

*DISCLAIMER: This information is provided "as is". The author, publishers and marketers of this information disclaim any loss or liability, either directly or indirectly as a consequence of applying the information presented herein, or in regard to the use and application of said information. No guarantee is given, either expressed or implied, in regard to the merchantability, accuracy, or acceptability of the information.*

# **15 Steps to PC Security**

## **Table of Contents**

**Step One - How Secure is Your Home Computer**

**Step Two - All About Viruses**

**Step Three - Password Protection**

**Step Four - Back Up Important Files**

**Step Five - Should You Have a Firewall?**

**Step Six - Do You Need a File Encryption Program?**

**Step Seven - What Are Patches and Do You Need Them?**

**Step Eight - Beware of Opening eMail Attachments**

**Step Nine - What You Should Know About Phishing**

**Step Ten – Download & Install Safely**

**Step Eleven - Instant Messaging Do's and Don'ts**

**Step Twelve - Setting Up a SAFE Home Network**

**Step Thirteen - Keeping Your Children Safe Online**

**Step Fourteen – Attacks on Your Computer**

**Step Fifteen - How to Stay Informed**

## **Step One - How Secure is Your Home Computer**

### Ensuring the Safety and Security of Your Home Computer

With the popularity of and the reliance on the Internet by almost the entire world population, there are suddenly a lot of things you can do and know with literally one click of the mouse. Making purchases nowadays doesn't require you to go to the shop or store; you can buy items online. Researching for various pieces of information can now be accomplished via the Internet.

However, there is an unfortunate reality that goes along with the wonders of the Internet. It also thanks to the Internet that computer security is always an issue. With the continued growth of the dependency of people (including businessmen, offices, government officials, and more) on computers and the Internet, this is a more important issue than what most believe.

If you are a home computer user, you still need to make sure that your computer is safe from any form of malicious online attack, including hacking. You might have important data (including any identification) in your computer which intruders can have access to.

That being said, it is important for you to find out just how safe your computer is from these potential attacks.

The very first step before actually tinkering with your computer is finding out the motive of intruders and why they target home computer users. They do this because (1) home computer users typically don't have security measures installed to counter them, which makes them easy targets; and (2) they often have valuable information stored that is enough to entice these intruders, such as credit card information. Think about it – you might potentially be a target.

Following that, you have to know what types of attack to expect – it is usually via email or clicking an ad-banner on a website. Opening an unknown, seemingly innocent email or clicking on an ad-banner will sometimes put you at unwanted risk and open the door for intruders. Once they're in, they're sometimes hard to get rid of, so your home computer security should start with you being careful about the things you do while connected to the Internet.

Being careful doesn't mean just choosing which emails to open or not, and which ad-banners to click to or not. This also includes sending

valuable information over the Internet, which is at risk for interception by a third party. It would be better to transmit really important information the old-fashioned way, unless you are very much confident in your security measures.

Next would be trying to place security measures in your computer itself. If your operating system is Microsoft Windows, they offer security updates and malicious software removal tools every month which are extremely helpful to you – the same goes for other operating systems such as Apple OS and LINUX. There are monthly updates because the intruders always try to find a way to get around these security measures.

After getting the free security updates of your operating system, you need to get an anti-virus program, preferably one that has the greatest number of virus definitions (you might need to purchase this). Viruses, aside from causing chaos to your computer, can also be used to retrieve information from you and spread out to attack other computers. By obtaining a high-quality anti-virus program, viruses would not be as much of a problem.

Since intruders know the capabilities of anti-virus programs, they sometimes choose to use what is known as spyware, which are little bits of data that can either be annoying or potentially dangerous. Aside from being able to slow down your computer processes, it can also be used to retrieve data from you. To combat this, there are anti-spyware programs available, both freeware and via purchase.

We will discuss spyware in depth further on.

The final security measure is a firewall. Normally, anti-virus programs offer firewalls; so acquiring one should not be much of a problem. A firewall acts like a security guard – it disallows outright entry to anything trying to access your computer (even if it is a program), without asking for your confirmation.

If you do not have these as your PC security and safety measures, you might be highly susceptible to an attack from intruders, if they haven't done so already. These measures ensure you that your computer and the data inside of it are safe and secure.

## **Step Two - All About Viruses**

### Computer Viruses and Guarding Against Them

In this modern Information Age, computers are necessities in life. Whether we use them for simple functions such as typing our homework and business reports, up to more important acts like online business meetings and transactions, one cannot deny that computers are a big part in our daily lives. Using a computer, particularly the Internet, is one task that even a ten year old can do at this particular period in time.

With the growing increase of popularity and reliance on computers, as well as the demand for it, security risks have also gone up, which is a reality that cannot be ignored. With the billions of information bits being spread across the World Wide Web, hackers and computer intruders (criminals) see the value in focusing their attention to computers and the Internet. The information they would retrieve here is (more often than not) more useful than when doing it the old-fashioned way.

As such, these intruders have devised methods to get information out of computer users, with or without these people knowing that they've been hacked. As is the case in real life, there are some computer programs that are disguised to be innocent, but actually act as spies, providing information to the intruders. These malicious programs, which are security threats, are called computer viruses.

Computer viruses should not be taken lightly. They work in many different ways; one of them may be to provide data to the one who planted the virus. Other viruses can simply be annoying - slowing down your computer, building unwanted files, etc. - while some can be very disruptive, such as deleting your hard drive, compromising your operating system, etc.

As such, there are different types of viruses, which normally differ in how they function and how they are spread. Examples of these include Trojan horses, worms, email viruses, and logic bombs. It would be important for you to know these kinds of viruses in order to better protect you from them, as well as to have the proper programs to get rid of them.

Trojan horses are simply computer programs that cannot reproduce themselves, but can do damage anywhere from minimal to extremely dangerous. It usually disguises itself as a common file (maybe an .mp3 music file or a .jpeg picture file) but does the damage when the computer user opens it. This is why you should take extra care when opening a suspicious looking file – it could very well be a Trojan horse.

