has anyone ever set the microwave for let's say two minutes and noticed that somehow while you were standing next to the microwave that the timer setting was changed mysteriously to 20 minutes?

How about having the toaster set to a low number and discovering that your toast has been burned to a crisp? And you were standing right next to it?
Did you ever wonder where your missing sock went in the clothes dryer?
Can anyone reading these words tell me where the missing sock went?
I'll leave this riddle for the Maytag repair man television commercial pitch man to figure out.

And lastly, how about getting hacked on your Microsoft Windows or Apple Operating System? Then you pick up the phone and call tech support and you explain the problem to the technician who walks you through a couple of steps to fix the problem. But he or she never explains what caused the malfunction. So, if you're like me, you want to know how to troubleshoot the problem to find the solution without ever having to call technical support.

The problems that I have cited in this introduction are the main reasons for writing this book. How many of you honestly read the manual (RTM) when you purchase a computer or any other electronic device?

Therefore, It is my hope that everyone reading this introduction will find my tips quite useful in this turbulent times. The information that can be found in this book are the result of over twenty years of my own personal experiences with computers.

Most of what I will be sharing with you are little known facts that computer manufacturers will not share with you. There job is to sell equipment. The more equipment they sell, the more money they will make. It is more to their liking to sell you a new piece of equipment than to fix the computer than one of their customers purchased. Once the computer warranty has expired, you're on your own. The manufacturer whether it be Apple, Microsoft, Toshiba, Hewlett Packard or any of the other manufacturer's, are going to do there best to sell you a new computer.

In this book, you'll learn how to turn lemons into lemonade. I will end this introduction will these final words “Trust But Verify.”

Sincerely,

Stephen Sindoni

Wi-Fi Connectivity

Before getting into the Computer Basics chapter, I feel it is necessary to explain Wi-Fi connectivity. So, what is Wi-Fi and how does it work?

Wi-Fi is a technology that uses radio waves to provide network connectivity. A Wi-Fi connection is established using a wireless adapter to create hot-spots- areas in the vicinity of a wireless router that are connected to the network which allows users to access the Internet. Once configured, Wi-Fi provides wireless connectivity to your devices by emitting frequencies between 2.4 GHZ- 5GHZ (Gigahertz), based on the amount of data on the network.

What Does Wini Stand For?

You may be surprised to learn that many people don't actually know that Wi-Fi is an abbreviated term. The most widely accepted definition for the term in the tech community is Wireless Fidelity.

Wireless technology has widely spread in recent years and you can get connected almost anywhere; at home, at work, in libraries, schools, airports, subway & trail transportation stations, hotels, star bucks, and even in some restaurants.

Any tech would tell you that Wireless Networking is known as Wi-Fi, or 802.11 Networking as it covers the IEEE 802.11 Technologies. The major advantage of Wi-Fi is that it is compatible with almost every operating system, game device, and advanced printer.

Like Mobile Phones, a Wi-Fi Network makes use of Radio Waves to transmit information across a network. The Computer should include a Wireless Adapter that will translate data sent into a Radio Signal. This same Signal will be Transmitted, via an Antenna, to a Decoder, known as the Router. Once Decoded, the Data will be sent to the Internet through a Wired Ethernet Connection.

As The Wireless Network works as a two-way traffic, the data received from the Internet will also pass through the router to be coded into a radio signal that will be received by the Computer's wireless adapter.

Wi-Fi Frequencies

As mentioned earlier, in this chapter, a Wireless Network will transmit at a frequency level of 2.4 GHZ or 5 GHZ to adapt to the amount of data that is being sent by the user. The 802.11 Networking Standards will somewhat vary depending mostly on the users needs.

The 802.11a will transmit at a frequency level of 5GHZ. For the techs, The Orthogonal Frequency- Division Multiplexing (OFDM) used enhances reception by dividing the radio signals into smaller signals before reaching the router. You can transmit a maximum of 54 Megabits of Data per Second.

The 802.11b will transmit data at a frequency level of 2.4 GHZ, which is a relatively slow speed. You can transmit a maximum of 11 Megabits of data per second, far less than the 802.11a which as previously indicated, was 54 Megabits per second.

The 802.11g will transmit data at 2.4 GHZ but can transmit a maximum of 54 Megabits of data per second as it uses an OPDM coding.

The most advanced 802.11n can transmit a maximum of 140 Megabits of data per second and uses a frequency level of 5 GHZ.

Hot-spots

What are Hot-spots? The term Hot-spot is is used to define an area where Wi-Fi access is available. It can either be through a closed Wireless Network at home or in public places such as in a restaurant or in an airport.

In order to to access hot-spots, your Computer should include a Wireless Adapter. If you are using an advanced laptop model, it will probably include a built-in Wireless Transmitter already. If it doesn't, you can purchase a Wireless Adapter that will plug into the PCI slot or USB Port. Once installed, your system should automatically detect the Wi-Fi Hot-spots and request connection. If not, you should use a software to handle this task for you.

Connecting to Wi-Fi Via Modem

To start a connection with a Wireless Router, you must first ensure that it is plugged into the Internet connection point. Turn on your external Modem before plugging the Router into your Computer via an Ethernet Cable. Then, switch on your Wireless Router and open your Internet Browser. You will be asked to enter in a Router IP Address.

The IP Address will vary, depending on the service you use. Users using Belkin should enter http://192.168.01.1. If you are a Linksys user, enter http://192.168.1.1. If you are not not using either service, enter the coed http://192.168.2.1.

Now fill in your Router's user name and password. Set your SSID (Wireless Capability) as active, and then type in the user name and password provided by your ISP and select either WEP or WPA Security. Then choose a New Passkey to finish the Wi-Fi Configuration.

Using Wi-Fi is like swimming in shark infested waters. The likelihood of getting hacked is probably over 95 per cent. We have seen examples of this in the news when the N.S.A. was caught spying on German Chancellor Angela Merkel and her closet advisors. WikiLeaks co-founder Julian Assange says that the N.S.A. intercepts nearly 98 per cent of South American communications.

Our Internet privacy and freedom of information is being threatened by Internet Service Providers (ISP) Technology Companies, The Government, (N.S.A.) Homeland Security, C.I.A.,F.B.I., and in my case the Israeli Mossad. We are all being spied upon.

That is why I have decided to write this book. We as a free nation can not allow a secret covert group monitor all of our actions. We can not let this happen. Even if you have nothing to hide, you still have the right to keep your personal sensitive information on the Internet safe from preying eyes.

