Building A "Secure" PC

This document outlines how to build a relatively secure PC environment. It assumes you are fairly proficient technically with PCs, especially with Windows based PCs. In fact, if you are proficient enough to do a "clean" install of Windows 10 onto a clean disk then I am confident that you'll be able to easily account for whatever gaps/omissions there are here. Also, the assumption here is that we'll be creating this "secure" environment on a PC with the capability of having multiple SATA drives connected concurrently. That is, a good name brand **DeskTop PC** that supports multiple SATA drives (the more the better). For laptops it's also possible but it's beyond the scope of this doc. More on that near the end of this doc. That said, let's continue.

One of the most secure home PC environments is one where we have a separate PC for the things we do such as:

- Email
- Online banking and bill-pay
- Software development (e.g. programming using MS Visual Studio)
- Blogging (e.g. using WordPress hosted by GoDaddy or other services)
- General web surfing (e.g. google searches or browsing RussianBrides.com)

Of course nobody wants to actually buy and care for and feed 5 individual PCs. But there is another way. **And that is to use just 1 PC but use a separate hard disk in that PC for each purpose**. Then we can "plug in" the disk we need, boot the computer, and perform ONLY the task we want to, such as banking, and when we are finished, we shut down the computer, disconnect the "Banking Disk," and move on to our next task (such as Email); and so on. Of course this is rather unwieldy. But there is a much easier way that accomplishes the same thing. We can...

> We can use just 1 computer that has the capability of having multiple Hard Disks (or SSDs) installed concurrently. For example, my computer has the ability to install up to 4 SATA disks. And just as important:
>
> > When booting, we can press F10 to get into the bios and at that point we can enable just the disk we need and at the same time disable all of the other disks.

Using the banking example, we can power-on and repeatedly press F10 until we are presented with the bios interface/screen. Then we can enable the "Banking disk," while disabling all other disks. Then we just continue the boot process. The PC will boot to the banking disk but no other disks can be accessed. Now we can do our banking (and ONLY our banking!). When we are finished we can re-start the PC without the need to completely power-off. During the next boot cycle we again go thru the same process only this time we might enable the "General web surfing" disk while disabling all other disks (including the disabling of the banking disk). In this way we can skype with our Russian bride-to-be without fear of contaminating the other disks/environments. That is, without fear of contaminating our banking environment.

I know. It sounds complicated and it sounds like a lot of work. And it's scary playing around with the bios. But it really isn't. We quickly get the hang of it. We memorize the keystrokes and they become

second nature. And very soon we get to the point where we can "switch environments" (switch drives) in less than 60 seconds while thinking of something else. **It's a very small price to pay** for a relatively secure online banking environment; and it's vastly more secure than commingling banking with all the other insecure crap we are wont to do with our PC. But yes, it's true, there is some initial work to do in setting up and maintaining the various environments (like the separate "banking" or "email" environments). That is, in building the different disks.

However, we only need to create/configure **just 1** "clean" hard disk that we can then EASILY replicate onto other disks that we'll use for our other environments. In other words, we'll build **just 1** "clean" PC environment with everything we'll need and then we'll EASILY replicate the result (the disk image) onto other disks.

We'll build this vastly more secure environment in just 7 easy steps.

Step 1 - Building The 1st Disk – Building The "Clean" PC

Perform a "***clean install***" of Windows onto a clean disk. Test it out but do NOT use the internet other than to make sure you can access it. For example, just go to google.com **once** and that's all. No going to RussianBrides or to GiveMeYourPasswords.com.

Or, just buy a new (and appropriate) desktop PC with Windows 10 and give it a quick test (avoid using the internet!).

It cannot be overstated how important it is to have a CLEAN installation to start with. It's folly to try and build a secure environment on an insecure pile of sand!

Step 2 – Make And Verify your first disk image.

The next step is to make a backup image of the "***clean***" disk we created in Step 1 (or of the disk in the newly purchased PC).

You'll need some good disk imaging software. I use **Acronis True Image**. With Acronis I always create and/or restore disk images by using its USB bootable media which Acronis can create for you on a thumb drive. See their documentation.