Worms are self-reproducing programs that mainly use security holes in order to spread itself throughout the network. If your computer is infected with a worm and is able to replicate itself a number of times, this usually causes your computer to slow down noticeably since it uses your computer resources and memory to do so. They often use security flaws in operating systems (such as Windows) in order to self-reproduce.

Email viruses are self-explanatory – they spread via email. Once a user opens the infected email, what it usually does is send itself to other computer users via the email addresses found in the user's address book. Because it uses email and a lot of people open emails without really checking or being careful, it spreads very quickly across the entire world and can cause chaos within just a few days.

Logic bombs are viruses that target specific computer applications, causing them to crash (for example, Windows). This can also be spread via email attachments or by innocently downloading it off the Internet. It can cause a great deal of harm (particularly if it infects Windows and the like), or just a small amount (small program).

Fortunately for computer users, there are anti-virus programs available anywhere, whether in the Internet or at the computer shop. These programs specifically target over thousands of viruses and wipe them clean from your system (if infected) or protect you from incoming attacks (if not yet infected).

Anti-virus programs are constantly updated (normally everyday) since there are always new virus definitions each day, and these new viruses can infect you. These software developers are always researching about the newest viruses to ensure you, the user, are protected from these viruses as much as possible. Your PC security and safety are always being considered.

## **Step Three - Password Protection**

### Preventing Password Hackers

PC security and safety is always an issue nowadays thanks to the advent of computer technology and the Internet. More computer intruders are boldly coming forward and are looking for ways to attack helpless computer users with valuable information stored in their PCs. Intruders are getting their hands on the latest security measures brought out by various developers and are looking for ways to get through them.

Anti-virus software developers are doing their best to ensure every computer user's safety and security from potential attacks by always updating their virus definitions and cleaning capabilities, as well as strengthening your firewalls. Sometimes however, it is not enough as intruders can be one or more steps ahead. They use various means of attacking computers so it is sometimes hard to tell what they're going to do next.

One of the ways is hacking in order to retrieve your password. Think of the many things they can do once they get your passwords – they can access any online accounts you may have, access your email to send

and retrieve messages from your address, enter secure networks – the possibilities seem to be limitless. In order to prevent these things from happening, you should have password protection.

The first thing you should do is secure your files and folders by using any password protection software, especially your highly important files and folders that could be potential targets of intruders. If these files are left unprotected, it would be easier for these intruders to get a hold of them and do what they want. Aside from that, other users of your computer (example – your kids) can accidentally move them or even delete them, which can be prevented by password protection.

Hackers and intruders would have an easier time figuring passwords out if they remain the same for a long period of time. It would be better for you if you change passwords regularly, especially for your more important data, for added security. By doing so, the intruders would have to start over again since you have a new password, thus making the possibility of frustrating them greater.

It would also be harder for hackers to figure out your password if you use a number of different characters, especially if it is a combination of letters, numbers, and symbols found in your keyboard. Of course, it

will be harder for you to remember a combination of these three also, so you have to make sure to memorize the combination, more so if you regularly change passwords.

A useful tip: it is recommended not to use passwords that are codes like your birth date, spouse's name, or other relevant information because it can make deducing your password quicker and easier. These "coded" passwords are often used by a lot of people, particularly in ATM machines and email passwords. By doing this, you are more susceptible to attacks since the password is easier to figure out.

Aside from following these tips that you can do on your own, it would be to your benefit if you obtain password encryption software. The meaning of encryption is that it disguises the password written in cleartext format into ciphertext, which is a combination of different symbols. Decryption is what the intruders try to do, which is change the ciphertext into cleartext that they can see and understand.

A password encryption software, which is available on the Internet via online purchasing or in your computer software shop, encrypts your passwords in order to discourage intruders and prevent them from accessing your password protected files. Various software come with

various levels of security, some of which contain a higher level of encryption than others. Higher encryption levels would make it more difficult for the intruder to break in.

Your PC safety and security is not limited to anti-virus software, anti-spyware software, and firewalls, because unauthorized people can target the passwords themselves. It would be better for your overall security if you take the necessary precautions and means when it comes to dealing with password protection. Securing your important files and folders with passwords, changing them regularly, using a combination of characters, and encrypting them through password encryption software, will ensure your safety from password hackers.

### **Step Four - Back Up Important Files**

Avoid a Computer Crash: Back Up Important Files

You've heard horror stories about it, or perhaps you've experienced it yourself. Many people have nearly gone insane after the disaster that all computer-dependent individuals shiver at the thought of: the great computer crash.

A person can literally lose everything he has saved on his computer in a blink of an eye. The reasons are varied. At times it occurs after an ample amount of warning signs, other times it comes as a complete surprise (making it more disconcerting). When these moments happen – and they do happen, and quite often actually – one can only hope that he has saved his files elsewhere, otherwise, there is little hope that they will be recovered.

Are you scared yet? If you don't want this to happen to you and your precious files (which I'm almost sure you don't), read on and find out how to create backups for your many important files.

But first off, if you're still not convinced of the importance of backing up, here are a few reasons that might convince you.

### Top Reasons Why You Should Back Up Your Files

1. One of the few universal truths in life is, no matter how in control you are of your universe, something, someday will inevitably go completely wrong, and usually it is something that will happen beyond your control. The same is true for the files on your computer. No

matter how updated and top-of-the-line your hard drive is, it will someday inevitably give up on you and your files.

2. Numerous viruses abound in the computers of individuals around the world – computers that send and receive files through the Internet. There are also the numerous floppy disks, CDs and flash drives that connect to your computer. Any one of these can be a carrier of a harmful virus that can wipe out the data stored on your computer. If you don't have a backup for this data, you're most likely never going to see them again.

3. Power failures are one of the computer's worst nightmares (which also include running water and becoming obsolete). They happen without notice, especially when the weather is bad. And power failures can just as easily ruin your computer and all the files on it. It is another good reason why you should back up your files.

The bottom line is it's better to be safe than to be sorry. There are many ways to bring about a data disaster, and there's only one way to be prepared for any of them, and that is through backing up your files.