Wi-Fi Connectivity

Before you begin using Wi-Fi to access the Internet with your personal sensitive information, here is something you should consider. Here are some of the organizations that are spying on you. I will also share simple steps you can take to protect yourself and your information. It's time to put the spotlight on the organizations who have been caught spying. No one has been caught more for spying than the National Security Agency (N.S.A.), But even outside of the United States of America, many governments have their own versions of the National Security Agency (N.S.A.).

The Most Prominent Ones Are:

- **The National Security Agency (N.S.A.)**
- **England's Government Communication Headquarters (GCHQ)**
- **Communications Security Establishment Canada (CSEC)**
- **Australian Signals Directorate (ASD)**
- **New Zealand's Government Communications Security Bureau (GCSB)**

Together with the National Security Agency (N.S.A.), they form the Five Eyes alliance. These government organizations regularly collaborate on spy programs with silly code names, example “You Dumb Schmucks.” But their work is no laughing matter.

But based on all of my years of experience monitoring covert Internet spying activity, the most ruthless of all is a little known group known as the Israeli Mossad. The Mossad spies on US. Citizens and all of our politicians throughout the Nation. For whatever the reason, the Israeli Mossad operates with immunity from prosecution. They are above the law. They operate in plain sight and hide behind their religion. It is only a matter of time before Americans connect the dots. Individuals such as myself will come forward and expose this group.

What really blows my mind is that the government can call upon Technology companies to learn about you and I. Although Technology companies such as Microsoft, Apple, Google and Yahoo don't want to rat out there own customers, they may simply have no choice. Just ask Steve Jobs of Apple who by the way after being visited from the Federal Bureau of Investigation and the National Security Agency dies from some mysterious exotic illness. It does make you wonder. I don't think Steve Jobs wanted to drink the Kool-Aid. It does make you wonder?

Here are some little known facts to think about before using Wi-Fi. Yahoo CEO Marissa Mayer said it's executives faced jail time if they revealed government secrets. Both Apple and Google track your phone's movements with location-based services. Apple stores your messages and whatever you store on the Cloud. Dropbox reads your files. Google sneaks code into advertisements that would install tracking cookies into user's devices without their knowledge. Through Android, Google knows nearly every Wi-Fi password in the world.

So, I now ask the 64 thousand dollar question, “What can be done to stop these massive intrusions of our Internet Privacy?” The answer is is very simple, never use Wi-Fi! Never surf the Internet with your Administrator Account. Only use a Standard Day to Day User Account with limited privileges (Parental Control). Use only a Guest Account with a USB Flash Drive to download Files. No one should ever sign on to the Internet exposing their Administrative account. There will be more on this topic in the following chapters of this book.

It has been my experience that because I value my computer and my personal highly sensitive information, I will never sign on to the Internet with my Administrator account. Unless I need to either update the software or make a purchase in a App Store or Software Center. I will only download approved and tested Software. I will never download third party software. Once the Application is downloaded, the hackers now have access to your Administrator Account. Never gamble. Always play it safe. Trust But Verify. When in doubt, don't click it.

The safest and best way to access the Internet is using a Live DVD Operating System. You can go to http://osdisc.com to purchase a Linux Operation System to use only when you want to go on to the Internet. There are at least 50 Linux Distributions to choose from. The Live Dvd's cost around 6 dollars. I recommend strongly purchasing Linux Mint 18.0 if you are a Microsoft user or Ubuntu 16.10 for Apple user's.

And for those of you who need more Internet privacy, I recommend purchasing a Tails Live DVD anonymous browser to surf the Internet from http://osdisc.com. Tails allows you to use GNP encryption when you are emailing or OTR encryption while instant messaging. Tails routes your Web connections through the TOR network by default. Tor offers a great degree of anonymity and privacy by encrypting your Internet connection and sending it through three (3) servers around the globe. Tor is a must for journalists and researchers who can not afford to have their information hacked. This is by far the best way to surf the INTERNET. Your Computer never has to be used on line. The only time you go on line with the Administrator account is do updates or install software.

I also recommend using the http://DuckDuckGo.com search engine and stop using http://Google.com for your INTERNET searches. Google likes to brag that there can predict within a month's time someone will go the store to purchase the searched item or buy it on line.

The best way to make any type of purchase on line is to make the purchase with a Gift Card. The Gift Card is backed by Master Card, Visa or American Express. It works the same as a debit card. The card can be purchased from any Walgreen's store. Remember, never use a personal credit card with an insecure Wi-Fi connection to make a purchase.

If you are planning to use Skype for Video Chat, try setting up the account as a Standard Day to Day user with limited privileges. If for some reason you are unable to do so, then install it with the administrator account. Once the software downloads to the Administrator account. Sign off the Internet. Shut down the computer and restart the computer logging in as a standard user. Then go back onto the Internet as a Guest or Standard user and complete the registration process. Upon doing so, you will be able to use Skype without compromising your Administrative account information. This method can also be used on Apple Face Time. I've used it several times under a Guest account. Using these tips could make your life much easier when chatting over the Internet.

In a brief few words “Wi-Fi is Spy-Fi.” Don't be fooled by anyone who tells you that it is safe to use. It is not! Based on what you now know, you should think twice before putting your personal information on the Internet. There isn't one employee who works for any of the government security bureaus that I have cited would ever use Wi-Fi to connect to the Internet. All of these governmental agencies warn each and every one of their employees about the dangers of this highly suspicious technology in a handbook. For those of you who would like to read what the NSA has to say about Wi-Fi, simply go their website and search for Wi-Fi or Bluetooth.

Our next chapter will cover the dangers of Bluetooth. This technology is totaled insure and has no password protection. It has a range of over 75 yards and anyone nearby can hack into your computer as your listening to music without you being aware of it. In the time it takes to listen to just one song, a hacker could have gotten into your computer and stolen all of your personal information. And lastly, if you were signed into your Administrator account they now have the password and can change it on you. How cruel is that? I know, I've had it happen to me. The next chapter will be about Bluetooth and should help make for a strong argument the importance of Internet security.

Bluetooth Connectivity

This chapter has been included to give you the reader a better understanding of Bluetooth technology, how it works, and how it can also be used against an unsuspecting citizen. I'll begin by asking the question, “So what is Bluetooth?” Bluetooth is a telecommunications industry specification that describes how Mobile Devices, Computers, and other Devices can easily communicate with each other using a short-range Wireless connection.

