THE SECRET OF SAFE PRIVACY

Virtualize your online activities and keep your privacy in a secure environment

OLIVER A. WARNER

THE SECRET OF SAFE PRIVACY

support@mysafeprivacy.com

“Virtualization doesn’t just complement our computers, it completely evolves the way in which we use them, providing safety and privacy on a virtual environment while protecting our most valuable information...”

Oliver A. Warner

About the author

Hi there! My name is Olive Warner and I am an IT professional who has been working in the IT industry for almost 20 years and for different companies in Europe and the United States. Mainly focused on large and complex systems infrastructure, I have spent a large amount of time offering direct support to users, helping them to follow best practices, improve their productivity at work, and troubleshooting all kinds of different problems and challenges they have had, with the main objective to make IT easy and a great experience for them.

During my career I have helped hundreds of users with their IT needs and to recover their computers from “important” malware infections, and have showed them different techniques to achieve certain privacy on their computers.

One of the main questions I keep getting from users is what they can do to efficiently protect their systems from being infected, and wondering what Antivirus I recommend to keep their systems safe.

I am tired of seeing how nasty viruses damage people’s systems, impacting their lives by losing their very important and valuable data. Yes, an Antivirus is always recommended and you shouldn’t run your computer without one, but they are not the ultimate solution in protecting your computer.

I want to show people a completely new way to browse the internet safely and privately. This has motivated me to write a short book to teach you this sophisticated method, so you can learn how to quickly and effectively implement this solution for you.

I am very happy you took the step in taking the time to learn and being willing to implement this solution. I really hope you find this book interesting and that it helps you improve the way you use your computer.

Introduction

For years I have seen users have very bad experiences with their computers. They have lost very important and valuable data that was not possible to recover, and that caused a lot of frustration and stress to them. Besides that, they had to spend several hundred dollars in order to have their computers repaired and back to normal.

There are two major things users can do to protect their computers and their data:

1- Keep your computer out of risk. This will automatically put your valuable data and information into a safe bubble that will not be reached by threats.

2- Back up your data. This will ensure your data is recoverable under any

circumstances.

In this book we are going to focus on step one—keeping your computer out of risk by using a technique that you probably you didn't know you could use, or even exist.

Not everyone is a victim of severe malware that will destroy their system, but it is true that millions of users have had very bad experiences on their computers because of nasty threats and the consequences have had a terrible impact on them.

The point is to avoid the odds and make sure you will never be a victim. If you take the necessary preventive steps, you will ensure your computer's protection and you will learn how to do it in this book.

This same solution will help you to keep your computing activities private, just to you, in case you are sharing your computer with family members or friends.

We all need time for us, just us, and this can be in very different ways, but if you are looking for privacy and making sure that no one who accesses your computer can track what you do on it, you are about to discover the best way possible to achieve this.

The objective of this book is to offer you two solutions—to achieve privacy in your computer, and to ensure that your internet activities will not endanger any valuable data stored in your computer.

Information Technology (IT) may be a boring subject for a lot of people, but you have to know that IT can help make your life easier if you use your computer in a smart way.

This book will expand your knowledge about computers and IT in a very fast and easy way. You will learn a technique that businesses and corporations have been using for years to reduce their IT costs and help their productivity.

Now, this solution will help you to use the same technology and take advantage of its benefits on your own computer, helping you to achieve the next level in your computer skills.

Surviving the Online World

The internet… that fantastic portal that expands our freedom into an endless world of information which blends reality with fiction.

These days, we use the internet for multiple purposes and from different places, mostly from home and work. The internet is a great tool that, if properly used, can help people at work or

while studying, keep us well informed, communicate with friends and family, research unlimited information, and with a ton of other activities that are useful in many ways.

In today's internet, it is very easy to go onto websites that can harm your system without spiking any kind of suspicion in you. While there are websites that are obviously not legit and can spark a defense mechanism in users, there are other websites that are very well designed to look professional in which you may think you are safe. By navigating these sites, you may get software threats installed that will eventually corrupt your system.