Ways to Back Up Your Files

There are various ways to back up the files on your computer. You can use Internet programs and services that allow you to back up your files on a separate server that can be accessed through the Internet. You can also use the conventional writable CD-ROM disc, where you can copy, paste, and burn the files on your computer through a no-brainer process. Zip disks are also effective for backing up files, as well as external hard drives.

#### How to Choose the Data You Should Back Up

When backing up files, you don't have to copy the entire contents of your computer. Computer programs that you have a CD-ROM installer for often need not have a back up. Here are some of the files that you should definitely have back ups for:

- Bank records and other files that have financial information
- Digital images and pictures
- Software and music files that you downloaded from the Internet
- The contacts of your email address book
- Any other personal projects (essays, research and term papers for students; presentations, documents, and reports for the working folk)

- Important emails

### Some Final Reminders on Backing Up Files

Do label your storage materials. If you are using CDs, for instance, be sure to label and file them properly. Back up files are of no use if you can't find what you are looking for among them – and they're sure to pile up.

Don't use floppy disks as permanent storage for your backup files. The data inside them easily get damaged and won't last long enough to be useful as a back up.

## **Step Five - Should You Have a Firewall?**

### Step Five: Should You Have a Firewall

As we have already discussed, the Internet is littered with evil intentions and malicious - albeit smart and brilliant – plotters. They are constantly in the prowl for innocent, unprotected computers. Internet hackers use all sorts of codes such as viruses, worms, and Trojans, to crack into and ruin your computer. You must therefore be

prepared to block them off from ever entering your computer's system at all times.

It is often said that the best cure is prevention. And the saying applies to your computers. If you want to protect your computer from the threat of viruses, worms, Trojans, and other malicious code, one of the best options to take is setting up a firewall.

What is a Firewall?

Imagine a firewall to be the fence that sits between your computer and the Internet, or between your computer network and all the other computer networks out there.

It serves as a defense mechanism against harmful codes or data that may destroy your computer, and it works by examining the information that attempts to enter your computer or your network.

When a firewall is set up properly, hackers will not be able to detect your computer in their search for vulnerable ones to victimize.

What are the Types of Firewalls?

Firewalls are generally divided into three categories: software firewalls, hardware routers, and wireless routers. To know which kind of firewall is suitable for your needs, there are two factors on which your decision should depend on:

1. The number of computers that your firewall will service
2. The kind of operating system that you use (it can be Linux, a version of Windows, Apple Macintosh, and so on).

### Choosing a Software Firewall

If you are planning to set up a firewall for a single computer, it is ideal to use a software firewall. It also works well with most Windows operating systems. They are readily available from software development companies for a certain fee.

Some of the advantages of a software firewall include:

- No additional hardware is required for it to work

- There is no additional wiring that needs to be installed for the software to work.

However, there are also some disadvantages to deciding on using a software firewall:

- A software firewall may cause money and can be a bit costly
- You will need to install and configure the software to get it to work properly
- If you have multiple computers, you will need to install the software on each one of them to get them protected.

### Choosing a Hardware Router

If you are planning to protect a small network of computers, say in your home or at a small office, a hardware router is probably more ideal for you.

The main advantage of using a hardware router is that they are more convenient to use for multiple computers as they usually have at least four network ports to which you can connect a number of computers.

However, its major disadvantage is that because of all the wiring that you will have to setup for it to work, it can potentially clutter your workspace.

### Choosing a Wireless Router

If you want a wireless network of computers, you would definitely want it protected by a wireless router.

Some advantages of using a wireless router include

- No wiring will be required, so it avoids clutter. It can connect personal computers, printers, and scanners, without the use of any physical wiring.
- It is ideal if you want to protect a set of laptops, notebook computers, and desktop computers

Some of the disadvantages of using a wireless router include:

- The radio signal that wireless devices use (including wireless routers) can be intercepted by other individuals with the right equipment.

- Wireless routers are not always equipped with a built-in firewall, so you might have to purchase a firewall separately
- You might have to purchase extra equipment to set up a wireless router

Operating systems such as Microsoft Windows XP and Microsoft Vista are already equipped with a built-in firewall, but older versions of Windows as well as other operating systems require that you set up a separate firewall.

Setting up a firewall is recommended to any computer owner, especially to those who have very important data stored in their computers. Often the question lies not on whether you need a firewall or not, but instead on which type of firewall you should set up.

### **Step Six - Do You Need a File Encryption Program?**

Step Six - Do You Need a File Encryption Program?

As the world becomes more advanced each day, it also seems to grow less and less secure. The creation of new virtual venues has also paved the way to the emergence of places where people can be

victims of criminal activity such as fraud and identity theft. In the real world, people of high stature get the service of bodyguards and security forces. Would such protective measures also be beneficial for the world of data?

Most people think that data security is something that only large business entities would have to be concerned about. However, the Internet is an open channel can be accessed by anyone. And now that people are doing more personal matters through the internet, such banking shopping, sending confidential mail and personal letters, it is probably just right for people to take more steps to keep their privacy and security.

The answer to this situation is file encryption, which is basically a more sophisticated and powerful manifestation of the age-old art of ciphering that has been used by humans throughout history. Do you actually need to take advantage of such programs that make your files secure through complicated encryption? Perhaps knowing more about file encryption would help you decide the right answer to this question.

What exactly is a File Encryption Program?

A file encryption program basically uses complex algorithms to create codes for file contents so people other than their intended recipients cannot easily read them. File encryption programs write messages, files, and other content into codes that can only be deciphered by persons who would have a decoder. It is somewhat similar to the way students write secret messages in class, they use different ways to manipulate messages in such a way that other people would not be able to understand them.

The big difference between the codes that people make and file encryption programs write is the complexity of the encryption being made. While the codes people normally make could take just a few analytical hours or minutes to decipher, the ones made by computers are so complex that they cannot be able to be unraveled by practically anyone even for a lifetime. In fact, even other computers who would not be able to decipher the codes without the right decoder.

The function of file encryption go beyond the field of information technology – computer files and electronic messages, it is also used by other industries such as in the entertainment business. For instance, DVD movies are encrypted so that consumers could not easily convert digital video into VHS format. Encryption is also used in to scramble

videos of pay-per-view channels and only those who would pay would be given the codes to unscramble the reception.

