BUILD YOUR OWN SECURITY

By Alan Tay

Table of Contents

About the Author and Build Your Own Security 5

Step 1 – Ensure your system is ready to be secured..... 7

Stop using the Administrator account 7

Use a Standard account 8

The best time to use the Administrator account 8

Summary of Step 1 9

Step 2 - Get an Antivirus 10

Can you rely on a free Antivirus? 10

What are your choices? 11

Install and use them 12

Summary of Step 2 13

Step 3 - Install a Firewall 14

Why Antivirus alone is not sufficient? 14

What are your choices? 15

Summary of Step 3 16

Step 4 - Clean your Registry 17

Why clean your registry? 17

Is there any free version around? 18

Summary of Step 4 19

Step 5 - Use Data Encryption Software 20

Common practice to protect file 20

Let the encryption software to do it 20

Summary of Step 5 21

Step 6 - Prepare your web browser 22

Choose one web browser for sensitive transaction 22

Scan for vulnerabilities 23

Update and patch 23

Summary of Step 6 24

Step 7 - Have a Reliable Password Management 25

Common solutions for people who easily forget passwords 26

Are there any free Password Managers around? 27

Summary of Step 7 27

Step 8 – Ensuring your computer is safe 28

Perform a full system scan 28

Check critical software for new updates 28

Operating System updates 29

Summary of Step 8 29

Step 9 – Clean up and Back up your computer 30

Clean up and defrag 30

Backup your data 31

Summary of Step 9 32

Step 10 - Schedule your work 33

Schedule your activity 33

What are my recommendations? 35

Summary of Step 10 36

The 15 DON'Ts of Computer and Internet Security 37

Build Your Own Security Round Up 42

Round Up for a Great Secure System 42

Round Up for Free Secure System 42

Resource Directory 43

Antivirus 43

Firewall 43

Registry Cleaner 44

Data Encryption Software 44

Password Management 44

Data Backup 44

About the Author and Build Your Own Security

Hi, welcome to **Build Your Own Security**. My name is Alan Tay and I am the author of this book. I run a security blog called IT Security Column and I write about security news, tips and product reviews. Writing about all these things is just my part time hobby where my full time job is a Software Engineer who specializes in IT security.

The purpose for me to start blogging about security is simply because I had joined a security company and fell in love into this niche. Over the past 7 months of me blogging about IT security, I find myself learned a lot more about security as I read about security news each passing day and blog about them.

Build Your Own Security is the first ever book which I personally authored from head to toe. The reason I write about building your own security is to let you know all the necessary things which you need in your computer and the attitude that you need to possess in order for you to achieve great security.

In this book, you will find that I had layout 10 simple steps for you to build your own security. For each steps, I included the free and paid software which will assist you to the security that everyone needs. The last part of this book is about the DON'Ts that you must know to get yourself ready to combat cyber criminals.

I hope you will enjoy reading this book and have yourself built a Malware-free environment. If you have any idea to discuss, just drop me a mail at admin@itscolumn.com. You can also follow me on Twitter @AlanOnSecurity or join my Facebook page.

Disclaimer: Some of product links in this book are affiliate links. This means that I will make some small commission if you bought the products. That does not mean my words cannot be trusted as I either personally use those products or those products are highly recommended by some of the top software review sites.

Build Your Own Security by Alan Tay is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.

Step 1 – Ensure your system is ready to be secured

Image Credit: nuttakit – FreeDigitalPhotos.net

Operating System is the core of whatever you are going to do such as internet browsing, gaming, messenger chatting and any computer related stuff. Without the Operating System, you can't do all the things that I had just mentioned.

As a result, securing the Operating System is vital. I would say that Operating System is the foundation of your computer which is the very first thing to be secured before anything else. Here are some configurations that need to be done in order to get your Operating System ready to be secured.

Being the owner of the computer does not make you the Administrator all the time

Stop using the Administrator account

The most common mistake done by many computer users is to use the Administrator account on a regular basis. If the Administrator

account is somehow compromised, then the attacker will be able to gain control of your Operating System as the Administrator account has full privilege to do everything. Therefore, it is not advisable to use the Administrator account regularly.

Use a Standard account

Operating System today comes with at least two types of accounts. In Windows case, you will find three types which are Administrator, Standard and Guest account.

A Guest account by default is not allowed to install any application. The Guest user is only able to use the internet and access certain files. If there is no other user that is going to use the computer, it is advisable to just disallow the Guest account. There is no use for this.