When we browse the internet, we are taking our computers on a very dangerous journey, in which being safe is not warranted, but that's not to say it's impossible.

The most known way to have a certain feeling of protection in our systems is to have an antivirus. It is genuinely true that an antivirus will give our systems some kind of shield that will block a large number of threats, and it is always recommended to have an antivirus installed in your computer. There are hundreds of different protection tools. Some work better than others, and while some are free, most of them require payment and yearly renewal.

Imagine that a computer is like a human body. People get sick because we are infected by viruses, germs, bacteria, etc. We are also capable of avoiding certain illnesses because of vaccines, which will prevent certain infections from hitting our immune system. However, there are hundreds of viruses that we can get infected with and we will need medicine in order to get cured from those.

Unfortunately, there are multiple viruses or illnesses that can be fatal for human beings that no medicine can help. The same happens with computers, but on a higher scale.

Every day, when people leave the safety of their home and walk into the world, they are exposed to all kinds of viral threats. We have a strong defensive system that is capable of fighting and defeating most threats and that is the reason we don't get sick often, as our body is capable of protecting itself from numerous threats. "Keep talking about this…"

The same thing happens with computers, when we take them into the internet, we expose our systems to threats, and we put our valuable information at risk by exposing it to threats that are looking to get into our personal information and valuable data with the only purpose to infect, steal, or destroy it.

In this book, you are reading about threats, viruses, malware… as you may be a little be confused, I am going to give you a quick overview of each threat that can harm your computer.

Threats, Malware, or Viruses are the most common names you may hear when referring to computers. Malware is the general name that refers to internet threats, and it can be all kind of viruses, Trojan-Horses, Keyloggers, Worms, Spyware, Adware, and the newer Ransomware.

- Viruses: software code that is capable of reproducing itself, which usually has a harmful effect, such as destroying your data or corrupting your system.

- Trojan-Horse: inspired by Greek Mythology, a Trojan-horse is a program that will be installed silently in your computer, and it is designed to breach the security of your system. Once it is installed in your system, it allows other users to hack into your computer to steal or delete your data, corrupt your system, or just spy on you.

- Keyloggers: usually this software is installed by Malware, but it also can be installed by other users. Keyloggers, as the word indicates, log any single key you press on your keyboard. It captures usernames, passwords, credit card numbers, and any other thing you may type in your computer. We will talk more in depth about Keyloggers and how to protect your bank access from them.

- Worms: similar to viruses, a worm is also capable of self-replicating, using your computer's memory. Worms will not alter your files, but over time, their uncontrolled replication will consume your system resources, negatively affecting your computer performance, slowing down your system's tasks, and impacting your activities.

- Spyware: also known as Spybot or Tracking Software, this is a piece of software designed to secretly gather information from your computer and send that data to third parties or interested organizations.

- Adware: software that installs on your computer and will automatically display unwanted advertisements, or may advise you about fake virus infections. Adware infections can be very dangerous, as they can infect you with more hazardous Malware, or may request money in order to remove the fake infection that it claims exists.

- Ransomware: this is the newest Malware added to our cyberspace, and the systems being affected by this new threat are growing exponentially. The number of infections of this threat has gone up 176% since 2015, and the reason this is becoming very common is because there is money involved. You will learn about this thread in more detail in the next pages, but basically this malicious software will encrypt your data or block access to your computer and will ask you for money in return for having your data or computer back.

Now imagine that you can do your online browsing or activities in a separate environment and use the internet in that environment; a system in which you don't need to be concerned about getting threats, losing data, or breaking your computer.

So, you may be thinking, what internet activities should I separate from my computer? The best answer I can give you is all of the ones with which you actually interact with the internet, which includes, email, social media, chatting (IM), video/music streaming/downloading, online gambling/trading, searching for applications, and internet browsing.

Let's get a little bit deeper into these online categories to understand how they can expose your system to different threats.

Email

Email..? Really? YES! Unfortunately, email is still a very powerful way to massively spread viruses to innocent users. Dangerous emails that can literally destroy your computer's Operating System are usually received from unknown senders, but also from friends and family.