Perhaps the most important application for file encryption programs is for privacy protection of people and organizations. The most commonly known example is this would be the message encryption being done for confidential electronic messages and projects being sent via the Internet. Another example would be the decryption used for telephone conversations and satellite transmissions that help protect the security of concerned parties.

Do you actually need to get a file encryption program?

As mentioned, file encryption has many functions and the need for such security measures depends on the way you use your data and the way you go about your activities in open channels such as the Internet. You have to carefully check what exactly you do when you are online.

Do you do banking transactions through the Internet, or do you just view websites of your favorite stars? Do you send business messages and projects to your clients and colleagues through email, or do you

just send jokes and funny quotes to your friends? Do you shop online and give out your credit card information, or do you just window shop and check out what you can buy in real stores?

When deciding whether you would need file encryption or not, you have to ask yourself if the things you do online actually require you to be secure. If you normally give vital personal information such as your credit card, social security number, addresses, and the like, then you might benefit from buying a file encryption program. But if you do not really do things that could compromise your security then, perhaps getting file encryption would just be a waste of your money.

But still, it never hurts to be safe. If you have extra cash and would like to be sure that you do not fall prey to the many dangers that lurk in technology, then by all means go and get a file encryption program. In these days where the world is becoming more and more complex, one can never be certain of what could happen.

### **Step Seven - What Are Patches and Do You Need Them?**

Step Seven - What Are Patches and Do You Need Them?

A patch is generally the term used to refer to pieces of software that are created to give updates or fixes to existing programs that need to be rehashed or repaired. Patches fixes bugs, replaces graphics and improves a program's performance or functionality. Patches are very useful and are usually needed if there are certain imperfections in the programs you are using, however, patches that are not made perfectly can also lead to other problems.

What are the different types of patches?

Programmers create different forms of patches, each having its own function and characteristics. Software that has proprietary policies is delivered as executable files instead of sources. Such types of patches alter the executable program run by the user by either completely replacing the entire executable program or just making changes to the binary file.

Other patches may also be circulated as actual source code themselves. In such cases, there would be certain textual differentiation between the original source code and the one included in the patch. Such kinds of patches are made for projects that have open sources. For these types of patches, the programmers assume

that the users would be able to do the update themselves without the help of executable files.

Patches may also come in larger forms. And since the term patch is usually associated with small or short fixes, bigger patches are sometimes called service packs or software updates. Microsoft Windows are known to use such terms to refer to their updates. However, even in the guise of another name, they are still patches nonetheless.

Other operating systems such, as Linux, among other systems that are similar to Unix, have patches that are distributed as full software packages. Such patches have their own installers that work so that they can serve as an upgrade to current existing versions or as stand-alone installers that can be set up on their own.

How are patches used?

Patch sizes vary and may be as small as some kilobytes or go as high as a hundred megabytes and higher – the larger the size, the larger the change the patch is bound to do. Typically, when media, such as pictures and sounds, are changed or added instead of program, files

become rather large. This is usually seen in patches designed to update or modify computer games.

Unlike software designed for initial installation process, patches generally are faster to apply. Some patches may be acquired from the manufacturers and sent to users in diskettes or discs, while others may be downloaded through the Internet. Patches that are downloadable could take longer to acquire depending on the connection speed.

Most patches that are designed for operating systems and software for computer servers are created to fix important holes in the security system. Some operating systems allow automatic update or semi-automatic updating that allows the continual feed of patches whenever there are changes done by their authors.

A lot of people, especially those in the corporate world, decline getting totally automatic updates because there were many experiences of patches causing glitches. Some software experts also believe that allowing totally automatic updates may let software companies acquire limitless control over people's computers. Thus, varying degrees of automation has been offered in relation to getting patches.

The use of totally automatic updates is rather more popular for the consumers because most operating systems, Microsoft Windows in particular, have added them as a support tool. Its creators have also set the automatic updates for Windows as default.

Some users, especially network system managers, are very wary about installing patches. They put off applying them until they have clear proof that the fixes are stable. Most large patches or those that promote sudden significant alterations are distributed first with limited availability as beta tests for qualified developers who would know what to do in case something wrong happens.

Patches that are made to modify the programming of hardware are called firmware and are rather challenging because they entail complicated steps such as re-embedding sets of code on devices that involves that total modification and installation new codes for programs instead of just simple alterations to the existing version. Usually such patches perform delicate modification processes that could compromise the device if not installed properly, rendering it useless.

Do you really need patches?

There is no quick answer to this question. Patches are intended to improve the performance of your programs, however, they have to be very stable so that they would not do more harm than good. Before installing a patch, check for its stability by asking around about reported problems with installation.

You can check Internet forums regarding users' experiences with the particular patch you are about to apply. It is usually wise to put off the patch installation for some time before going with it to see how people react to its effects.

### **Step Eight - Beware of Opening eMail Attachments**

Step Eight – Beware of Opening eMail Attachments – the Danger of Unknown Packages

Among the most popular and useful functions of the Internet is email. Not only could people send messages to practically anyone all over the world, they can also send digital files such as pictures, sounds, and programs. However, much caution must be taken when opening such attachments because the Internet is teeming with malicious minds that

craft ways of inconveniencing people, or even getting something of value from them.

What are the dangers of opening email attachments without caution?

While a lot of email attachments, especially those that come from your contacts, may typically just contain innocent stuff such as pictures of your friends, the latest music from your favorite band, or spreadsheet reports from your colleagues, email attachments may also come with things that could damage your computer. Among such things are viruses and spyware.

Every day, people in the online community discover new viruses, worms, and Trojans – software packets that are designed by malicious hackers to do damage to your computer. These programs usually attach themselves to unknown files that are sent to your inbox, and when you open them, you are often unaware that you are already triggering some damage to your unit. Sometimes, seemingly innocent files come up and since they seem so harmless, you just go on and open them without worry, but a lot of such seemingly safe files can actually be very damaging.

Why do people do such a thing?