An Administrator account is like a super account. You can do almost everything including installing application, creating new user, and also modifying system files. Therefore, you should not use this type of account on a regular basis as mentioned.

The best type of account to use is the Standard account type. One of the reason is you get to have the convenient to install any new application as long as it does not modify the system file or registry.

The other reason is that you get the limitation from destroying the system files as it is restricted by the Operating System unless it is permitted by the Administrator. However, the condition here is that the User Account Control (UAC) needs to be enabled.

The best time to use the Administrator account

The best time to use the Administrator account is to use it when you are going to do some system maintenance. System maintenance such as Windows update, updating existing application or even installing new application can be done using the

Administrator account. This is to reduce the hassle of the UAC pop up if you are using the Standard account.

Summary of Step 1

This is the summary of the first step in building a secure environment for your computer.

- Stop using the Administrator account
- Use the Standard account. Create one if you don't have any.
- Setup a strong password for both accounts.
- Enable the UAC if it is disabled.

Step 2 - Get an Antivirus

Image Credit: Salvatore Vuono – FreeDigitalPhotos.net

I know that there isn't anyone is using a computer without an Antivirus today, but I am not taking any chances by missing this step. If you are not installing any Antivirus now, don't rush to Google and start looking for one now. I will tell you directly what your choices are later.

Basically, Antivirus is there to help you to disinfect a virus, worm, Trojan or spyware infection. It also should give you a real-time protection as soon as your computer started until it is shutdown. So when you are looking for an Antivirus, be sure you evaluate these two points in detail.

Can you rely on a free Antivirus?

Today there are many free and paid Antivirus around. You might probably see so many paid Antivirus lying around the internet and begin to think whether the free one is reliable. My answer to this question is:

Yes. You can rely on the free version of Antivirus.

Free Antivirus is as reliable as paid Antivirus. The point where they started to make a different is when you start to look for more and better feature. You will realize that a free Antivirus comes with only basic features and does not have other tools to better secure your computer.

The other thing about free Antivirus is you got to live with advertisement. There are plenty of advertisements that have only the intention to lure you into purchasing a paid one. As a result, free Antivirus comes with only the basic stuff. If you are still not sure whether you should purchase one or use a free one, you can always refer to this write up on how to tell if you need a paid antivirus.

What are your choices?

Your choices are now down to only two types which are free and paid one. I will start off with the paid one first.

I highly recommend everyone to use a paid antivirus instead of a free one. Usually, paid antivirus comes with good support feature where you don't have to run into multiple forums to ask for help. You can directly contact the antivirus support line to get your problems resolved.

Apart from that, a paid antivirus usually bundled with a lot of features that can be very useful when you need them. If you ask me, I will not get just a basic Antivirus. I will recommend getting the internet security suite instead. My personal favorites are as below listing them from most favorites to least favorites.

- Kaspersky Internet Security (more info)
- Bitdefender Total Security (more info)
- ZoneAlarm Antivirus plus Firewall (more info)

As for the free version, my recommendations are the brands such Avast, AVG and Microsoft Security Essentials. I highly recommend Avast as I had been using it for quite some time and have no trouble with it. It is also one of the longest Antivirus in the security software market providing free antivirus since long time ago. However in the recent Antivirus False Alarm test, Avast seems to be not doing so well as it had detected lots of false alarm.

Microsoft Security Essentials (MSE) is also another good antivirus simply because I find it very light and does not take up lots of resources. However, the feature in MSE is the issue here where it does not have any other features apart from scanning for Malware.

The best thing about free antivirus is that they are free and able to fill the needs where every computer needs an antivirus. I will still recommend going for the paid one but will not insists that everyone should invest money into security. Below is the list of free antivirus from most favorites to least favorites.

- Avast Free Antivirus (more info)
- Microsoft Security Essentials (more info)
- AVG Free Antivirus (more info)

Install and use them

Today, most of us had an antivirus installed into your computer. However, did you use your antivirus as much as you can? Some of us just install the Antivirus and leave it there. You will only start using it when it prompts you with some infection issue that needs your attention.

It is quite a waste when had an Antivirus but did not maximize the usage, especially when we had already bought them instead of downloading them for free. It is good that we start browsing what our Antivirus is capable of and start using the features that might be useful. Apart from the special feature, below are the basic stuffs that you can do with any Antivirus.

- Perform a Full System scan once every week or fortnight.
- Perform a System/Quick scan daily.
- Perform a scan on the CD/DVD/USB media whenever you receive them from anyone even if it is your best friend.
- Perform a scan on the file that you had just downloaded.