Early Bluetooth versions allowed users of Cellular Phones, Pagers, and personal Digital assistants to buy a three-in-one phone ex. Tracfone that could double as a portable phone at home or in the office, get quickly synchronized with information in a Desktop or Notebook Computer, initiate the sending or receiving of a Fax, initiate a Print Out, and, in general, have all Mobile and fixed Computer Devices be TOTALLY coordinated over a short distance.

It has been my misfortune to have had my Tracfone recently hacked. Therefore, I have first hand knowledge surrounding this topic to share with you. My Bluetooth settings had been mysteriously changed upon activation of the phone. My pass code had been changed and somehow after getting all of my personal information, someone called Tracfone and using all of my personal information convinced the Customer Service Representative to be allowed to change my telephone number on the same day I activated it.

Being organized, I wrote down the phone number in the Tracfone manual that came with phone. I then wrote down all the other pertinent information. Make, Model Number, Serial Number, Replacement Battery Model Number information, and Accessories that came with the Tracfone in the booklet.

After writing down all of the basic information in the manual, I wrote down the new telephone number and the customer service contact phone and then scotch taped the numbers to the back of the Tracfone. In that way, should I ever need to call customer service I would have my new activated phone number ready.

The next thing I did was call a couple of people with the new Tracfone and informed them that the number I was calling on would be my new phone number. Without giving out number, the area code was (917) 555-1212. I even got return phone calls from individuals who I had left voice messages on their phone for call backs.
I then created a two-step verification on a number of gmail accounts. Initially, I was able to receive the text code verification numbers to use to access my accounts. Shortly thereafter, I wasn't receiving any verifications to my gmail accounts and was now unable to sign in any of the accounts. This was a huge problem. How in the world could this happen. I thought having a Two-Step Verification would make my email account more secure. But what was now happening was totally the opposite.

In order to resolve this matter, I now had to contact Google and wait 3 days before having to send them personal information to unlock all of my gmail accounts. Patience is a virtue, so all I could do was wait for Google to get back to me resolve the matter. Within a week, all of my accounts on gmail and Youtube were once again working.

After discovering my latest Tracfone hack the idea for this book came into fruition. Being a truth searcher comes with a warning label: The Truth Can Get You Hacked Or Even Worse Killed. Nothing that happens is bad. It is only a learning experience that can be used to benefit others. Okay, let's get back to the story….

I now ask the question “Convenience or Personal Privacy?” Based on my personal experiences, privacy is more important than new fangled gadgets with the potential of being susceptible to “Man In The Middle” attacks by hackers within 100 yards of my home.

Here is another example that I would like to share with you. It is now possible for a hacker to sync a Wireless Keyboard with a Tablet-Style Device, such as an Apple iPod or Apple iPad. Let's say you have a Mac Book Laptop with a music library that you want to sync to an iPod or Ipad handheld device. An open Bluetooth setting can allow a hacker to get into all three devices without you ever knowing. That is why using an Administrator account to access all of your files, documents, or music can cause irreparable harm. I can not stress enough how important it is not to the Administrator account for any of your work.

There are numerous security risks using Bluetooth- ranging from the ability for a hacker to turn on the Computer's internal microphone to eavesdrop on your conversations. The ability to turn on the Web Cam and watch your every move, including watching you type a password into the keyboard. Hackers can also turn on and off any of the Apple Devices that are synced together. They can listen to whatever is being said or done in the privacy of your bedroom. They can even tune in using Siri when you and your significant other are in a moment of passion. How do I know this? Because, it has happened to me.

Here is another personal story that happened approximately two years ago. It was around 3am in the morning, and I was asleep. I was awakened by the voice of Siri coming from my iPad communicating with my Ipod. When I realized what was happening, I quickly turned off each device and went through all of my security settings. I was shocked to learn that all of my settings were changing on each device giving a hacker access to both my iPad and Ipod. But how could that be, “I asked myself?” The truth was stranger than fiction.

I visited the Apple store and spoke to a Genius to explain my dilemma. The Tech looked at me as though I had been drinking or smoking something hallucinogenic. The solution I was given get not make sense. The Genius returned the settings to the factory default and asked that I change my password. He tiptoed around what I had dicovered about Siri being used to bypass my passcode and access all of the functions on each devise. So, I decided never to use either device.

I then created a video that you can search on Google entitled “iPad Security Blues.” Not long after I created the video, I call Apple and retold my story giving them the link to my video. Within a couple of months, Apple admitting to having a security issue with Siri. They then cme out with a 7.1 patch to correct the problem. Sad but true. I kid you not.

The best way I can summarize this chapter is tell you the NSA bluntly sates in its security guidelines to never use standard commercial Bluetooth Headsets. People should understand the risks of using Blutooth. Bluetooth is Spy-Fi without the protection of being password protected with a short-range of 75-100 yards. Which means, that a man living in the next apartment or directly across the street can hack into your computer and you wouldn't even knew it. Unless of course, you were like me and purchased an Electro Magnetic Frequency (EMF) detector to send out a signal to catch the intruder's incoming radio frequency signal. I now know my Hacker. I even know his last name. I now have videos of him on my http://Youtube.com/StephensWorldTV channel for the world to see. You can find these videos under my Reality Surveillance and Meiscles World playlist to view. The video can also be found on my http://StephenSindoni.Webs.com site.

After going to the Police and informing them about this illegal surveillance and having my plea for help fall upon deaf years, I decided to put the spotlight on this illegal surveilance. Presently there are at least ten men who work around the clock trying to hack into my computer. There isn't a day that goes by that these hackers don't try to find another way to hack into my equipment. The challenges I face each day for the last twenty years has given a mountain of information to share with you. In our next chapter I will get into the Computer Basic of what I think each of everyone reading this book will need to know in order to keep their Computers safe from hackers and prying eyes.

Computer Basics

Here in the Computer Basics chapter, we will cover the following topics:

- Administrator Account/ Root User/ Super User
- Standard Account (Day to Day User With Limited Privileges
- Guest Account (With Limited Privileges)

What I am about to share with you isn't being taught to the best of my knowledge by any of the Computer Manufacturers. You would think that what I am about to share with you would be found in every Computer Operating System Manual. But it is not. Why? Because Computer Manufacturers sell Computers. Companies like Microsoft and Apple would rather sell you new and improved software or Anti Virus software that for the most part doesn't really work.