After creating the disk image (the backup) make sure to VERIFY it to ensure its integrity; so that you can always restore/reload the disk in the future. See "*verify*" in the Acronis documentation. My own preference is to actually restore the disk from the backup image right after verifying the backup image. Then I do a quick test of the PC (avoid the internet!). In this way I am even more confident all is well. Finally, I make a copy of the backup image on a thumb drive and have it Federal Expressed to a storage facility in a salt mine in Utah that is guarded by 1,000 heavily armed young Mormons.

Step 3 - Install Apps/Software

Install all the software you'll be using. Like MS Office, Visual Studio, skype, the Chrome browser, etc. Again, avoid the internet when possible! You don't want to inadvertently contaminate the environment.

Give everything a quick test. When everything checks out then...

Step 4 - Shrink the C: drive (partition) and create a partition for data.

This is a very important step. In the future, as things change, or if you happen to get malware on your PC, you'll need to restore your disk from your last clean backup image. If you have a lot stuff on your C: drive (e.g. a lot of Word docs in your documents folder) then everything gets very complicated very fast!

What I do is **always** keep the C: drive "clean." All data I create is created in folders on a "data partition." Then, if something "bad" happens I can quickly and easily restore the operating environment from the last image of my C: partition without clobbering or having to account for data in the documents folder, or the pictures folder, or the desktop folder, etc. all of which exist on the C: drive/partition.

That said, **use Disk Manager to shrink the C: partition** while leaving some empty space for temporary (non-critical) stuff. I shrink the C: partition down to the minimum + about 20gb.

Then use Disk Manager to create 1 or more new partitions that can be used **for data.**

When all that is done, then from now on you will only have to image (backup) the

- C: drive
- the Windows Recovery Partition
- the EFI System Partition
- the MBR (the disk's Master Boot Record)

The above might sound complicated but, trust me, it's not.

Step 5 - Make and verify your 2nd disk image.

Now we can make our 2nd clean backup ("disk image"). If we are using Acronis for the

backup/imaging we will tell it to backup/image ONLY the following:

- C: drive
- the Windows Recovery Partition
- the EFI System Partition
- the MBR (the disk's Master Boot Record)

In this way **we are backing up the operating environment ONLY.** We are NOT backing up user data partitions. If malware strikes us and we have to restore the operating environment then we restore the above 4 items from the backup/image file to their appropriate places on the disk. This will restore the operating environment quickly and easily; including all of the apps/software we had installed.

Note that the backup will NOT contain any user data such as Word documents. You will need to decide how to periodically backup your data. Of course, even if one didn't want to go this "secure" route we'd have to figure out our data backup procedures anyway (except that now some/all of our data is on the C: partition mixed in with the operating environment). If you ponder it for a while you will come to appreciate the advantages of having your user data (like Word docs) on a different partition(s) than your C: partition.

Step 6 – Replicate The Clean Operating Environment Onto Additional Disks.

Steps 6-7 are EASY.

Now we physically install the additional hard disks into the PC and initialize them. I suggest using SSDs for the additional disks.

Then, using the Acronis disk imaging/backup software, we will restore our last backup onto one of these other disks. Then we should be able to reboot the PC and using our PC's appropriate method, enter the bios where we can **enable the new disk and disable the original disk**. Then save this configuration and reboot.

> On this next boot, depending on the PC's bios idiosyncrasies, we might have to interrupt the boot process again to specify what disk to boot from (we'll simply select it from a list and press Enter). This can be a minor annoyance but it only takes a few seconds and we get used to it.

I suggest restoring to these disks one at a time and after each restore performing a quick test. Then restore the last image to the next disk, test, and so on.

At this point we should have multiple disks in our PC and, by using the bios during the boot process, we can select a disk to enable AND to disable the other disks. Then we save the configuration and continue the boot process. The PC will boot to the disk we enabled and the "disabled" disks will not be visible and cannot be accessed.

Step 7 – Discipline Discipline Discipline

So let's say that at this point, as on my PC, we have 4 disks in our PC and they are all identically configured. **The next and final step in the "secure" PC is simply to have discipline.** For example, on my PC I use the disks like so:

- Disk 1 - General web surfing
- Disk 2 – Email, and Blogging/Wordpress
- Disk 3 - Online banking and bill-pay
- Disk 4 - Software development (e.g. programming using MS Visual Studio)

When doing email, I ONLY read/send emails. I NEVER click on a link in an email. If I want to follow a link in an email, I copy the link to a text file on a thumb drive and wait until I boot to Disk 1 (General web surfing). And when I exit Yahoo mail or Google Mail I do NOT do ANYTHING else. I either shut down or restart the PC (on restart I'll boot to a different disk/environment).