Don't blame your best friend, your sister, or any other important person in your life for sending you a nasty virus. They don't even know it until it's too late. Viruses already installed on computers can use a user's email to auto-send emails by using their email contacts. This can happen to you, your friends, and family.

Have you ever received a strange email from any of your friends or family members? Like a nonsense, weird email that doesn't match your friend or family member's personality? If so, what have you done? If your answer is "I called my friend and asked…" Congratulations, then you probably just removed that email. However, you may have opened the email, just because it came from someone you trust. Unluckily, in that case you may have been infected and most likely will start experiencing poor computer performance.

This kind of emails, though, are most likely to come from unknown senders. While most of them will be detected as spam, some pass the defense barrier and hit your inbox, making you think it is a legit email and safe to open.

These emails come with attachments in the form of an application or any kind of executable file, that once you click to open, it will infect your computer with a Trojan-horse, virus, worm, or any other type of Malware threat that can totally destroy your computer.

Social Media

Stop being social on the internet, it is a trap! Just kidding. This topic may be a little confusing but it is actually very simple. If you are asking yourself if you can get malware threats through social media sites, the answer is yes. But let's get into detail to clarify.

If you are using any of the most common social media services, their websites themselves will not infect your computer directly. Browsing their website is totally safe and if their systems are hit by any threats, they will solve the problem before those threats can hit your computer.

So, where is the danger? It comes from the users that participate on the social media sites, and the information they can post in there and share with other users.

If you participate in any or multiple social media sites, you may belong to different groups related to different topics in which users share information. Unfortunately, cruel and malicious people exist online as well. Those users are called Scammers, among other names, and they will try to lure you and other users to click a link they post in a message, and by clicking that link you will leave the safety of the social media site, as that link will lead you to an external website and will expose your computer to a potential Malware infection.

The most common social media sites are Facebook, YouTube, Twitter, LinkedIn, Pinterest, Instagram, etc. Their service and websites don't represent a risk to you, but remember that users share information on these sites, and that information can lead you to other websites that are not related to these social media sites.

Chatting (IM)

Similar to social media, participating in Chatrooms can be a potentially dangerous activity, because you are interacting with other users.

Chatrooms are shared with hundreds of users, and usually rooms are set in regards to specific topics. Scammers can use these chat rooms to target users with a specific interest and lure them to their websites with the final goal of either stealing information or infecting or hacking your system.

Besides Scammers, there is also this type of users that, just for fun, send threats to other users to infect their computers. Usually those users can be very sympathetic at first, to generate some kind of trust, the same way a Scammer would do, then send you a file with the excuse of being a photo of him/her, a music clip, a document, whatever kind of file, that will infect your computer once you try to open it.

Their only purpose by doing that is to try to hack you, by using a Trojan-horse. With this kind of Malware, they can gain access to your computer and spy on you, even use your webcam, steal your information, or completely delete your data or destroy your system by doing a complete hard disk format. Scary if they get into your primary system, isn't it?

Don't worry; the solution to fight back these online terrorists and defeat them, even if you fall into their trap through chatting or social media, will be explained in the following chapters.

Video/Music Streaming/Downloading

Have you ever been researching for your favorite music or movie clips? If so, hunting down your favorite music or videos is not free of danger.

Nowadays, there are very good source websites to safely stream music or videos, but searching for them when you don't know where to go can be quite dangerous.

There are hundreds if not thousands of websites on the internet that you can stream or download music and/or movies from. A big portion of those sites are illegal resources for movies or videos and it is very easy to come across them.

Browsing these sites in search for your music or movie, besides the hassle it takes to find what you are looking for, is extremely dangerous due the amount of ads on these sites, most of them being adware, advertising you fake products, software updates, fake antivirus alerts, etc.

The real danger in this type of websites is that malicious software can be installed into your system when pop-ups from the site open, even if you don't click on them. This is a fact, and a problem that you can find on many websites on the internet.

Online Gambling/Trading

Money, money, money… Las Vegas is not the only place for gambling—the internet is a great place for gambling as well. There unlimited websites, services, and applications for gambling online, and guess what? Online gambling is not exempt of danger for your system and your data.

