



# Home (SOHO) Computing Safety

By CK Wong 2005.09.18

[http://www.ck-wong.ca/Technologies/home%20\(soho\)%20computing%20safety%2020050918.pdf](http://www.ck-wong.ca/Technologies/home%20(soho)%20computing%20safety%2020050918.pdf)

## Introduction

Ten years ago, we may use a lot of PC for many good reasons but they usually maintained by technicians. Nowadays, the perforation of PC is so deep that most of us have the challenge to do some daily maintenance and setup by ourselves. This article will point out a few solutions for some non-technical people who are comfortable to do it yourself. Otherwise, like maintaining your house, you may want to find out what needed to be done and talk wisely to the tradesman (the computer nerds).

## No PC is an Island

Why island is related to PC? It is all because we are all connected to a greater collective mind, like the Borg, whether you like it or not. They are the Internet and power grid. Anything bad happens to these two networks will directly affecting you beloved PC.

When you invested in PC, you are not just fond of this heat generator but also the stuffs you stored on it. You want the contents to be proper protected with a reasonable cost from unwarranted accidents and corruption. The first line of defense is to avoid any electrical damage caused by the power. Once you have security on the power side, we have to ensure those viruses and worms do not corrupt you beautiful memories stored on you PC.

## No Security System is 100% Fool Proof

We should always remember that no security measures are 100% fool proof. All walls will come down given enough time and proper tools. What we are talking here is just some common sense and low budget do-it-yourself work like safe proof your house or change engine oil for your car.

## More Power Does not mean Better

With the energy crisis, we experience more power outage than 10 years ago. It would also be a good educated guess that the power is not as clean as before because the fluctuation of on and off of appliances and generators. You would have surge or drop of powers when appliance is switched on and off, like your favorite Air Cond or the washing machine you don't like that much. Computers, monitors and likewise your big screen HDTV's are very sophisticated equipments that demand a very steady electrical

voltage. Most of the equipments have built-in power regulator but sometime the power surge could be beyond their scope.

The protection covers in two areas: damage protection and continuation of usage. A \$5 surge protection power bar may do the job but the surge could come from the phone line, the TV cable as well as the power line. A good surge power bar usually comes with all these three protections and an insurance coverage. Consider it as the additional insurance for your equipment, a \$30 - \$50 power bar is a good deal, especially your house insurance may not have a power surge coverage or there may be a \$500 deductible.

To allow you to continue your work means you need the juice. A backup generator is definitely a good idea but you may lose all your precious data while the generator kicks in. An alternative is connect you equipment to an Uninterrupted Power Supply (UPS) which is a battery plus the electronics that do the power surge protection, power regulation and provide you continue supply of electricity when a brown-out or a black-out happens. You have to decide on which equipment you need during the power outage. Find out the total wattage requirements and buy as many UPS as needed. For most people, one for the computer and monitor could be sufficient. Others may need a separate one for your DSL/Cable modem, router, PC, monitor so that they could finish their work for that extra half or one hour. For those who do not familiar with UPS, the UPS could shutdown you PC during power failure. Usually, it takes just a minute or so. Therefore, the rating of the UPS could be a low one (so does the price too).

Other than the computer, you also need to take care of your super-duper multi-functions phone with call display. It is a regulatory requirement to have the phone line in working condition under all situations. However, your phone may not work without power. At least not the caller ID. Likewise you may need power for your cell phone charger and MP3 charger.

## **Computer Security**

There is a joke that a computer will pass the most stringent military security check if you do not connect the machine to the power and network. Let's take a look and see why.

First, there will be no data lost or could be stolen. Second, no one could break into the system even they have the account password; what a feature. Third, you can completely trust this computer because no worm or virus could infect it. Four, it will not be a target of any attack because it is not visible.

Of course, it is also dysfunctional. But this is the basic principles of computer security.

## **The Invisible Man**

If you have your computer sitting behind a router, the router can be set up in a way that the network will see the router but not necessary your computer. This set up may not be very useful because you will go out. Once you go out, you could be tracked.

After you installed the wireless router for your home LAN, you becomes the secretary of your own home LAN security. The first order of business is to change the default SSID name (i.e. the name you assigned to the router) so that no one could connect to you accidentally.

On a home wireless LAN, if the router does not broadcast your SSID, no one could connect to the router. However, you know its name so you could set up your wireless card to connect to the wireless router.

## **Restricted Access from Outside**

The simplest thing is to ensure each account has a password which is not the name of the account. Any crack could be ajar will be the source of break in. It is just like your home.