Some hackers make viruses just for the heck of it or just for laughs. Such hackers just want to prove to the world how good (or rather bad) they are about the computer. But some hackers have more motives other than making pranks. There are hackers that are out there to get something from you that they can use for criminal activities.

A lot of viruses that are distributed through email typically get access to the infected computer's list of contacts or address book to look for email addresses to which it can distribute itself. There are viruses that can even forge your name and appear as if that you are the one sending it to your contacts. By doing this, it can replicate and spread itself all over the world to do its damage.

There are also viruses that get vital information from your computer that its creators may use for themselves. Critical data such as your credit card number, social security, and addresses, among many others may be maliciously obtained and used for crimes such as fraud or identity theft. While most of the viruses would not automatically retrieve this from your computer, they could lead you to give the

information yourself, without you knowing that you are actually falling prey to those cunning malicious minds.

But do security systems and antivirus programs not protect people?

Indeed you may get a certain level of protection from firewalls and antivirus programs, you may even get a very good level of security. However, multitudes of viruses are created each day, and there is not telling if what you receive is the latest one. Your computer might be equipped to fend off millions of viruses that have infected people in the previous days, but when you catch a new virus, the chances that your program may be able to fight it could be pretty slim.

What should then be done with such danger lurking in emails?

The most that you can do is to be cautious about your online activities, particularly when opening file attachments to the email you receive. Be very cautious when you are opening email attachments, particularly for computers that are using Microsoft Windows, because such computers are what most viruses' target.

Before opening an email attachment, be sure that it comes from a trusted source. However, do not be too complacent about opening attachments from friends and colleagues because as said earlier, viruses may mimic your contact's information to make it appear that these attachments come from them.

Do not open file attachments that you did not expect to receive. If you get an unexpected email with an attachment from one of your contacts, ask them if they did send something and what is inside that file. Avoid opening attachments with file extensions such as .cmd .scr. .pif .bat and .exe, because such files easy for viruses to attach to.

You can never be too careful in such an open channel as the Internet. As the old people would say, it is always better to be safe than sorry.

### **Step Nine - What You Should Know About Phishing**

Are you Phishing?

You can say that the Internet is a short cut for "international networking." By just logging on, you can connect to people all over the world. They may be people you personally know or people you just know online. Whatever the case, there is always somebody on the other end of your Internet connection.

As accessible and easy daily life is now thanks to the Internet, there are disadvantages from this convenience. Criminal activities such as eliciting sexual activities on the web are an example of online problems society has to deal with.

Another online criminal activity is phishing. Phishing is acquiring personal information like passwords and credit card details by pretending to be a representative of a company. Phishing is done through email or instant messaging.

It is called 'phishing' because it is similar to the recreational activity fishing. It 'fishes' for users' personal information such as passwords and financial data.

Phishers create accounts on AOL by using fake algorithmically generated credit card numbers. These accounts are maintained for a number of months. Due to the reports of phishing incidences, AOL has brought in measures preventing this from happening by securing the data of their users and confirming the information of those signing up for AOL accounts.

On AOL, a phisher pretends that he is an AOL employee and sends out instant messages to a random customer that asks for passwords of their account. Luring the victim further, the phisher includes in the message "verify your account" or "confirm billing information."

Thus, a number of clients get lured in and give off their password. Once the phisher gains access of this sensitive information, he can use the victim's account for spamming. Check your inbox and take a look at the spam messages you've received. Yes, those are real names of people. These people's accounts have been hacked and are now being used to relay spam messages.

Because of this, AOL assures their clients that no one from the staff of AOL asks for their personal or billing information. Also, AOL has created a system that deactivates accounts as soon as there are signs that it is used for phishing.

Other recent phishing incidences involve that of the Internal Revenue Service. There is a way for phishers to know the bank of their potential victim. Then they pose as an employee of that bank and send an email to their victim.

Also, social networking sites can be a home base for phishers because personal details that have been printed online are used for identity theft. Statistics show that over 70% phishing attempts are done in social networks.

Another technique used by phishers is coming up with a link in an email that belongs to a fake organization. They often use misspelled URLs or sub domains to trick potential victims.

Note the web address and check the @ symbol. For example, <http://www.google.com@members.tripod.com> may be a link that can easily deceive anyone casually observing the page. However, whoever clicks on this will be merely directed to a page that simply does not exist.

To tend to this problem, Internet Explorer and Mozilla give users the option of either continuing or canceling their surfing. With a warning message, the user can just go to that questionable page or not.

There are some phishing scams that utilize JavaScript commands. These alter the address bar and are done by imposing a picture of a

credible entity URL over it. These visually deceive a casual Internet user.

Another phishing technique is the cross-site scripting. Here, the culprit uses a legitimate company's own scripts on a potential victim. In doing so, the user is directed to sign in for the services of the imposed company. The security certificates and web address appearing on the page may seem correct for the non-professional eye. In truth though, this link the potential victim has clicked on is a way for a phisher to know his personal and financial information.

Damages from phishing are:

1. Loss of access to email that can also lead to financial loss.
2. Identity theft making the victim vulnerable to online criminal activities.
3. Access of public records

Once sensitive information such as credit card numbers, social security numbers and mother's maiden name are acquired, it will be so easy for the phisher to manipulate the account of his victim.

For every problem, there is a solution and anti-phishing techniques been created to prevent this online criminal activity from taking place. Users are taught to not believe every email sent to their inbox. When you get a message asking for your personal information, contact your bank or the company that supposedly sent you the email and verify it with them.

Then there is the Anti-Phishing Working Group that serves as the law enforcement association dealing with phishing incidences. From them, anti-phishing software can be downloaded by websites and uploaded as their homepage web content. Eventually, the toolbar displays the real domain name and serves also the guard dog against suspected phishers.

Installing Firefox and spam filters also protect the users from phishers. These programs reduce the email received by their clients.

In the end, it is all carefully reading the messages you receive in your email. As soon as it sounds suspicious, report it to the Anti-Phishing Working Group.

## **Step Ten – Download & Install Safely**

### Safety First When Downloading and Installing Programs

Not only people can get virus. Even computers can get those annoying buggers. Do you want your PC or MAC to crash just because you were careless enough to let one small virus eat up its way around your files?