Gambling and trading online is one of the highest activities in this new era of technology, and because of that, users looking for these services may be victims of all kind of scammers and malware if they go to the wrong websites.

Searching for Applications

Installing software is what computers are about. We install applications on our computers in order to have a set of services and tools available to us to perform multiple activities of our interest.

Unless an application you are looking for comes from physical media like a CD/DVD or USB pen drive, you have to search it online. Applications can be found on the internet from secure and non-secure sources. Also, applications can be downloaded by using P2P

applications.

Searching software on the internet or through P2P applications can be a dangerous activity as well, as depending the type of software you are looking for, you can be surfing on very hazardous websites that will infect your system as soon as you try to download something from them, or just by pop-up windows when browsing the site.

P2P applications are risky as well, as you may perfectly download fake or non-legal software from other users, which may be infected with malware and will infect your computer when you execute the related files.

Internet Browsing

This probably is the primary activity we all do on the internet. We browse the internet for multiple things like work, study, or entertainment.

Practically all of the categories we just talked about can be gathered into the topic of internet browsing, as this is what we do in order obtain what we are looking for on the net.

Depending on the type of content we are looking for, this can be when we can get onto very dangerous websites. There are red flag categories; most of them we have already talked about, but we didn't talk about pornography.

Statistically, pornography is one of the primary categories users are interested in when researching the internet. Pornography has risen exponentially on the internet over the years, and if you are one of the users interested in that topic, you should be extra careful when surfing porn sites, because you may be placing your system and your valuable data at high risk, turning a great source of entertainment into a real nightmare.

If you land on the wrong website, that may not just cost you the loss of valuable data, but a lot of money in order to have your system back.

You may be overwhelmed with all the information you have learned after this chapter. You have probably realized how dangerous some of the online activities you do on daily basis can be to your system and your valuable data.

You may be asking yourself what can be done to overcome this situation and have a safe environment in which you don't expose your system and information to these threats. You may have already an idea, after reading the introduction of this book. Just keep reading to keep learning.

With the method that you are about to learn, if you get any threats, your computer will not suffer any consequences, will not ruin your system (which would make you spend money on

repairs), and, most importantly, will keep your data and information safe and out of danger. Not to mention that recovering that system would take you literally two minutes to have it back to a healthy state.

Does it sound impossible to you? Uhmm… are you thinking this is a sales technique? Haha… not at all! Actually, you will realize you will be saving money while using your computer more efficiently. You can even move to a free antivirus if you are currently paying a subscription.

The fact is, you can achieve a very good solution completely free and legally, but we will talk about this later on.

Virtualization. What is it?

Virtualization is “magic” in the IT world. It allows computers to duplicate into multiple virtual computers. This means you can run multiple and independent computers at the same time and from a single physical computer.

You may have heard about Virtualization, but never really thought about what it is and what it does. Even you may have confused Virtualization with Virtual Reality.

Virtualization changed the IT industry. It allowed corporations not to just save big amounts of money, but to reduce the amount of energy used and to help companies go green.

Before the Virtualization era, companies were running under regular physical servers. The bigger the company, the more dedicated systems were needed to run the company’s IT infrastructure.

For example, a company with 10,000 employees may perfectly have 600 servers in production needed to run their business successfully. Let's set an average price per server around $5,000. With this pricing, it would cost $5,000,000 just to purchase 600 physical servers, plus the cost of energy consumed, and maintenance needed.

With Virtualization, you can have 30 physical servers, instead of the 600, and then run 20 Virtual Servers on each. That makes the total of the 600 servers needed to run the company’s business. If we calculate the cost again, 30 servers at $5,000 would be $150,000 in physical servers cost, with a big reduction on energy consumed and maintenance needed. You get the idea, right?

Virtualization is a very important investment companies use for their IT infrastructures, but it is also a great investment for you at home. Companies invest money to virtualize their

environment, but virtualization at home has no cost and the only investment needed is a little bit of your time to create the proper environment for you.