Summary of Step 2

This is the summary of the second step in building a secure environment for your computer.

- Download a free Antivirus or purchase one.
- Install into your computer.
- Start using it.

Step 3 - Install a Firewall

Image Credit: jscreationzs – FreeDigitalPhotos.net

Firewall is a piece of software where many users did not take it seriously. Worse, some of them even disabled the firewall just to make their task such as file sharing easier. If you think that having an Antivirus is sufficient to your security, then you might not understand the difference between a firewall and Antivirus.

Why Antivirus alone is not sufficient?

The role of an Antivirus is to **disinfect** any infections in your computer. It acts like a policeman in any country. Whenever there is a crime, the policeman will be there to catch them. Same goes to your computer, whenever there is an infection, your Antivirus will be there to either quarantine or delete them as part of the disinfection process.

Firewall does not do the above. The role of a firewall is to **prevent** any malicious software from going into your computer. Take the Great Wall of China as an example; it prevents the enemy of China from going in to the country. It is far more effective when you compare the security to an Antivirus. However, it does not disinfect

your computer. As a result, you eventually need to have both firewall and Antivirus to help you prevent and disinfect any treat.

Traditionally, a firewall is installed in a computer to prevent any attack from going in. However, as technology kept improving, a firewall can not only protect the user from incoming data, but also outgoing data. This is what they call "Two-Way Firewall" and you read more at one of my blog post on the two-way firewall. The reason to protect yourself in the outgoing data is to ensure that the data that you sent out is towards a legitimate source and not some cyber crooks' server.

Do you know that a Firewall can block almost 99% of Windows-based Malware attack?

What are your choices?

You need to choose among the two-way firewall software. If you are still using Windows XP and older, try not to use the default Windows firewall as it is only a one-way firewall. Windows Vista Operating System and newer provides a two-way firewall, but it is not so user friendly when it comes to the configuration.

If you want a good firewall which is free, I will strongly recommend Comodo Firewall. Comodo has one of the most solid firewall around even when you compare with the paid ones. However, the drawback for this software is that it is not so user friendly in general because it has lots of pops up to handle.

As for myself, I had been using the firewall bundled in Kaspersky Internet Security which also provides a two-way firewall. You can do the same but if you are using a free Antivirus and require a good

and more user-friendly firewall, ZoneAlarm Firewall is the way to go. They had already been in the firewall industry long time ago and their firewall is one of the most reliable around.

Summary of Step 3

This is the summary of the third step in building a secure environment for your computer.

- Download a free Firewall or purchase one.
- Install into your computer.
- Start using it.
- Never disable the Firewall protection

Step 4 - Clean your Registry

Image Credit: jscreationzs – FreeDigitalPhotos.net

The Windows Registry is the place where your operating system configuration files are stored. It tells the operating system where to locate all the important and critical files that need to run your Operating System and other applications installed.

Why clean your registry?

Imagine one day, you have a Malware registered some information into your registry and your Operating System is not capable to recognize it as a form of Malware, your Operating System is going to locate and run the Malware every time you boot up your computer. Scary isn't it?

That is just the security part of not cleaning your registry. Imagine again that you had previously installed many applications and none of them uninstalled successfully. They still leave the registry part which is not cleared and every time your computer reboot, it is going to attempt to locate for the files that already uninstalled by you. This is call waste of resources.

Spending all the resources on the things that you don't need is going to slow your PC down. That is why Registry Cleaner has to exist. It cleans your registry to ensure that only necessary configuration files are stored. You can try to clean your registry manually, but I doubt that many of us can do it because it is not easy to understand the Windows Registry structure.

Is there any free version around?

There are always free and paid versions around the internet. If you are looking for a free version, you can probably try out Wise Registry Cleaner. I had tried other free Registry Cleaner as well but not so effective as after I cleaned my computer, the same error occurred when I immediately re-scan.

Windows Registry is a very sensitive section of your Operating System. The drawback of using a free version is that if you run into trouble, you need to run into multiple forums to look for your answer. If your computer is not your 'life', then you can still stick with the free version.

If you are looking for a paid Registry Cleaner which comes with a good support, you can try out PC Fix Registry Cleaner. Reason is you only need to pay for the software once because the license is lifetime. All you need to commit annually is the Technical Support fee which cost you not more than $10. There is also other paid Registry Cleaner around that worth the try such as Registry Mechanic and many more that comes with good support as well.

Summary of Step 4

This is the summary of the fourth step in building a secure environment for your computer.