Most computer viruses come from the countless programs the World Wide Web offers. Each one of them is appealing and tempting for the modern-day consumer. However, a smart consumer knows that before buying (some require credit card payments) or downloading a program, a thorough research must have been conducted beforehand.

Some say that searching for the appropriate programs for your system is very much like searching for the right appliances for your home. That is not exactly the case. The former is more complicated than the latter.

With appliances, there is an assurance of what the product does. Also, there is a warranty. Once, the appliance you bought is not functioning as much as you would want it to, you can always have it replaced or get your money back.

Whereas with programs, you have no idea what the CD can do to your system the minute you put it in. There will always be side effects so how do you gauge the possible risks involved?

The reason why you are resorting to a program is because your computer has needs, which you want to satisfy. Nonetheless, some programs cause changes into your system the minute they are installed. You have to figure these out all on your own.

Here are some tips you can apply when buying programs:

1. You must know as much as you can about the program before you download or install this into your computer. The free program offers may be quite inviting but you must be updated on the possible changes it can contribute into your system once you have installed it.
2. There must be a refund/return policy. Do understand these important terms just in case the program you bought does not meet your expectations and standards.

3. Buy from a local store with a credible reputation. Read up on the best place where you could get the program that you need.

Moving on to another situation, what about those programs that can easily be downloaded from the web? How would you know whether these are worth installing into your system? Sometimes, these programs are virus-carriers because of their easy access.

That being the case, these steps can help you determine whether it is worth downloading and installing or not:

1. Ask yourself this: what does the program do? The web page (when you're downloading it online) or the CD-Rom (when you're installing it on your computer) must clearly state the exact description of the program for the customer's benefit. Learn as much as you can but you must also take into consideration the credibility of the author.

2. Ask yourself whether you are okay with the changes that will occur in your system upon installation of the program.

3. If the author is stated on the web page or on the CD Rom, the better. In that case, you can contact him via email or telephone and ask about the program first-hand.

4. Testimonials from previous customers are also good information you can rely on when researching on the program. Naturally, they would have experienced what you eventually would.

Some customers go with their instincts. Regardless, they are careful enough to back-up the important files and folders from their systems just in case the program creates a problem and their computers go awry.

There are programs that help you prevent the virus from entering into your system in the first place. It is best that you have this in your computer. But you must also note that there are situations wherein the computer will not be able to instantly recognize a virus.

For example, you clicked open a forwarded message in your inbox containing a virus. Now your computer had a hard time detecting this virus. You may have an anti-virus program installed into your system but these situations still do happen.

In the end, you must always rely on you. Read up on the program you want to install or download. Check on the credibility of the information stated on the web page or the CD Rom. Contact the author if you can to verify the statements. And always back-up!

### **Step Eleven - Instant Messaging Do's and Don'ts**

Beware of what's in instant messaging.

Believe it or not, instant messaging services are now just as susceptible to viruses and other scammers.

Since almost anyone and everyone has access to e-mail, viruses now have the ability to infiltrate both your office and home as this popular form of communication is being used by virus writers to spread electronic worms and viruses.

According to a study conducted way back in 2003 by the Internet Security of Symantec, viruses and worms that were spread using instant messaging services have increased to 400%.

The instant messaging worms

Currently, the worms Bizex and Jitux.A are now targeting the instant messaging services of MSN as well as ICQ.

Infiltrating the contacts of a particular user's IM currently spreads the worm Jitux.A. However, the Bizex worm has an intent that is more malicious, it sends a user a link to a particular web site that have already scanned the computer you are using for any electronic finances or payments.

Since it was discovered, the site has since been shutdown, however it is yet to be known the quantity of data they have already collected, albeit maliciously.

Do not be complacent

Though the major virus threats have already been discovered, this is no time to be complacent. Threats could still continue. As more users know better on how to stop traditional virus attacks, writers of viruses will continually look for other targets.

This is according to CyberScrub president, Bill Adler. And the soft targets are currently instant messaging services.

Yet do not panic

Relax this is still no reason for you to throw away your instant messaging service. Be aware that many viruses in IMs do not automatically propagate.

Usually, clicking a link or downloading an applet is what would be required to download a virus or a worm.

Avoiding these threats require that users constantly be vigilant and always do safe computing.

Do not trust friends

Or at least those messages sent by friends. Unbeknownst to your friend, he could be sending you a link that would lead you to a particular site (under the guise that it was supposed to be a picture of someone you both know) that would get you to download software.

When actually, it is a Trojan horse that would automatically install spyware and adware on your PC and easily distribute itself.

It's during these moments that anti-virus software would be a big help.

Another thing that should not be trusted are games. One such example is a game called Osama. It's been found that it is spread via instant messaging.

It is spread via instant messaging via a link inviting users to download the game wherein the idea is to pretend that one is catching Bin Laden.

Those who clicked and downloaded the game and BuddyLinks which were able to grab all the user's contacts in IM and sent the same message link to everyone.

A lot of software could help

Thankfully, there are security and anti-virus software that could extend the coverage protection of instant messaging services.

Zone Labs, for instance, has released IMSecure. It is a program that makes it possible to encrypt messages as well as block hazardous and dangerous URLs.

The anti-virus software of Norton by Symantec has in its feature the scanning of instant messages as well as McAfee. These software programs are able to remove different viruses from any files that were received through instant messaging.

The good thing about the mentioned software is that it works. Based on the tests conducted by PC World, a lot of anti-virus software has been able to catch known worms and viruses that were sent via instant messaging.

However, it is also a fact that there is really no defined anti-virus software program that could one hundred percent prevent all known attacks from viruses or worms.

Vigilance is always the most excellent defense.

All in all, one way to prevent threats from worms and viruses is by not putting your whole trust to any content that you receive from the Internet especially through instant messaging.

Prevention is always better than a pound of cure. Being wary of any files sent through IM is not being paranoid; it is being safe rather than sorry later on.

### **Step Twelve - Setting Up a SAFE Home Network**

Networking computers at home is easy as 1-2-3

Securing the computer in your home is a task that requires your full and serious attention.