Yes, you read it right. Using virtualization at home has no cost. Well-known companies from the IT sector offer a free version of their software (called Hypervisor) for personal use, so you can take advantage of Virtualization at home and use its benefits for totally free.

You may be wondering how you can deploy this technology if you don't have any IT knowledge. This book will give you the basics, help you to understand the concepts, and finally teach you how to deploy your first virtual environment using the detailed "how to" guide that comes with this book.

Before I move forward on this topic, I would like to introduce you to some basic virtualization concepts and a glossary of terms, so you are familiar with them and better understand the overall basics of Virtualization.

- Host, or Host Machine: the physical computer which hosts one or more Virtual Machines.
- OS, or Operating System: the main software installed on your computer that supports your computer's basic functions, such as executing applications and controlling peripherals. Microsoft Windows is an example of an Operating System.
- Guest VM, or just VM: This stands for Virtual Machine or Virtual Computer. These don't physically exist, but share resources from your physical computer.
- Hypervisor: software in which we can create and manage Virtual Machines. The hypervisor connects virtual hardware added to Virtual Machines with hardware on your physical computer. Examples of hardware are memory RAM, Processor, Network Adapter, Hard Drive, Network Adapter, Sound Adapter, USB adapter, etc.
- Server: Dedicated computer, more powerful than a regular user desktop computer, that runs applications that are offered to the users.

In the previous chapter, I explained that you can browse the internet in a separate environment. Now that you know what Virtualization is and what you can do with this technology, I am sure you are already picturing the idea and what you can do with it.

If you are still wondering why you would separate your internet browsing into a different environment, the main reason is to protect your valuable data and your computer. If you don't get threats installed on your main system, your Operating System will keep performing well without the risk of crashing, which would result in having you spend money and time to have it repaired. And, the most important part, it will keep your data safe.

So what does it really mean to use the internet in a separate environment? It literally means doing it on another computer. The good news is that the other computer is going to run virtualized under your main computer, and you can easily switch between them.

How would this concept have worked in the past, without virtualization? It was as simple as purchasing two computers and having both of them, one next to each other, at your desktop, with two mice, two keyboards, and at least two monitors, one for each computer.

It may seem weird and excessive to have two physical computers, but so many people, including myself, have done it in the past for so many different reasons. I have always kept my primary computer safe with my data and information on it; then I have used a secondary computer on which I used internet and email, and also used it for testing multiple things.

The point is that I have always kept a safe environment and used a computer in which I can have the luxury of crashing it without impacting my primary system and, most importantly, this protects my valuable data that I really want to protect and preserve.

As you can imagine, I keep using a secondary computer, but it has been several years now that I have been using a secondary computer as a Virtual System. I don't have two computers anymore, and I just have a single set of mouse and keyboard. What I do have is two monitors, so usually I have my Virtual System on one monitor and my regular system on the other monitor and I switch between them as if I were on just one system.

Computers are so powerful these days, and any computer you purchase now or had purchased several years ago is capable of hosting one or more virtual systems on it. New computers these days come with a very decent amount of memory and hard drive space, while processors are powerful enough to not just process activities in one system, but can handle multiple systems using the same processor at the same time.

When you set up a Virtual Computer, the same way that a regular computer has memory, a processor, network adapter, hard drive, DVD-Rom, etc., the Virtual Computer will need the same resources, but they will be virtual.

The concept is simple: if your computer has 8 GB of RAM (memory), you can setup a Virtual Machine (VM) with 2GB of RAM, leaving your computer with 6GB. Virtual Machines don't need the same performance power as physical computers, so a Virtual Machine with 1GB or 2GB of RAM is enough for most cases of your home virtualization.

If you are a designer who works with tools like Photoshop, AutoCAD, or any other video or image editing tool, I would recommend you to keep using these tools in your physical computer. That doesn't mean such tools cannot run virtually—they do, but you would need to add more resources to your Virtual Machine (VM). It is better to virtualize your internet browsing and online activities, which use a relatively small amount of your computer resources, and keep using your work/hobby tools running on your main computer for best performance. In the end, that kind of work and data is one of the things you want to protect from the internet threats.