- Download a free Registry Cleaner or purchase one.
- Install into your computer.
- Scan and Fix your registry

Note: You don't have to do it daily. Scanning once a month is good enough as I assume that you should not have major changes in your registry daily or even weekly.

Step 5 - Use Data Encryption Software

Image Credit: renjith Krishnan – FreeDigitalPhotos.net

Encryption is a process of transforming a readable data into unreadable data which is also known as gibberish data. This is to ensure that if somehow your laptop is stolen by some thief and manage to crack down your Windows account password, they still unable to grab your data due to the encryption.

Common practice to protect file

Usually, an ordinary computer user will not protect their file up to the level of encrypting them. What they normally do is to create a folder to keep all the important files and hide the folder. Smarter user might combine the step mentioned together with some zipping software such as Winrar and zip those files with password protected.

Good thing is your files are all protected but the bad things are the larger your file is, the longer the time you need to extract out and worst of all, there are tools to break the password protected zipped file. As a result, those files are not really protected.

Let the encryption software to do it

As technology improves, we have more and more software to help us out in our daily life. One of the best free disk encryption tool is

TrueCrypt. This software uses one of the strongest encryption algorithms, AES-256 where it is not easy to crack if the password that protects your key is strong as well.

However, as it is free, the drawback is always not user-friendly and no technical support. So if you happen to lock yourself, you can kiss your encryption drive goodbye. There is also a simple way to use TrueCrypt, but whether how strong is the security if you just simply implement it remains a question. As a result, TrueCrypt is suitable for people who look for simply a drive encryption but not maximum protection.

If you are looking for a maximum protection, one of the software which I highly recommend is the ZoneAlarm DataLock. This software basically encrypts the entire drive where if you do not provide the password, your computer will not boot at all. In addition to that, if you found yourself locked out, you can always contact the 24x7 hotline to get yourself back into your computer. However, the software is a little pricey where with the price where you can eventually get a whole Internet Security Suite. If you are really looking for maximum protection to protect your highly sensitive data at all cost, this is the software that you should check out.

Summary of Step 5

This is the summary of the fifth step in building a secure environment for your computer.

- Download a free Encryption Tool or purchase one.
- Install into your computer.
- Gather all your files and folders that need to be protected.
- Encrypt them and keep your key safe – Best is separate your key from your computer.

Step 6 - Prepare your web browser

Image Credit: Idea go – FreeDigitalPhotos.net

Web browser is a very important item simply because it is the item that brings internet to most you. However, if you are not careful, hackers can launch an exploit to compromise your computer via a web browser. When you are compromised, they will install some information stealing Trojan to steal your credentials especially the one where you used for internet banking.

If you ask around all the security experts, the best is to have a dedicated PC for your important activity such as internet banking. That computer can only be used for those activities and cannot be used on normal web browsing and if possible, not even USB or CD/DVD Rom interaction as well. This will build a super secure computer but also a computer that it is not so user friendly.

Choose one web browser for sensitive transaction

What I would suggest here is to have a balance in convenience and security. As a result, from the computer that you used regularly, pick a web browser that you want to use **ONLY** for important transactions such as internet banking. Next is to remove all the plugins or extensions. The more plugins you have, the more

vulnerable your computer is. As a result, removing them away will keep you safer.

Scan for vulnerabilities

The next thing that you need to do after removing all the unnecessary plugins is to run a scan on your web browser. This scan is to ensure that all your necessary plugins are completely updated and also you had completely removed the unnecessary ones. You should also run a scan on your other web browser to ensure that the plugins that you are using are up to date. The scanner that I had been using all this while to scan my web browser is the Qualys Browser Check and you can give it a try. It is free after all.

Update and patch

You should already have all your issues gathered by now after the scan. Your next move is to find the latest patch for all the outdated plugins. Once you had already found them, patch them. You should also check your web browser whether it needs an update or not. By performing all these steps, you are one step safer on the internet. I should remind you again that the web browser that you had chosen for important activity is not supposed to use for regular web browsing.

Lastly, you should always scan your web browser for vulnerability. There are plenty of threats especially on the Adobe Flash Player and Adobe Acrobat/Reader where those plugins are needed to be patched from time to time. Hackers like to make use of these two plugins' vulnerabilities to create an exploit.

Summary of Step 6

This is the summary of the sixth step in building a secure environment for your computer.

- Select an internet web browser for important activity.
- Remove all the unnecessary plugins and extensions.
- Scan the web browser for vulnerabilities.
- Update and patch the vulnerabilities
- Update and patch the web browser.