When I worked in retail electronics there was a standard phrase used by all of the salesman (RTM) which stood for READ THE MANUAL. Most of the customers who I ever came in contact with never took the time to thoroughly read the manual for the item that they had just purchased. Thus, I was not surprised when the customer came back to the store with the product demanding their money back. In those days, all salesman were on commission. Which meant, their sales number was on the invoice and they were informed over the loud speaker to report to the return department where they would find their unhappy customer with the product that they recently had purchased wanting to return it. The first thought that came to my mind was, “I would bet anything that the customer never read the manual.” Because if the customer had taken the time to read the manual, the customer would be knowlegable about all of the products features and nefits functions. The customer would be sitting at home enjoying the benefits of there product.

Let's say you just purchased a Hewlett Packard 15 inch Laptop Computer. When you start up the Computer for the first time you are greeted by a Microsoft Windows Operating System, ex. Windows 10. Following the instructions, you are asked to create an Administrator Account. In this example I will use johndoe. Next you are asked to create a password for the Administrator Account that you named johndoe. You now choose what you believe to be a very secure password, example 89Lv8Gy42Knt36./. The password consists of numbers, letters, upped case and lower case and symbols. This type of Administrator password would take a team of hackers a year to crack.

My advise to everyone reading this book to do when it it comes to an Administrator password is to change the password monthly and only use the Administrator account on the Internet to updates or to download software from a recognized Company in Apple's App Store, Microsoft's Software Center or from a Linux software center.

It is important to remember that the Administrator User, Root User, or Super User has supreme power over your system. There can only be one Super User. This account has total control over the Computer and all aspects of the system. This account can access any part of the file system, read, change, or delete any file; grant and revoke access to files and directories; and carry out any operation on the system, including destroying it if the Root User so wishes.

With this in mind, it is important that you do not work as a Root User because you might inadvertently cause serious damage to your system, perhaps even making it unusable. Instead, rely on Root only when you need to make specific changes to your system, example Graphic User Interface (GUI) customization that require an Administrator password. As soon as you are finished making all the necessary changes, sign out of the Administrator account and log out of the INTERNET. Then restart your computer and sign back in to the Administrator Account, example johndoe with the password that you have just created.

Once back in to the Administrator Account make sure that the computer is offline and you are not plugged into a wall outlet or using a wireless mouse. You'll need to go into the User Account settings to add a Standard User (Day to Day Account) with limited privileges.

1. You will create a New Standard User, example john. Then give it a strong password. You can even add a photo to the Standard john account easier to recognize. It should only time 5-10 minutes to complete the process.

Then log out of the Administrator Account and restart the Computer. After the Computer reboots the start up process, you will see a screen with both the Administrator Account and Standard User Account icons on the desktop. Choose the Standard User john account to sign on to the computer. Type in the password that you have just choosen.

The Computer should now log on to the Standard User john account. Here in this account is where you will do all of your work. You can customize the desktop to your hearts content. Remember to save all of your important information on an external hard drive or USB Flash Drive.

Guest Account

In order to create a Guest Account with standard limited privileges, you simply follow the previous steps when you set up the Standard (Day To Day) User john account. You can name the Guest account whatever you like. This account should also have a password. I recommend using this account to surf the Internet.

Should you need to save any files, documents, Videos, etc. you can transfer them to an external Drive or USB Flash Drive. Remember before logging out of a Guest Account, the Computer will give you a warning that upon shutting down you will lose all of the information for that session. So, please be mindfull to transfer all of your work before shutting down the Guest Account session.

Remember, never use the Administrator Account to surf the internet. Never use the Administrator Account to Download Files or Free Applications. If you must download anything off the internet use the Guest Account or sparingly the Standard User (Day To Day) account.

Should you experience a problem as a Standard User or Guest Account User, your entire Computer will not get infected by a Virus or Malware, only the Account that you are signed into will be affected. Fixing this attack is simple. Sign out of the affected account and then log off the Computer. Then restart the Computer remembering to be offline and then going back into the User Accouts settings delete the affected user and then recreate a new Standard User with a new secure password and your back in business. In this way, you will not see the Blue Screen of Death. Your Computer will be completely operational.

As a final note in this chapter, I recommend only a Computer with an ethernet connection behind a secure firewall. Do not use Wi-Fi at all. Do not use Blutooth for any of your devises. Do not use a Wireless Mouse. If you must use a mouse, use one that is hard wired through a USB Computer connection.

In the next chapter I will discuss Securing Your Computer. Here in this chapter, I will do my best to explain Computer Network Connectivity and the importance of keeping your computer safe from preying eyes.

It is my hope that everyone following along finds this information useless. Some of you reading along might think that you will never get hacked or that you don't have anything to hide. But the truth of the matter is, you're business is nobody else's business.

Securing Your Computer

No Computer with a connection to the Internet is one hundred percent safe. There is no way to guarantee the ability for a creative, savvy, hacker who is intent on getting into your Computer from gaining access to your system. Fortunately, there are ways to make it more difficult for the hackers. There are now software applications that will alert you when unusual traffic has entered your computer.

This chapter will cover a great deal of aspects of securing your Computer. It is my personal experience that a Linux Operating System is by far the best system for Internet security. I can proud to say, I am a Linux Operating System user for life. The reason for me is simple; Should you ever have a problem with a Linux Distribution, all you have to do is a Google search and you'll find the answer. Try that on a proprietary software like Apple or Microsoft Windows. Google will answer just about all of my questions and point me in the right direction one hundred percent of the time. Youtube is another great source for tutorials. Help is only a few clicks away.

I'd like to begin this paragraph by discussing what a Computer attack consists of. There are a variety of ways in which Computer attacks can be divided for classification. Perhaps the simplest dichotomy is to separate attacks as internal, which are Computer attacks done by someone with access to a Computer on the local network, and external which are attacks by someone with access to a Computer through the Internet.

Setting up secure passwords are important. Aso, encrypting the Hard Drive and setting up a Computer password to access the computer. This feature cen be accomplished by going into the BIOS and adding a log in password. In that way, anyone having physical access to your computer will need to have the Computer password before being given access to the Desktop Log In Accounts.

I strongly recommend following a Computer start up check list before using the system on the internet. Should you be dealing with important files and sensitive information, never ignore the internal threat. Yes, things are more difficult on the internal front, but users who sit inside your firewall are already past your primary source of defense, and, worse they might even have access to your Computer. And, it is for this reason, that I recommend only using a Standard (Day To Day) User Account with limited privileges when working offline on the Computer. Using the Computer in this way, reduces the risk of getting hacked from an internal or external source.