Also, by virtualizing your internet activities, you will separate important assets stored in your

computer like your data, work tools, etc. from being exposed to the internet and this will keep them safe. I know, I know… I already told you about it, but I cannot stress enough how important it is.

If you need to work with two or more computers at home, you can have just one physical computer and virtualize the others you need. This would save you money and space, and also will save on electricity.

Realistically, the main advantage you can take of virtualization is to protect your computer, your valuable data, and your information to become corrupted and lost because of a threat that destroyed your computer's Operating System.

Next, I am going to expose the most common situations you may face when your computer is infected with threats and what would happen in a scenario in which you are not using Virtualization, and a scenario in which you are using Virtualization.

1- You get a threat that deletes all your hard disk information and reboots your computer.
In this case, when the computer tries to startup, not only the system has been removed, leaving your computer hardware empty, but you have also lost all your valuable data and information. This is the most severe case.

Remediation:

a) Take your computer to get repaired or have a technician come over to your house to evaluate damage and give you a repair plan and price.
b) Before the repair process starts, the technician may try to recover deleted data. This is delicate, and depending what process was used by the threat that deleted files, a partial recovery can be possible. This process may be included in the price to get your computer repaired, but if you really want to recover the data, the hard drive would need to be sent to the lab and that is expensive. That process is realized by a specific data recovery company, basically used by corporates at a high price due to the advanced technology used.
c) Getting your computer back will not take more than three hours. You need to have an OS installed, configured, and then it's ready to go. You may be charged the time dedicated to try to recover data with any software/tool the technician might try. The average price can be $110 per hour. Let's assume the technician spends two hours trying to get your data back, this can perfectly cost you $550 + taxes.
d) You will get home with your computer fully operative again. Now you will need to reinstall the applications you used, assuming you have them available, like games, configurations, etc. You will need to do everything from scratch, like the first time.
e) Depending on the success of the technician recovering your data, if you are lucky you may have some files back. It is hard to predict the percentage that will be recovered, but the result will leave you with a low rate of data recovered and a lot of

totally corrupted, unusable files .

2- You get a threat that corrupts your system, by removing critical system files and destroying boot processes.

Similar to the first case, your system was lost and needs to be reinstalled. When the technician starts working on your computer though, they will notice that current data exists and will be able to do a clean system installation, but you will get all your data and information back, as it was never deleted.

The remediation steps would be similar to the first case, but without the need to attempt the data recovery. The price may vary between $200 to $400 in order to have your computer back, but once again, you will need to reinstall your applications from scratch.

3- You get the common adware threats. These are classical window messages which pop-up from time-to-time with any kind of advertising or alerting message notification about fake infections. You may be experiencing this already, and even though it doesn't seem like a big deal, they are annoying, affect your computer performance, and if accidentally you click on them, you may get infected with a more serious threat.

Remediation steps for these types of infections may vary. If you are lucky and have a good up-to-date antivirus, it can eliminate these kind of threats and clean up your system. There are other known tools that may help clean your system from this annoying malware.

No matter what threat you get, it is an inconvenience for you. Threats that corrupt your computer may cost you money and time, along with the possible loss of valuable data.

Now imagine that you isolated your internet activities into a virtual system and got the same threat as in case 1 or 2 above. Recovering your Virtual Computer will take you literally two minutes to bring your system to a prior state, before the infection happened. Even if you had important data that had been lost on the Virtual Computer, you will have it back. Not only will you will have your virtual system back in no time, but your computer didn't get affected by any threat, as it was isolated from online activities.

This may sound hard to believe, but this is what Virtualization does—not just make Information Technology more efficient, but also more simple to manage. Managing a Virtual Computer is not the same as managing a physical one. The Virtual Computer can be easily be protected and recovered, and helps you, the user, to work in a very efficient computer environment.

Before finishing this chapter, I would like to delve a little bit deeper into two malware threats that I commented on in the last chapter: Keyloggers and Ransomware.