Step 7 - Have a Reliable Password Management

Image Credit: Salvatore Vuono – FreeDigitalPhotos.net

By now, your environment should be secure enough where it is going to be difficult for Malware to break into your computer. You have Antivirus, firewall and your Operating System and web browser are all fully patched. The only problem that you might have now is hackers might break your credentials by guessing your username and password.

Using a single authentication with static password has a flaw which is the username and password can be hacked by using the brute-force method. Brute-force method is a trial and error method used in guessing a person's password until it is successful.

This method might take from a very short time to a very long time depending on how you create your password. As a result, the best way to make this technique more difficult to success is to create a long and sophisticated password with lower case, upper case, numeric and special characters like symbols.

Common solutions for people who easily forget passwords

Usually when we ask someone to create a super strong password with long characters and combination of alphanumeric and symbols, they will create the password only once and use it for every account forgetting the rule of not having the same password for different accounts. The reason behind is pretty simple, such long password can still be remembered for once, but it might be impossible if you have 20 online accounts and each carries a different strong password.

As a result, people will only create once and reuse it on other websites as well. This is a bad practice because hackers today don't go directly and compromise the bank account's password; they will instead compromise the social network accounts such as Facebook, and Twitter and reuse those credentials on their online banking or other highly important online account.

The common solution is to write it on a physical paper or write in a notepad and save it. Both solutions are not practical at all as the passwords written can be seen easily. The best solution in managing your password is to have Password Management software. One of the Password Management software that I will recommend is the Kaspersky Password Manager.

This software will store your long and sophisticated passwords into the Password Manager and automatically load into your form when you need to present your password. Unlike the Antivirus, this product is a lifetime license where you only need to purchase once and use for life. If you are willing to pay, the Kaspersky Password Manager is the product that you are looking for to keep your passwords for every websites.

Are there any free Password Managers around?

Yes, there are two free Password Manager that I will recommend if you are planning to head down the free software road. One of them is KeePass Password Safe where it is an open source project and it works more or less like the Kaspersky Password Manager. However, based on several reviews, the drawback of this software is that it is not so user friendly and you have to run into community forums for the technical support. These are common issue with the free and open source software and be sure you are ready for these if you are heading on the free software road.

The other free Password Manager is LastPass where this software is a cloud based Password Manager. It is very good software to me except that the database which is your passwords is stored on the internet. Personally, I don't feel comfortable storing my online banking password on the internet. I prefer to store this type of sensitive information on my local PC. As a result, LastPass is not my choice for Password Manager but not going to close this option off as not everyone thinks the same as me. If you are comfortable storing your password on the internet, LastPass can be a very good solution and best of all, it is free.

Summary of Step 7

This is the summary of the seventh step in building a secure environment for your computer.

- Create a unique strong password for each account.
- Manage them with a Password Manager.
- Change your password often – your password should not last any longer than 3 months.

Step 8 – Ensuring your computer is safe

Image Credit: Stuart Miles – FreeDigitalPhotos.net

By now, you should have all the necessary things to start with. However, being able to keep all the incoming threat away is not good enough. Who knows that your existing system is clean? Before you start to prepare to battle the incoming threats, these are the things that you need to do to ensure that your existing system is worth to be protected.

Perform a full system scan

Having an Antivirus installed is good but not good enough. You need to ensure that you had run at least once on the full system scan. This is to ensure that your current system is Malware-free and only with that, your system is worth to be protected. There is no use to protect an infected system, isn't it?

Check critical software for new updates

Make a list on all the installed software in your system. Check each of the installed software to ensure that you are using the latest version. Any unpatched software can lead to vulnerabilities and security breach. I had previously mentioned that the Adobe Flash

Player and Adobe Reader are highly important and you should always pay attention on the latest patch.

Operating System updates

Next is to make an update on your Operating System if you did not previously configure to update automatically. It is also important to ensure that you had already done all the Operating System patches especially the security patches. Apart from making use of the vulnerabilities of your critical software and web browser to exploit your system, the vulnerabilities in your Operating System are also another area where hackers are looking to penetrate. A well patched system can knock off 90% of all the Windows-based Malware and you have no reason not to patch your Operating System and Applications. Ensure as well that you set your Operating System to automatically download and install new updates.

Summary of Step 8

This is the summary of the eighth step in building a secure environment for your computer.

- Use your Antivirus to perform a full system scan.
- Get a list of your installed application and update them.
- Run your Operating System update to ensure that your system is fully updated.