Please do not forget to change the password on the router's administrator account. Otherwise, you are opening your Chubb safe's one foot thick steel door to everyone.

Another way to prevent someone comes to your network is to use the MAC Filtering features on your computer. To use it you have to enable your router's Firewall feature first. MAC Filtering is to grant the computer access to the router. It uses the network card's physical ID (called the MAC address which is set by the manufacturer) as the fingerprint to identify itself. This will be particular useful to block another computer's wireless access. It is less effective for the wired connection because they could extract your network card and put on their computer. In such a case, it is a break in. For a small office environment, this is a must to prevent someone to tap to your network.

## **Restrict Access from the Insider**

We hear the danger of a worm. It spreads the disease by send itself to next victim. There are two common methods: through email and through execution of a program.

To stop the execution of the worm in a mail system is simple: disable the execution of script in incoming email. It is a small price to pay but it is worth. The second is to use a firewall on your computer to prevent unauthorized program going out or accepting incoming traffic. There is a number of products in the market such as Symantec's Norton, Network Associate's McAfee have an integrated solution that offers SPAM control, anti-virus and PC firewall.

The concept of stopping the virus or worm to spread or attack is a proactive defense which should be shared by everyone. Without this strategy, many PC users become the involuntary cyber terrorist.

### **Prevention Lost of Data**

One major benefit of using a PC is to create a single file cabinet (the hard drive) to store our information. With all the wonderful tools you can have from Internet, you could catalogue and arrange them until you drop. Lost of data can be divided in 3 types of hole: black hole, worm hole and rotten hole.

**Black hole** means the file is lost in the sea of information. There are different desktop search engines, e.g. Google Desktop, you could use to find your file based on name or contents. A better way could be using a proper file directory tree as your virtual file cabinet. You classify the files by their nature. In case a file belongs to multiple categories, you can use short cut to refer to a single copy. This leads to another common problem. People think their data is too secretive. They encrypt it. As time go by, they forget or lost the encryption key. Don't encrypt data unless it is really needed.

**Worm hole** happens when the file is accidentally corrupted like a hole created by the book worm. The rule of thumb is that you should not let everyone have the capability to modify it, including yourself. Once the file is archive, ensure it is read only. On many file system, the access control can have the granularity of general read permission or specific read permission. So set the file to the permission accordingly.

**Rotten hole** is the common problem that when we have too many files, the files could be rotten out because we store it in a format that can no longer be read. Once upon a time, floppy disk is everywhere, I mean the 5¼ inch one not the 3½ inch one. You store your precious program, data and memory there. As time gone by, the data deteriorates. Unlike your VHS tape, some noise is still acceptable. Once the bit is rotten and you will see the I/O error message that telling you the file could not be read. So store the data in a proper medium and converting them appropriately.

### **Beam me up**

To prevent data lost, I would strongly suggest people to go out and buy a DVD writer to do regular backup, a reliable one like LG, Aopen, HP, Liteon, etc. DVD becomes such a commodity that prices different is not that significant. An internal or external drive works well. Because of the price I prefer to have one on every computer including laptop. It is also important to know that in the future software distribution industry will use DVD. CD will be abandon because everything is so huge, 700 MB does not cut it.

## Safe Sex Practice for PC

When it comes to AIDS and STD, we all know that it has to be cautious to when body fluid is exchanged. In case of PC, it is the exchange of data we have to be carefuls. USB is so popular that you could exchange data between computers. But be careful, follow the safe sex practice to prevent any disease. If you exchange file using USB key, ensure the key is read only if you transfer the data to your friend. Some key does not have the read only or write protected switch, then scan for virus after use, just like you do a blood test after unprotected sex. It is a really live and dead matter. Do take it seriously.

## Operational Security

Now is the time to talk about operational security. What I mean is the continuous of usage and identity fraud prevention: no spyware. Spyware does not only slow you down by monitoring a lot of function, leaks your identity, it also sends the information, when you access the web site. Sometime, these spywares are written so badly, it causes system crash. If not so, it could take up so much disk space that you don't have any more usable space. They could be detected and removed using the famous and free tools: Spybot and Ad-Aware. Both of them can be downloaded from [www.download.com](http://www.download.com). You should be warned that some spyware I call them leech spyware. It modifies the system. When you remove them it will destroy some part of operating system. Just like the old saying, prevention is better than cure.

## Conclusion

I hope I have provided you a picture of how to achieve home (and SOHO) computing safety. I don't expect everyone will able to implement this. I am writing a DIY Home Computing Safety Plan. It will be a low budget plan and hope I could finish it soon.