These two threats really scare me and they should scare you too. They can really impact your finances, by either getting your money stolen or having to pay money in order to have important and valuable data back.

Ransomware

Ransomware is very new and its infection has grown greatly during 2016. The fact that it involves a way to get money for the attackers is making this threat very popular, and what it is alerting is the fact that the cause of this growth is because people actually pay in order to get their systems back.

On April 2016, the FBI reported that more than $24 million has been paid from victims infected with Ransomware that wanted their data back, just in the United States. The amount is bigger globally and this number is growing more.

You can defeat Ransomware attackers easily by separating your online activities into a virtual system in which you don't store any valuable data. If you get infected and the attacker asks you for money, just restore the Virtual Computer to its last state and you are done.

Keyloggers

On the other side, we have Keyloggers. Can you imagine getting up in the morning on a regular day, and while you are drinking your coffee peacefully you check if your paycheck has been deposited, only to find that your bank account is missing a good amount of money?

Keyloggers will record any single key you type on the keyboard. If your computer is infected with this threat and you access your online banking, your username and password combination will be logged and sent to the attacker, who later on would be able to access your account and set up a payment transfer to themselves.

There are different strategies you can use with Virtualization to protect your bank account's online access. If you use a Virtual Computer to do your online activities, don't use access your bank on that Virtual Computer. Deploy another Virtual Computer dedicated to use for sensitive access, or since you have been using the internet on a Virtual Computer (keeping your local computer clean and safe), use the internet on your local computer to access your bank account online. The bank website will not represent a risk to your computer.

Since you have been using your Virtual Computer to do all your internet activities, the virtual machine has a higher risk of being infected than your local computer, and a system that can be infected should never be used to do sensitive activities, like managing your finances on your bank website.

Also, setting up two-factor authentication for your bank access is another way to defeat Keyloggers, as it will not be enough to just provide username and password. If you want to

know about this service, just contact your bank. Most of them offer this added level of security at no extra cost.

Common sense is very important when using the internet. Remember that Virtualization is a technology that allows you to use your computer in a very smart way.

Your Virtual Privacy - Safe Haven

As I covered in the beginning of this book, safety is very important, and privacy is also. Computers are a tool for work, but also for entertainment. There are countless ways that people can use computers for enjoyment, and you may want to have privacy for some of them. If you want to keep some internet activities private just to you, using a Virtual Computer will solve that problem.

Imagine a system in which you can do absolutely anything you want without being concerned of things like: a) who is going to discover the websites you look at, b) what applications you use, or c) who you talk too. Imagine a system that you just turn on when you want to use it, and that just you have access to.

Do you share your computer with other members of your household? If more than one person is accessing the same computer, it could be possible that your activities are tracked from other profiles. Also, if you install applications, they would be visible for the other users too.

Are you browsing sensitive data, adult content, chatting with other people, working on a secret project, or just browsing content that you want to ensure is private and that no one can find out about?

Think of your Virtual Machine as your private virtual environment that is just for you. Even though you may share your computer with friends and/or family, the Virtual Machine that runs on it will be just yours, and no one will have access. It’s just like having another computer that you don’t share with anybody.

People have been creating different profiles on computers for a long time. This has been the preferred method for users to share their computers while trying to have some privacy. This method is still being used by users, probably because they don’t know that there is something better that they can take advantage of.

It is true that profiles can give you certain privacy, but you can access other profiles’ data from your profile, discover what other users are looking at on the internet if you really want to know, and, most importantly, if a profile gets infected with viruses and threats, it will affect all the overall Operating System on your computer, not just a specific profile.

Also, someone accessing your computer, even using their own profile, can install a Keylogger to track down what you or others do on the computer. Keyloggers often come in

the form of a threat, but they are also tools used by people you may know to spy on you.

It is perfectly okay to still use profiles, so each user can personalize it and have shortcuts to their favorite applications and games. Just make sure to tell anyone using your PC to not do any internet browsing or online activity on the physical computer under that profile.