Step 9 – Clean up and Back up your computer

Image Credit: Naypong – FreeDigitalPhotos.net

This is going to be the last step where your system should be ready to go live securely in the next step. In this step, I personally advice that you should clean up your computer and backup all your data so that you can retrieve back if there is anything wrong with your system. I'm not saying that whatever we had gone so far will crash your computer but what we had gone through is for the good of your system and it is a good practice to always backup your data and optimizes your system.

Clean up and defrag

Whenever you performed an update on your Operating System, it is worth to run a disk cleanup to remove all the unnecessary files where at times, it can be pretty huge. In Windows, it is called Disk Cleanup and you need to run in in Administration Mode so that you can get all of the unnecessary data completely removed. If you had not run this application for quite some time, you will realize a sudden boost of free space after cleaning up your disk.

After getting all the data removed, the next step is to defrag your disk. In Windows, it is called Disk Defragmenter where this software

will defrag your entire disk to ensure that you have a faster performance. The concept of disk defragmentation is like arranging the books in the library in order. It makes the process of finding a particular book faster than unorganized one. If your disk is fragmented and you do not defrag them, it is going to be like looking for a book in an unorganized library.

Backup your data

Have you been practicing the habit of backing up your data? What if one day, your hard disk crashed and all your data inside are gone forever? Have you ever thought of the worst situation and what you are going to do to get all your data back? I had been always thinking of this and I always keep part of the data which I cannot afford to lose in another separate medium.

There are two ways to back up your data. The most common way is the manual way. You copied all the important data to one folder and then copied that folder into your backup location such as CD, DVD, another hard disk or your own FTP site. This sort of backup is only applicable for a small size backup. If you want to back up everything in your computer, it is going to be difficult.

For a bigger size backup, you might want to consider using the backup feature provided by your Operating System. However, that type of backup might take some time and file size can be very big. I had used the Windows 7 backup feature and it can still be considered a feature to be used by ordinary home user.

If you are someone that is very particular about data backup and looking for a very professional tool, you can probably check out the Genie Backup Manager Pro where it is the Editor's Choice of PC Mag due to its user friendly and powerful backup.

Genie Backup Manager Pro is powerful, flexible, exceptionally well-designed and reliable backup powerhouse –PC Mag

Summary of Step 9

This is the summary of the ninth step in building a secure environment for your computer.

- Run the Disk Cleanup.
- Run the Disk Defragmenter.
- Download or purchase backup software if necessary.
- Backup your data.

Step 10 - Schedule your work

By now, you should have the necessary tool in your computer. What I afraid now is that whatever that you had applied might eventually just return to nothing when you close this book and forget everything. I try to avoid such event and that is why in my last step, I will guide you all as well to schedule your things so that you will not forget.

Schedule your activity

There are couples of things here that need to be scheduled.

- **Quick Antivirus scan**. You should scan your computer on a daily basis. Yes, I am still in my sanity and what I actually mean here is to perform some sort of critical scan or quick scan on a daily basis. It should not take a very long time and I estimated that it can be completed within an hour. Most Antivirus today comes with a complete scan and a quick scan where you don't need to worry on how to perform that.
- **Full Antivirus scan**. You cannot avoid performing a full scan but you don't have to do it every day. I recommended a weekly basis for a full system scan. If you somehow need to

abort the full scan, try not to do it more than 3 times as I do not advice going to the internet or using a computer without scanning for at least once a month.

- **Registry scan.** Don't scan your registry only when you have problem with the performance. You should schedule a regular scan on your registry and I recommended a monthly scan on your registry if you are not performing massive installing and uninstalling.
- **Web browser scan.** If you keep your number of plugins low and set your browser to automatically update the latest version, you simply don't have to schedule this. As I had mentioned, the most secure way is to have as little plugins as possible. It boosts your security and eases your configuration.
- **Disk defragmentation.** You should defrag your disk at least once a month. If you like to create and delete things in your Operating System, your disk can easily fragmented and you need to defrag them. Depending on how you use your computer and generally I would recommend once every fortnight for a heavy user and once a month for a normal user.
- **Disk cleanup.** Disk cleanup will give you a little more free space after performing that and you do not have to do it often if you have lots of free space in your hard disk. However, I always try to run all these things at least once a month and you should as well, cleanup your disk at least once a month.
- **Data backup.** Data backup is extremely vital if you have important data going into your computer every day. For an ordinary user, it might not be the case which I suggest backing up your data at least once a month is sufficient. If you have important data that needs to back up every day, you might want to consider buying professional backup software to schedule your backup.