There are a couple more security tips we need to be mindful of. In the first tip, I will discuss is Wi-Fi Network Connectivity. So, what is Wi-Fi? Here is a basic description. Wi-Fi is a technology that uses Radio Waves to provide Network Connectivity.
A Wi-Fi connection is established using a Wireless Adapter to create Hot-spots- areas in the vicinity of a Wireless Router that are connected to the Network and allow users to access Internet services.

Unless, you need Wireless, avoid its usage; particularly if your machine is a server. Never plug a server into a Wireless Network Connection because it is riddled with security problems. My advise to anyone using Wi-Fi is if you are going to use it, then after signing off the Internet session, change whatever passwords that you logged into while using Wi-Fi on the Internet. One Access for each password. For some, that might mean changing passwords like you change your socks. And Lastly, remember to change your password while offline on your Computer bfore logging out. This is a great practice to get into. Alwys put Internet security first over convenience.

Because a Wi-Fi Wireless Network is very insecure, by its own nature, transmitting data even encrypted, it can be retrieved by remote devices, such as when using Bluetooth to connect to other personal electronic devices. Bluetooth has no password protection. Most people are totally unaware of the risk of using this communication technology.
I personally will never use Wi-Fi or use Bluetooth to connect to an iPod, iPad,Wireless speakers, or a Wireless printer. The only way I now go onto the Internet is using an Ethernet hard wired connection with a firewall connected to it as a Standard Account, Guest Account user. Knowing what I am about to share with you the reader, will explain why I have taken this position.

This may come as a surprise to some of you. The National Security Agency surveillance capabilities was recently revealed during Berlin's Chaos Communications Congress, including the agency's ability to hack private Wi-Fi Networks from up to eight (8) miles away.

Security researcher Jacob Applebaum co-wrote a Der Speigel Article detailing how the NSA intercepts new-purchased Computer products mid-shipment to install surveillance Malware before reaching the buyer. Applebaum went into further detail about the NSA's survallance vans and even drones that could be used to get within hackable range and Wirelessly deliver the software packages similar to Domino's Pizza delivering a Pizza. So, what is the NSA's mission in Domestic Intelligence? And more importantly what can we do to stop them? In order to stop them, you need to know how they operate to beat them at their own sick and twisted game. Information is power. I will now share more…

The NSA at Ft. Meade, Maryland has the most advanced Computers in the world. The agency's main responsibility in the US and the world is to ensure national security. NSA technology is developed and implemented in secret by private corporations, academia, and the general public.

The Signals Intelligence mission of the NSA has evolved into a program of decoding Electro Magnetic Frequency (EMF) waves in the environment fot Wirelessly tapping into Computers and track persons of interest with the electrical currents in their bodies, such as myself. Why? Probably because some of use refuse to drink the Kool-Aid. It might be because they think they are smarter than us. They have figured out a way to manage our money and now they are coming for our minds. These are the thought Police that author George Orwell warned us about in his book “1984.”

Signals Intelligence is based on the fact that everything in the environment with an electric current in it has a magnetic flux around it which gives off Electro Magnetic Frequency (EMF) waves. The National Security Agency (NSA) and the Department of Defense (DOD) have developed advanced digital equipment which can remotely analyze all objects whether they are manmade or organic, that contain electrical activity.

The NSA has records on all US citizens. The NSA gathers information on US citizens who might be of interest to any of the over fifty thousand (50,000) NSA agents. These agents are authorized by executive order to spy on anyone. I wonder which President signed the Executive Order to have the NSA and Israeli Mossad spy on me? My best guess would be Bill Clinton or George W. Bush were the men responsible for putting me under constant surveillance. I guess after writing this book and exposing a great number of their tricks, I will go to Washington, DC. or Trump Towers in New York to see President Trump and ask him to remove the Executive Order from the books, giving me clemency, to make me a free man as God intended for me to be again.

The NSA has a permanent Anti-Terrorist Surveillance Network in place. This Surveillance Network is completely disguised and hidden from the public. Thousands of persons are used as Spotters and Walk-Bys in Metropolitan areas following and checking on subjects who have been identified for covert control by NSA personnel. There isn't a day that goes by, that I am not followed, have my picture taken, or interrupted by a stranger trying to see what magazine I'm buying from Barnes & Noble. In my mind, I'm kind of flattered by the needless attention that all of these agents are giving me. It's like the papparazzi stalking the Hollywood celebrities taking a walk in public so they can take their picture or capture the lates t gossip for the tabloids or TMZ. They must think I look like Richard Gere…

The NSA uses techniques such as remote monitoring/tracking of individuals in any location, inside any building, continuously, anywhere in the country. A hand held device that resembles an iphone or iPad is there tracking device of choice. It is an inexpensive device for these type of surveillance operations that allow thousands of persons in every community to be spied on constantly by the NSA. To add to these numbers, there thousands of Hasidic Jews that are dressed in black hiding behind their religion. The Israeli Mossad has sent them to America to spy on all of gentiles. We the American public give these people a pass. If I had a dollar for every Israeli Hasidic agent that I have caught trying to do harm to me, I could retire quite wealthy. No, I am not Anti-Semetic. My mother was a Jew, her last name is Abrahams. Which makes me a Jew… Whether the Israeli Mossad like it or not. They are trying to do away with one of their own. I hold no grudges. God will judge each and every one of them. That is why I have choosen to speak out at this time and let my writing ability expose all there hidden secrets. In this book,I plan to tell it like it is.

And lastly, the NSA keeps track of all personal Computers sold in the United States. This in an integral part of the Domestic Intelligence Network. The NSA's Electro Magnetic Frequency (EMF) equipment can tune in remote frequency emissions from personal computer circuit boars (While filtering out emissions from monitors and power supplies. All of the never Computers will be made with solid state circuitry making easier to hack into the system. The best work around would be to use a computer with a rechargeable battery and only use the Computer with a charged battery and never plugged with the power adapter to a wall outlet. It Doesn't matter if you have the computer plugged into a surge protected, the NSA or Israeli Mossad will bypass the power strip and attack the computer.

So, what is the solution? For me, the solution was rather simple. Never use your Computer to go directly onto the Internet. Use a Live DVD and save your searches to an external hard drive or USB Flash Drive.

The best advice I can give you the reader is do the following:

- Always Use A Laptop on A fully charged battery.
- Disable Wi-Fi Connectivity.
- Disable Blutooth Capability.
- Only use a Live DVD Linux Operating System to Surf the Internet.
- Convert an older computer to a Linux Operating System.