When blogging I ONLY do what's necessary via WordPress to write the blog. Then I either shut down or restart the PC.

When Banking I ONLY go to the bank's web site(s). I ONLY go to the bank's web site(s). I ONLY go to the bank's web site(s). I ONLY go to the bank's web site(s). I ONLY go to the bank's web site(s). I ONLY go to the bank's web site(s). Then shutdown or restart to another disk.

In all of the above DISCIPLINE IS THE KEY. Only do what the disk was intended for!

When in the General Surfing environment just about anything goes (within reason). If something bad happens it should only happen to the General Surfing disk/environment. And if bad things happen, or if I even have a slight suspicion that something bad might have happened then I can EASILY and QUICKLY reload that disk and it will be a clean environment again. And the reloading is quick and easy using Acronis True Image.

And keep in mind that none of this will work easily unless we keep our data in a partition(s) different from our C: partition.

OTHER INFO

But I don't want to buy additional disks.

> Disks, even SSDs are **not** expensive any more. In general even the small disks (e.g. 120 gb SSD) are sufficient for what you want to do. E.g., when doing banking you are only using the browser and maybe your printer. And maybe you'll create some spreadsheets.

A 120gb SSD is cheap and way bigger than you'll need. Doing email? Again, minimal disk size is all you need. Same for blogging and for programming via Visual Studio.

I have found that the only disk I need of any significant size is the one I use for general surfing (so I can have a lot of music and podcasts and photos and videos etc. **in the data partition(s)** on the "surfing disk."

Windows Updates

Updates to Windows will be applied to each of your disks (automatically) over time. What I do is:

- Periodically (e.g. every X months) reload one of my disks from the last image/backup.
- Then I apply all existing Windows updates and make whatever changes I might want to make since the prior clean backup/image. E.g. I will install and test any additional software I might want to use. Then I test it quickly (avoiding the internet).
- Then I create my next backup/image. The will become my current backup/image that I will use going forward.
- Finally, I restore the backup/image I just created to all of the other disks. Now all disks have the same operating environment.

It's very important to realize that all of the above is quick, easy, and straightforward but only if your data on each disk is in partitions separate/different from the C: partition! The importance of this cannot be overstated.

So why do I go thru this process every x months? It's so it doesn't take forever if/when I need to do a restore. 12 or 18 or more months of Windows updates can get complicated and also it can take a long time!

BTW, I retain quite a number of prior backups "*just in case!*" It's probably an obsessive/compulsive thing. But its cheap and easy to do so why not? It's certainly cheaper than my therapist(s).

Why not just use a VM environment?

I have done some research on this and I am not convinced that it's as secure and certainly not as easy imho as the method outlined here **if you use a desktop machine with multiple SATA ports and associated power connectors** (mine has 4 and I looked at some DELL machines with 3). Additionally, for whatever desktop machine one contemplates, one needs to verify how the bios works (can individual drives/ports be enabled/disabled – individually?). I have a HP ProDesK 400 and the whole process is very simple and straightforward.

However, for laptops, using Virtual Machines (VMs) is very likely the best bet.

Or, **<u>if one is adventurous</u>**, they could open up the case (or drive cover) and run a short SATA extender thru the case or drive cover. Then one could physically plug/unplug individual SSDs into the now external "extender" as needed using separate SSDs for Banking, email, surfing, etc. The main problem here is that you have to **<u>carefully</u>** cut a small slot in the case/cover in order to get the short SATA extender external to the laptop... but it's doable... but probably not what most people want to do unless they have a spare laptop they are willing to use for such a purpose. But it can be done (you'll probably have to buy or borrow a Dremel).

Yes, doing all of this is initially time consuming because there's a learning curve. You have to learn how to use the disk imaging/backup software (I recommend Acronis True Image). You have to learn the ins and outs of working with the bios. You have to separate your data from your C: partition. But hey... what else do you have to do? And in the end you'll have learned a few things along the way. AND you'll end up with a pretty secure PC environment.

The End