- **Change your password.** Passwords should be change at least once in every 3 months. Your password should not last you for life and I highly recommend you to change your password monthly on those highly important accounts such as online banking or money related account.

What are my recommendations?

I will advise you to use the scheduler provided by your application to run the tasks below. This is to ensure that you do not forget to run them and do check on the scheduled tasks to ensure that they are properly executed from time to time. Assuming that you have 4 awesome weeks in a month and you should utilize them as below.

- Week 1
  - ✓ Quick Antivirus Scan daily.
  - ✓ Full Antivirus Scan on one of the days on weekends.
  - ✓ Disk Cleanup and Registry Scan on the other day on weekends.
- Week 2
  - ✓ Quick Antivirus Scan daily.
  - ✓ Full Antivirus Scan on one of the days on weekends.
  - ✓ Disk Defragmentation on the other day on weekends.
- Week 3
  - ✓ Quick Antivirus Scan daily.
  - ✓ Full Antivirus Scan on one of the days on weekends.
  - ✓ Data Backup on the other day on weekends.
- Week 4
  - ✓ Quick Antivirus Scan daily.
  - ✓ Full Antivirus Scan on one of the days on weekends.
  - ✓ Change your passwords and double check your scheduled activities on the other day on weekends.

Summary of Step 10

This is the summary of the last step in building a secure environment for your computer.

- Run through all the items mentioned in this step and create a schedule for them.
- Manually execute the tasks if you unable to schedule them to execute automatically.
- At the end of month, check the logs to ensure that all the tasks are properly executed.

The 15 DON'Ts of Computer and Internet Security

Having all the great software does not ensure your security without having a good attitude in using your computer and the internet. Just like having great weapons with great fire power but do not have a great soldier, it does not ensure you that you have a strong troop of army. Below you will find 15 things that you should not do on your computer or when you are on the internet.

1. **Don't click on any incoming links on your instant messenger especially from an unknown sender.**
   Incoming links from an unknown sender are very likely malicious. They mostly so-called claim that they had a sexy picture of you to lure you into clicking so that they can either phish you or inject a Malware into your computer. So don't click on anything if you do not know the sender.
2. **Don't click on the links in your email especially the notification type of email.**
   Lots of notifications today especially from social networks such as Facebook, Twitter, and LinkedIn are not 100% legitimate. I had encountered a few notifications which are fake and the links in the email leads me to somewhere that contains Malware. I had taken one of those samples and wrote it on my blog where you can check it out to see the proof of it. Read the article here.
3. **Don't disable your Antivirus protection.**
   Computer gamers like to disable their Antivirus when they experience poor gaming experience with their computer due to the reason where the Antivirus took most of the resources. Disabling Antivirus is like asking all the policemen in a country to go to sleep and never wake up. It is not secure and you should not disable your Antivirus at any sort of

condition. Learn how to enable Gaming Mode from your antivirus or get one that can do it. There are many good Antivirus today that comes with this feature such as the BitDefender series.

4. **Don't disable your Firewall.**
   People like to disable their firewall when they have problems in sharing their files on a Local Area Network. This situation can be worse when forget to enable back the firewall protection. My advice is to learn how to configure your firewall to allow access to certain files or folders for certain user. You only need to learn it once and you will be safe starting from that day rather than just disable your firewall protection.
5. **Don't reveal your password.**
   Never tell your friends about your password or even write it down. Password is supposed to remain private and confidential where nobody should know or even physically see it. You should always remain your password as '******' if you really planning to write it down.
6. **Don't disable the UAC (User Account Control).**
   This thing usually happened when you are on the spree to install and uninstall lots of applications. You will find it troublesome where your Operating System keeps asking you the administrator's password. Don't disable your UAC for convenience sake as there should be some effort to pay for a good security. Be inconvenience and be secure.
7. **Don't just download and run an executable file.**
   Most of us just download an application or installer and just run it right after the download is completed. If you are very sure that you are downloading from a reliable source, such as downloading Windows 7 from Microsoft official site, it is still acceptable to just run after download. However, if you

are downloading from a site which you don't even know, make sure you scan the file first before running it. Who knows that you might have just downloaded a piece of fast spreading Malware?