Passwords

This chapter will cover how to create strong passwords and why this is so important. Choosing a strong password should be a top priority for everyone around the globe. Passwords should always be stored in a safe place. Once you have created all of your passwords, it is not a good idea to store your passwords on a USB Flash drive, external hard drive, or on the cloud. It has been my personal experience that you can be easily hacked using any of these methods. Therefore, I strongly recommend purchasing a 50 sheet spiral ruled index cards 3x 5 in size. You can get the white or multi-colored cards. I like using the Multi-colored cards so that I am able to create different tabs for each section, example Computer Passwords, Website Passwords, Email Passwords and important numbers for companies, such as Amazon, Paypal, or Ebay.

The method that I use requires using a pen and pencil to write down the information. The pen is user to write things down that will not change, as an example; johndoe@gmail.com. The password is always written with a pencil. The reason for this pretty simple, the User Email doesn't change, therefore it should be in ink. But the password might be changed on a regular basis. Using a pencil for the password allows me the ability to erase an old password and then write in the new password without a great deal of effort. Being organized is the key to good password management. Having the spiral 3 X 5 index cards allows me to easily open and close the book and be able to find all of my important information in one place. I do not have to go searching to find any of my personal information. Should I need to go on the Internet from a Hot-spot or in an airport, I can quickly access any of the information and be able to conceal the contents from preying eyes when using a Computer in a public place.

I strongly recommend creating passwords that are at least 15-18 characters long using numbers, letters upper and lower case, and symbols, example 15Cha6Num/Let.#87@. In this example, I have chosen to capitalize the C,N and L only. It's a good idea to change your passwords at least once a month, especially if you are using passwords over the Internet, example email.

One of the tricks hackers use most often to steal a password over the Internet is to trick the user when he or she is has just completed typing in their email address user name, example johndoe@gmail.com. Now I will explain how the hackers trick you into typing in your password making it visible for them to read. As you begin typing the password that normally is invisible for anyone to read, they flip the letters that you are typing in the password field and have appear in the Email User Name field.

Attacks like this are common for anyone who is using Wi-Fi or Bluetooth. One of the best ways to solve this intrusion is to simply slowly type in the Email User name and password one letter at a time at an extremely slow rate looking over the entire screen before typing each letter of your password.

Should you find that a hacker has flipped any characters of your password, quickly refresh the Computer screen and try signing in again to your gmail account. Another trick you might use is to type in three fake letters for the password as you begin typing, example ABC123 or XYZ456. This password protection hacker test should reveal if its safe or not to type in the real password. If it's safe to use, then erase the fake letters and type in slowly your correct password. Never rush to type in a password over the Internet to check email. A couple of extra precautionary seconds could make all the difference in the world. Patience is a virtue. It is better to error on the sign of caution. Remember, only fools rush in.

The Internet can be a dangerous place when the user is unaware of who may be lurking close by. Wi-Fi and Bluetooth connectivity are the main reasons for Identity theft and credit card fraud. Once a hacker gets a hold of your personal banking account information they can easily clean out your checking and savings account.

Do not use the Administrator account to surf the Internet. As I have previously stated, sign in as a Standard User or Guest User Account. Should you really want to safe, as I have also previously stated, Use a Live Linux DVD to surf the Internet. They are easily easy to use. You do not have to install the software to use it. This is for me the best and only way to surf the Internet. Should you need to download any files, or documents off the Internet, you can download them to the download folder and then transfer everything that you downloaded to the computer and then attach a external hard drive or USB Flash Drive to transfer all of the information from that Computer session.

In the next chapter, I will expand on why I have personally gone away from using Microsoft Windows or any type of Apple Operating System. The best reason that I can give for me making the switch to a Linux Operating System, is that there were too many times that my Microsoft Windows based Computers and my Apple Operating systems were hacked. In every adversity there is a seed of befit to be derived from it. For me, it was learning how to use Linux and then detoxing myself from the conventional hackable operating systems. The switch to Linux was an easy one. Here isn't any software that I am deprived on a Linux System. All of the thousands of software applications are free. Could use ask for anything more? Paying for for Apps can become quite expensive.
In this economy, it's not how much you make that counts, it's how much you can save.

Internet Freedom

After being hacked a great number of times using Microsoft Windows and Apple Operating Systems, I came to the frustrating conclusion, “There had to be an alternative to these invasive and easily hackable operating systems. I began my search seeking a solution to this Computer chaos. It was at that moment that I remembered a conversation that I had with a man that I had met while traveling back to California. After explaining to him what I was experiencing using Microsoft Windows and Apple Operating Systems, the man told me that if I wanted the hackers to stop, then I needed to learn Linux. This was like a light bulb being turned on in my head, the lights were on and fortunately someone was home. That someone was me.

I began doing a Google search typing in many variations of Linux Operating systems to accumulate as much information that I could possibly find about Linux. My Google search returned hundreds of results surrounding Linux. The Google search revealed that there was a viable alternative to the proprietary computer operating systems that I had grown up on. The information was so important, that I purchased a composition notebook with section tab dividers to label and categorize all of the important information that I could easily reference later.

Being a visual type of guy, I searched Youtube for tutorials on a Linux Operating system. Was surprised to learn that there were many different Linux Distributions to choose from. After doing a thorough search, I found three Youtubers, one of which was Joe Collins who was very proficient using Linux and was an excellent teacher explaining the Computer Software. I then downloaded a number of his videos watching each one at least three (3) times. Inventor Nicola Tesla would read things three times to solidify the information to memory. Albert Einstein would also use the magical mystique of the number three. If it worked for theses great thinkers, it should work for me.

I then put myself through twelve (12) rigorous weeks of intensive Linux training Boot Camp. I was amazed to find an unbelievable amount of information on Linux Operating systems. There was far more information on Linux than there was on Microsoft Windows and an Apple operating system combined.

I remember going over to the wall calendar and marking the date that my Boot Camp Linux training was to begin. It was my goal to set aside two hours each day to watch tutorials and set aside one hour each day to adding information in the category section of my notebook. I would review each section daily to solidify the information in my mind.

The first chapter in the composition note book was titled “ What is Linux?” I will begin by providing a definition for a Linux Operating System and its history. I will also explain the differences between a Linux Operating System and the Microsoft Windows or Apple's Unix based Operating systems.

Linux is the core or kernel of a Computer Operating system, first developed and released by Linus Torvalds in 1991. Linus Torvalds hold the rights for the Linux trademark. Throughout the years it has been improved, refined, and distributed by Debian, Canonical, Red Hat, Linux Mint and many others.