They take a lot of your time and there are steps that need to be done. The following are some of the tips and advice you could do to be able to secure your very own personal computer.

Anti-virus programs is a must

Imagine it this way, would you allow someone to knock at your door and enter your own living space in order to make you buy something or use your own telephone?

If they were neat and presentable enough you could probably let them inside your own home, but just like anyone else, you definitely would be watching their every move.

Observe just what it is you have done. You have already profiled that person and based on the profile you have come up with, have also decided what you will do.

This is because you are very much cautious and concerned on just who enters your own space.

Basically, this is how anti-virus programs work.

These programs scan all contents of every file, looking for patterns that are specific and one that would match a particular profile. This is basically termed as virus signature – or something that is notoriously harmful to your computer.

Every file that has a signature match, the program provides options on just how it should respond. One such response is by removing the patterns that are offensive or one that destroys the file.

A virus basically works this way. They are like salesmen who knock in your own living space and they would get you to buy or listen to their sales pitch. However, they could try to pilfer your money or valuables.

One way to know if a particular scammer is prowling in your neighborhood is probably by reading about them in the news or seeing them in a TV news report. These reports could give you an idea of what these scammers look like or what are the things to be wary and watch out for.

Anti-virus software programs basically work similarly. When the vendors know of a new potentially threatening virus, they have a set of updated signature viruses that could include the new virus threat.

Scan and check, check and scan

Other ways and means for viruses to enter your personal computer is via floppy disks, web sites, email, CD-ROM as well as downloaded files.

As much as possible, all these avenues must be checked if they contain viruses or not.

For instance, prior to using a particular floppy disk, it must first be checked for any viruses.

Also, when downloading a specific file from the net, these must be checked for any viruses. Your own anti-virus software program usually allows you to specify and check these places for any viruses. They may also do this scan automatically.

Patch it now, patch it good

The instance your computer's system breaks down, do you have an idea on how you should restore its functions?

Many vendors have patches whose purpose is to fix any types of bugs. Usually, vendors offer patches that are free in their own web sites. When purchasing programs, it is a great idea if you ask the vendor how they supply patches.

Software vendor programs also have a service that allows you to a recall. Notices for patches could be received via e-mail through mailing list subscription. Through this service, one can easily learn computer problems even if you have yet to discover them and before any intruders could have the opportunity to exploit your computer's system.

Be cautious when reading attachments via e-mail

Always be careful when opening received e-mails that carry attachments. Sometimes, the potentially threatening messages could come from unsolicited e-mails.

To be able to determine if an email is safe or not, it would be best to conduct the following test and ask these questions: did someone you know send the email? Did you receive this e-mail before? Is the subject of the email described in a clear manner?

A suspicious e-mail usually reads as BradPitt.jpg.vbs. Worms could travel this way and reading / opening it could bring damage to your computer system.

All in all, caution and care is needed to be able to protect your computer from unnecessary attacks by malicious viruses and worms.

### **Step Thirteen - Keeping Your Children Safe Online**

Keep your children safe from pc and online security threat

Children, like adults, are just as susceptible from computer and Internet security risks. Thus, it is important to keep children safe and have your data protected.

The following are simple yet effective steps so that security threats could be reduced dramatically.

Implement parental pc control

It is always best to implement a kind of parental control when kids are using the computer. Fortunately, there are ISPs available that could be purchased as software that is separate.

However, keep in mind that a software program is really a poor substitute for authentic supervision provided by a parent.

Through using the Internet Explorer, it allows anyone to conveniently restrict or simply do not allow particular web sites to be seen.

Settings for these could be set through passwords.

In order to see these options, click on Tools on the menu bar, then choose Internet Options, select the tab named Content, click the button named Enable under the Content Advisor.

It is also best if you purchase software that enables you to watch and monitor any and all sites your kids go to.

Partition it now, partition it right.

It is advisable to partition your personal computer into accounts that are separate. Many operating systems (these include the Mac, Windows XP, Linux) provide users the option to create different and various user accounts.

This works well especially if you have that fear of your kid accessing, modifying or deleting your own files. Giving your child an account that

is separate decreases the access amount and the privileges your child has.

Use anti-virus, anti-spyware, firewall

Software that provides anti-virus activities protects computers from any viruses that could destroy data, help prevent slow performance of your computer, helps prevent crashes and does not allow any spammers to infiltrate your e-mail.

Basically, this works through scanning the computer and any e-mails that are incoming. If there are any that contains viruses, these are automatically deleted.

An effective anti-virus program should have constant and routine updates as well as antidotes for any latest bugs that are currently in the Internet.

Meanwhile, firewalls have the ability to keep any hackers away from your own computer thereby preventing them from accessing any of your personal info without your express permission.

Basically, a firewall is a guard that watches any attempts from the outside to access your personal computer system. It also blocks communications to and from sources that does not have your permission. As much as possible, always turn on your firewall and regularly update it.

Anti-spyware programs meanwhile protect your personal computers from any malicious forms of spyware. What spyware does is monitor all activities you do online. It also collects your personal info while you innocently do your surfing on the web.

Through anti-spyware, it scans in a periodic manner your computer to check if it has any spyware software and programs available. After which, it offers you the opportunity to immediately remove harmful software.

Password protect your pc

Using passwords that are strong or utilizing authentication technology that is strong helps you protect your personal info.

As much as possible, keep all your passwords in a secure and safe place. Do not share your passwords over the Internet, phone or e-mail.

Remember that your ISP should not ask your password.

Hackers have the ability to acquire your password, unless of course you make it difficult for them to guess it through the following efforts: use passwords that contain eight characters including with it symbols and numerals; avoiding words that are common; avoiding using personal info; changing regularly your passwords (at least every three months).

A good way of creating a password is to come up with a phrase that is memorable and using first letters of every word as the password of your choice. Convert these letters into particular numbers that look like letters.

Do not forget to back up files that are important

The fact of the matter is that there is no such system that is one hundred percent secure. If there are any files that are important and are currently stored in your own computer, always copy them in discs that are removable.

After which, store them in a place that is secure.