All users on your computer can create their own Virtual Machine, so every time they use the computer, they can do their internet activities on the virtual system. You will not see others' profiles Virtual Computers on your profile. Virtual Computers are unique to each profile, and no one will see if you have Virtual Machines set up or how many.

Using your Virtual Computer

What would you usually do after purchasing a brand new computer? Setting up a virtual machine is like acquiring a totally new computer. You will have a brand new Operating System installed, ready to be used for your online activities.

You will learn how to deploy a Virtual Computer with the free guide that comes with this book. The guide is a step-by-step "how to" technical document that will show you all the necessary steps to have your Virtual Computer up and running and the necessary setup so can use internet on there.

The Operating System used is a Linux based OS, called Ubuntu. Ubuntu is free to use, and it is a great Operating System to run on your Virtual Computer. It is a very good system and performs great with low resources.

If you are a Microsoft Windows user, you will find that Ubuntu is a little bit different, but you will get used to it very quickly. You will see that it has a menu like you have in a Windows system, and Ubuntu comes with Mozilla Firefox browser, which you may be already familiar with.

If you are a Mac OS X user, you will find more similarities with Ubuntu, and you will probably get adapted to it quicker than a Windows user. But at the end, it is an Operating System that you will use to browse the internet, watch videos, etc., and you should not have any issues using it.

If you are wondering why Ubuntu has been used instead of a Windows system, basically it is because Ubuntu is free for personal use and it is a great system to virtualize. This solution has been thought of for users to be able to develop a virtual environment where they can browse internet privately and safely, using their existing computer without any extra cost.

Of course, you can virtualize Windows 7, 8, or 10, but you would need to pay for a Windows

license in order to install a new copy of Windows on your virtual computer. If you are interested in pursuing that option, I can help you to achieve that.

I really recommend you using at least two monitors. There is no problem in using just one monitor, but when you have two monitors, you can place the Virtual Computer on one of them, and use the other monitor for the local applications or other local activities you do on your regular computer. This is up to you and obviously you can use just one monitor as always, especially if you are using a laptop.

Conclusion

The internet is a fantastic platform that we can use for work, study, and entertainment, but it is also a very dangerous place in which we may have very bad experiences if we don't take the necessary steps to protect our computers and data.

There are endless threats on the internet. Threats are not just in the form of some virus that will break your computer, but also tools designed to run silent in your system that you are unaware of. They steal your data, monitor everything you do on your computer, basically break into your privacy, and steal your and/or your loved ones' information.

Getting our computers infected can have a very negative impact on our lives. If your computer's Operating System gets crashed, the consequences can be dreadful, risking the loss of valuable data and having to spend an elevated amount of money in repairs.

By using Virtualization, you will achieve a level of safety and privacy, and not just that, your computer will keep performing well without acting weird, rebooting itself, errors, or annoying behaviors that take our productivity or enjoyment away.

I really hope you have found this eBook interesting and a useful tool to learn about how to achieve safe privacy in your computer. Now, ahead of you, you have the challenge to setup your first virtual computer with the help of the "how to" technical document provided to you.

Backups and Disaster Recovery

If you are interested in learning backup techniques, not just for your Virtual Machine as a whole system, but also protecting data inside of the Virtual Machine, a new eBook will be available soon. The eBook will also show you how to protect your physical computer—in case something happens, you can recover it yourself in no time, without needing to pay hundreds of dollars to a computer technician. Also, you will learn how to move your Virtual Machine from one computer to another, in case your computer crashes and you need the VM

while you recover the other computer.

Most people, and even companies, don’t realize how important backups are. Not just to save you big amounts of money on repair processes if a disaster happens, but to protect your most important and valuable data, like family and personal photos, documents, work documents, etc. It is important you stay ahead of any problem your systems may have and be proactive by having an efficient and very inexpensive backup plan for your systems in place.

If you have any questions, need advice for a specific setup, or have any concerns, please email to support@mysafeprivacy.com

To download your free How-To Master Guide to deploy your Virtual Environment, visit my website at this link http://www.mysafeprivacy.com/download.html

The Download page is protected. Please, type the following Password in order to download the file: **Virtu4lPriv4cy!**