The Graphical User Interface (GUI) as it is referred to is the brainchild of Richard Stallman, the founder of The Free Software Foundation. The GPL is the guiding document for Linux and its ownership, distribution and copyright. Richard Stallman and Linus Torvalds both agree that the software will always be free.

What I was pleased to learn, was that millions of people around the globe had been using Linux for over twenty years. There were no licensing fees, and you could download the software to multiple desktop computers and laptops with a single Live DVD. Linux could also be used on server platforms. Linux even provided a Royalty Free platform.

What was even more impressive was that IBM was using Linux on its entire Computer product line. Another little known fact was that ALL of The World's Super Computers were operating on Linux. Even the US government was using Linux on all of its Submarines and Space Station. These were some very good reasons to switch to a Linux Operating System.

The clincher for me was that you didn't have to install a Linux Operation System on a computer to use it. The Live DVD gave everyone the ability to try it out first to become familiar with it. In theory, I could learn at my own pace before ever deciding to install the Linux Operating System on my computer.

What made the switch easy for me was that there literally thousands of websites that exist with information about Linux and well over fifty of its distributions, such as Ubuntu, Ubuntu Mate, and Linux Mint. I mention these three distributions primarily because of their ease of operation, Internet Security, and user friendly graphic desktop customization. Getting help was as easy as joining a local user group. How cool is that?

For any of you readers who are Techs, you would be happy to learn that Linux Operating Systems allow a person the ability to see code. Linux also allows anyone to change code. Simply doing a Google search for a Linux Operating System manual, example Linux Mint 18.0 (Sarah Edition) will take you to a page where you can download the manual to your computer. There is also a handy help guide that comes pre-installed with the software.

Being a bit conservative, I spent approximately three months getting familiar with a number of different Linux distributions. Doing a Google search on the top 10 Linux distributions, revealed a list of the most popular Linux distributions. I read all of the comments pertaining to the software. Narrowing down my list, I had over a dozen Live DVD's to choose from. Each distribution had its merits. I then went on line to http://osdisc.com to purchase the Live DVD's to try out. Basically, it came down to my personal needs and what would work best for me.

The next thing I did was go on Ebay to find a used Hewlett Packard 14" Laptop Computer that had a Microsoft Windows 7 Operating System on it. I was able to find one for around two hundred and fifty dollars in mint condition.

When the Hewlett Packard 14 inch laptop Computer arrived, I followed these easy steps:

1. Plugged The Laptop Computer into a Electrical Power Strip.
2. Hold down the power button on the Computer.
3. Manual opened up the DVD Tray Door.
4. Inserted the Live DVD into the Tray.
5. Manually Closed the DVD Tray
6. Turned off the Computer (Holding Down the Power Button)
7. Restarted the Computer by manually holding down Power Button.
8. Then holding down a function key- (in my case HP's Key was F8)

Note: Depending on the Model of computer it might be, F2,F8,F8,F10,F12,ESC, or Delete. You may have to shut down and restart a couple of times before you see a command at the very bottom of the desktop screen the function command, ex. F8.

After receiving the placed one of the Live DVD's into the DVD tray and proceeded to check out the Linux Mint 17.0 Operating System. Everything checked out when viewing the software. I was now ready to select the Install button and erase the Microsoft Windows 7 Operating System Software.

The Navigation Screen (BIOS) Bypass Input Operating System appears. Then following the instructions using the arrow keys (Left, Right,Up, or Down) to change the Boot Order. As an example, Internal CD Drive. Once selected hit F10 to Save the Boot Order instructions. Then hit the Enter button on your Computer.

Final BIOS Instructions.

1. Then turn off the Computer Manually.
2. Restart the Computer Holding down the Power Button.
3. Computer will now Boot Up recognizing the Internal CD as Primary Source
4. For the Installation you must be hard wired using an Ethernet Connection.
5. You must have the Computer fully charged or plugged into Electrical outlet

Note#1: The Linux Mint 18.0 Operating System will Boot Up and you will be follow the basic instructions creating an Administrator User Name and strong password.
Note#2: Having an Internet connection enables you to get all updates for the software.
Note#3: Software should take approximately 45 minutes to install.
Note:#4 Updates could take as long as 15 minutes to install.
Note:#5 Take time to check out the software center to download additional Applications

Remember: There are thousands of free software applications to choose from.

For those of you who do not want to install the software simply select the try option and you will be able to use the Linux software without doing a full installation. It is a good idea to use the Live DVD when planning to go onto the Internet. As I have stated before, it is the safest way to surf the Internet. For some of us, it is the only way to use the Internet.

Before signing off the Computer, attach a USB Flash Drive or External Hard Drive to the Computer to transfer all of the information from your Internet session onto the device. Then log off the Computer. There will be no trace on your Computer that you have used the Computer to access the Internet. As mentioned earlier in a previous chapter, use a Tails anonymous browser should you need more Internet privacy.

After you have installed the Linux Operating System, refer to the Securing Your Computer chapter. Then follow the easy step-by-step instructions to set up a Standard User (Day To Day) Limited Privileges Account and a Guest User Account. Within a matter of days, you'll be enjoying your new found Internet Freedom.

External Hard Drive

In this chapter, I will discuss the importance of reading the manual (RTM). I will also share valuable insight into getting the most out of a External Hard Drive device.

Security is the key to keeping your information away from preying eyes. The External Hard Drive must have a strong password. I can not stress that enough. “It is better to be safe, than sorry.”

People are “Creatures of Habit,” I am sorry to say. Most people are lazy. Yeah, I know some of you will say, “I'm just too busy to take the time to Read The Manual (RTM). They might even say, “The External Hard Drive I recently purchased did not come with a manual.

During my career as a Electronics Product Sales Counselor, I heard countless reasons given by the customer why he or she did not Read The Manual (RTM). It was my observation that most of the electronic products that were returned to the store were not defective. The products were returned primarily because the customer never took the time to read the manual that in most cases, came in the box with the product.

Many “Open Box” returned items that were determined to be operational, could not be sent back to the manufacturer for a store credit. The products had to be sold at a discount and categorized as “Open Box Merchandise.”

Another one of my observations, was that many of the Sales Counselors never read any of the manuals of the products that they were selling to the customer. Therefore, it was impossible for any of the Sales Counselors to intelligently explain the features, functions and benefits of the products they were selling. This was for a Store Manager a telling sign that his Sales Counselors needed additional product training. This in my opinion was the main reason for lost sales.