8. **Don't ignore error messages.**
   Whenever you see an error message, don't ignore them. Try to understand what it is trying to tell you. Especially when you are accessing a HTTPS or SSL site, ensure that you do not do any of your online banking stuff if the site has an issue with the SSL certificate. It could be that the certificate had been revoke, expired or you are not accessing a valid domain.
9. **Don't panic.**
   If you are someone that easily panics, then you are the favorite target for any Scareware attacker. Some programs are programmed to tell you how many Malware that had infected your system which you don't have. The trick here is to get you to buy a fake Malware removal program which does basically nothing. So don't panic. Get a reliable Antivirus to do a full scan and let them tell you the truth whether you actually have an infection or not.
10. **Don't forget to logout especially from public computer.**
    Public computer is not your home computer. The minute where you are done with checking your Facebook or any other things on a public computer and just walk away, the next person comes in will be able to see and do all the things that you can do to your Facebook account. Not just Facebook but what I mean here is every online account as well. Remember to logout and ensure that your session is already cleared before walking away from using the public computer. Best is, don't login at all. Use public computer only to read news or some blogs.

11. **Don’t forget to lock when you are away from keyboard.**
    Ensure that no one touches your computer except for you. By having the habit of locking your Operating System whenever you are not in front of your keyboard will ensure that no one else touches your computer. You need to protect your privacy and certainly, you can’t trust your colleagues, friends and people around you.
12. **Don’t visit Adult Site frequently.**
    If you are a big fan of adult materials, be sure you don’t do it often or don’t even do it on a computer where you want to use it for important transactions. There are many adult sites which contains Malware and generates lots of unnecessary pop ups. If you want to stay away from those and keep your computer clean, don’t go to any Adult site especially the ones that you don’t even know.
13. **Don’t keep the unnecessary.**
    Although hard disk size is pretty big today, it is not advisable to keep all the unnecessary programs. If you know that you have 10 programs which you did not use for the past 3 months, delete them. Keeping them is not only wasting space, but also lead to security issue. Who knows one day where those programs will have a vulnerability to be exploited?
14. **Don’t just enable everything.**
    From time to time, you should be very clear on what you are doing. If you want to share a specific file, then just share that file. Don’t share the entire folder or drive. If you want to share for specific person, then just share it to him/her. Don’t share to everyone. Know what you are doing and don’t allow everything or enable everything in your computer.

15. **Don’t trust anyone.**

When we talk about security, there isn’t anyone that we can really trust. If your friend sends you a message which contains a link, don’t just trust him and click on it. His account might already compromise and trusting him is like trusting the hacker who hacked into his account. Don’t trust the people around you as well by not keeping your privacy private. Sometimes, people might just want something really important from your computer and will take full advantage from it when you walk away from your computer without locking it. So trust no one but yourself.

Build Your Own Security Round Up

Round Up for a Secure System

Antivirus – Kaspersky Internet Security more info

Firewall – Kaspersky Internet Security (more info)

Registry Cleaner – PC Fix 2011 Registry Cleaner (more info)

Data Encryption – ZoneAlarm DataLock (more info)

Password Manager – Kaspersky Password Manager (more info)

Data Back Up – Genie9 Backup Pro (more info)

Round Up for Free Secure System

Antivirus – Avast Antivirus (more info)

Firewall – Comodo Firewall (more info)

Registry Cleaner – Wise Registry Cleaner (more info)

Data Encryption – TrueCrypt (more info)

Password Manager – KeePass (more info)

Data Back Up – None

Resource Directory

Antivirus

Kaspersky Internet Security – more info

ZoneAlarm Antivirus plus Firewall– more info

BitDefender Total Security – more info

Avast Antivirus (Free) – more info

AVG Antivirus (Free) – more info

Microsoft Security Essentials (Free) – more info

Panda Cloud Antivirus (Free) – more info

Avira Free Antivirus (Free) – more info

Firewall

ZoneAlarm Pro Firewall – more info

Kaspersky Internet Security – more info

BitDefender Total Security – more info

Comodo Firewall (free) – more info

ZoneAlarm Free Firewall (free) – more info

Outpost Free Security Suite (free) – more info

Online Armor (free) – more info

Registry Cleaner

PC Fix 2011 – more info

Registry Mechanic – more info

Wise Registry Cleaner (free) – more info

Eusing Free Registry Cleaner (free) – more info

WinMend Registry Defrag (free) – more info

Registry Life Registry Cleaner (free) – more info

Data Encryption Software

ZoneAlarm DataLock – more info

Kaspersky KryptoStorage – more info

TrueCrypt (free) – more info

Password Management

Kaspersky Password Manager – more info

LastPass – more info

KeePass – more info

Data Backup

Genie9 Backup Pro – more info