As a customer, I was always looking to save money. Returned items (Open Box Merchandise) was a great way to save money. It was my experience that more than likely the Open Box Merchandise that was returned to the selling floor, was going to work nearly one percent of the time. The stores all had a seven day return policy, provided that the customer had the receipt, the box, the product, and all of the items that came in the box, with the packaging. Then, they could get their money back or a store credit to purchase other products. As a Sales Counselor, it has my experience that if the product was defective, it would happen within the stores seven day return policy.
Here now is a good example of what steps I took when exploring all the possibilities to purchase the right External Hard Drive with all the right specifications needed.

The first step in the discovery process was to do a Google Search using the term "Top Five External Hard Drives Sold." The Google search returned at least ten (10) manufacturers of External Hard Drives. There were so many choices. Which External Hard Drive should I choose?

I began reading some of the customer comments to find out what each customer had to say after using the product. Reading over all of the customer comments, I was pleased to learn one of the most reliable External Hard Drive Manufacturers was by a company named Western Digital.

Surfing the Internet, I typed in Western Digitals URL, http://support.wdc.com and was taken to the site. Once on the website, I jotted down the "Toll Free" Technical Support phone number, 1 (800) 275- 4932. Within a matter of minutes, I was able to find the right External Hard Drive to fit my specific needs.

One of the things that I was most suspicious of, was having my new Western Digital External Hard Drive intercepted by the NSA in Mid-Shipment. So, I decided to take all of the information that I had written down about the products and visited a nearby electronics retailer who was the recognized authorized distributor for Western Digital devices.

Entering a "Best Buy" Electronic Store, I was able to find the right Western Digital External Hard Drive. I purchased two hard drives in different sizes. The salesman made me a great deal on both devices. I was given a store discount which made the trip to the store well worth while.

When I returned home, I opened the Western Digital External Hard Drive box. I purchased the My Passport For Mac version. I then removed the shiny red Western Digital External Hard Drive from its plastic mold and did a physical inspection of all the components that came in the box with the product.

Now holding the External Hard Drive in my hand, I turned over the product to write down the products serial number in a notebook. Also including the make and model number with the manufacturers Technical Support telephone number. Thumbing through the box, I could not find the manual. The only items in the box, were the product, the limited warranty guide and a tiny My Passport For Mac booklet that contained pertinent customer service information.
After discovering that the Western Digital External Hard Drive My Passport For Mac was missing, I went on line and visited the Manufacturers website and downloaded the manual for the product that I had purchased.

I then opened the PDF document that I had just downloaded and began reading the manual (RTM) to learn about the features, functions, and benefits of the product. I then saved the manual in my documents folder, which I planned to transfer over to the new External Hard Drive after it was operational. In that way, should I ever need to refer to the manual, it could easily be found in a folder directly on the External Hard Drive itself.

Next, I opened up my products notebook and turned to the Western Digital information products page and called the Western Digital Technical Support “Toll Free” phone number to talk with a technical support technician to register the product.

Listening to all of the automated telephone prompts, I choose the correct number that corresponded to registering the product. I was now directed to a customer service technical support representative. I was greeted courteously and asked for the serial number of the product. Having the information handy, I verbalized all the numbers of the products serial number.

The Representative verified the product serial number and then informed me I needed to go to the Western Digital website on line and he would then ask a couple of required questions needed to complete the registration process. Following his instructions, I answered all of the Representative's questions. Shortly thereafter, I was told by the Representative that the registration process was now complete.

The Representative then explained the product warranty information. He then informed me that I had thirty (30) days of “Free” product installation Technical support. He next asked, “If I needed help with the Installation of setting up the External Hard Drive. I then answered,”Yes.”

Without going into all the details, the Representative guided me through the installation. Once the installation was done, the Representative assisted me in creating a strong password for the External Hard Drive.

It was now time to test out the new External Hard Drive. The Representative asked me to drag and drop a file into the hard drive. I then went to my documents folder and selected the Western Digital product manual file and dragged it onto the External Hard Drive.

Following the Representative's instructions, we then checked the External Hard Drive for the file. Once in the External Hard Drive, we located the folder, selected it, then opened it to reveal its contents. There it was, the Western Digital External Hard Drive manual. The External Hard Drive was functioning properly. I was now good to go.

Based on my Western Digital Technical Support telephone experience, I can strongly recommend the company to anyone who needs to purchase an External Hard Drive. It was a pleasure doing business with the company. The Technical Support Representative whom I had the pleasure of working with, had a strong knowledge of the product and was very professional in his approach when dealing with my situation.

In these final paragraphs of this chapter, I felt the need to go through the entire thought process to help you the reader better understand the required steps taken by me from beginning to end. I tried to do my best to use simple every day language to explain the entire customer buying process with grace and ease.

It is my belief that keeping it simple makes it much easier for everyone to understand. I follow the motto “Keep It Simple Stephen” or (KISS) as most people who know the acronym prefer to call it.

I will end the last paragraph with the phrase “The difference between knowledge and wisdom is knowing what to do next.”

Below The Radar

We have come to the conclusion of this book. I have gone over a great deal of information. It is my hope that you the reader, have found this information useful. Most all of the security tips will not be found in any literature created by any of the Computer Manufacturers or any of the manufacturers of electronic devices. You will not find any of this information in their manuals, on the Internet, or anywhere else for that matter.

As I mentioned earlier, the Computer manufacturers are only interested in selling equipment. It is not their job to educate you the consumer. Why should they? It is our responsibility learn as much as we can about the electronic products that we purchase. It has been my experience that "Reading The Manual" (RTM) is the key to becoming proficient in anything you are attempting to do.

Many of the things that I have shared with you have come from my own personal experiences with Computers and interconnected electronic devices. Life experiences can be some of our best instructors.

In closing, I would like to thank everyone who has taken the time to read this book.

Respectfully,

Stephen Sindoni

References

1. **Hewlett Packard - www.hp.com/us**
2. **Linux Guy Guru - http://LinuxGuy.Guru**
3. **Linux Mint - http://LinuxMint.com**
4. **OSDisc.com - https://osdisc.com**
5. **Ubuntu - https://Ubuntu.com**
6. **Ubuntu Forums - http://UbuntuForums.org**
7. **Western Digital - www.wdc.com**
8. **Wikipedia - https://enwikipedia.org/wiki/linux_usergroup**
9. **Stephen Sindoni - http://stephensindoni.webs.com**