You could also consider software encryption. It is also best if the start-up disks in the original software you bought are readily available just in case your computer system crashes.

All in all, helping your children safe from online security threats is an effort that is well worth it.

### **Step Fourteen – Attacks on Your Computer**

Make your computer immune to attack

Prevention is always better than a pound of cure.

Believe it or not, it is now utterly impossible to survive without a computer. Almost anything and everything could be done on-line nowadays.

From purchasing to selling to paying bills, one really need not go out as any transaction could actually be made thru the computer thanks to the Internet. Unless, of course, fresh air is also available online.

However, the computer's flexibility has also allowed it to be vulnerable to attack from one of the most potentially harmful entities around: the computer virus.

The instance you detect that the computer you own is infected with a virus, the following are helpful tasks that you could do to protect it further and to also avoid other personal computers to be affected as well.

Use disks from trusted sources

You do not allow your shoes to tread on any mud puddle or any dirty floor, or your shirts to be easily vulnerable to stains or dirt. Therefore, it is always best to treat your computer the same way.

As much as possible, always be careful with what kinds of disks as well as files enter your computer. The files were downloaded from the Internet or the disks borrowed from friends, it is always best to make sure where they come from or to scan them in order to avoid any potentially harmful viruses.

It is also not a good idea to download any files from Internet sites that are unsafe or insecure. Also, do not immediately open attachments received via e-mail.

Take a good look on the subject of the email as well as where the email came from. Be wary even if the email was from your contacts.

Fortunately, there are now facilities in email services that immediately scan attachments prior to opening them. Email subjects that are vague and from senders that have gibberish email addresses must arouse your suspicion.

Included in this group are those emails that aggressively claim that you should "Check out this message!" Or that you should "See the following pics!"

Acquire a program that fights viruses

Fortunately, there are a lot of anti-virus software programs that scan and eliminate viruses once they are detected. This allows anyone to safely and confidently share data and disks, the freedom to download

any files from the Internet as well as open any attachments received via e-mail.

When the virus hits

Fear not. As much as possible, relax. There is a way out of this predicament. All you have to do is to visit the web site of the manufacturer of your anti-virus software. They may have the latest software, which, if it will not delete the harmful virus, could identify and detect it.

Search for a vaccine

The world wide web is available at your beck and call so you could search for any information you may need with regards to the particular virus that you want deleted.

By entering the virus name on the search engine, all information as well as vaccine may present itself.

Download, download, download

Be free to install as well as download any patches of software or programs that could help in eliminating the computer virus.

You could also try to religiously follow any of the instructions that you will find in order to manually delete the virus.

Do not rest on your laurels

Do not be easily convinced that once the computer virus has been deleted, the virus is now totally eliminated.

The best way to determine if the virus is completely destroyed is via running a virus scan. If the scan reports that no virus components have been detected, you can now relax.

Un-attach yourself from attachments

Caution must always be practiced once attachments have been received. The file extensions that one should be careful in opening are those that end in \*.exe, \*.doc, \*.ppt or \*.xls.

However, those that end in the following extensions such as: \*.js, \*.vbs should – as much as possible – never be opened.

All in all, every computer is vulnerable to be attacked. What one needs to protect your own PC is caution and preparedness to look towards the future and anticipate any potential attack prior to it happening. This ensures your computer to run as smoothly as it possibly could.

### **Step Fifteen - How to Stay Informed**

Be updated with current and future security threats now

Now that we have discussed the threats to your online security, let's review and summarize how you can remain informed about potential threats.

The Internet and e-mail are amazing resources that everyone utilizes to communicate with each other.

Unfortunately, it is also being used for malicious activities such as scammers that use the e-mail to get money from computer users.

Fortunately, there is an easy way to recognize any attempts of scamming that arrive through e-mail.

Knowledge is power and the descriptions indicated below are three of the email scams currently being used by scrupulous individuals. Stay informed and read on.

Scams via phisher

How this e-mail scam works is through this: usually, you will receive an e-mail from a service online provider or through a bank that will ask you to go click a specific link or visit a particular website and from there you will be elicited to provide your personal info.

This type of scam is called phishing.

Basically, this scam is where victims are asked and tricked to entering all their personal info like passwords, account numbers to an organization or company that presents itself as legitimate.

Ingenious scammers who create a site that looks a lot like the authentic web site do this trick.

E-mails are usually used to invite and bait potential online victims to go to the fake website.

As much as possible, always be cautious and wary of e-mails that ask you to click a link and give out personal sensitive info like bank details.

You should know that any info provided on these fake sites are farmed and harvested by scammers which they in turn use to steal the funds from the user's bank account or steal the identity of the victim.

Be aware that companies that are legitimate would never ask for any sensitive info through e-mail.

Never, ever click on these e-mail links. Never give out any info about you. If there are doubts on the veracity of the e-mail, it is always best to directly contact the legitimate company.

How to know a scam if you see one

Generally, a scam has the following characteristics. It makes the promise to give you lots of money, lots of prizes or a job.

It also asks you for donations. It also proposes business deals that are lucrative. It also asks that you provide personal and very sensitive info. It also asks that you follow a specific link to a particular website and log in to a particular account.

Educating yourself is an essential contribution against being vulnerable to fraud as well as any virus or security threat.

The worm

Just this year, a worm that has the ability to e-mail itself in massive amounts target users of Yahoo Mail by arriving in inboxes with a subject that says: New site, along with it an attached forwarded message.

The worm was written using JavaScript and allows embedded scripts written in html to automatically run in the browsers of users.

Basically what this worm does is fool unknowing e-mail recipients to believe that they have received an online card and to click on a particular web link to access it.

However, once clicked, a Trojan is immediately downloaded to the user's computer and is disguised as an html file thus innocently appearing as a web site page.

Receiving any e-mail that is similar to this should not let you be fooled. As much as possible, do not in any way follow these links in an e-mail message especially if you are not sure that it would lead you to a greeting card web site.

As much as possible, check the site's true destination prior to clicking it. It would help if you course your mouse over the link and thru doing so immediately see the file extension.

All in all, staying informed is one way to harness power thru knowledge of current trends and updates on potential security and online threats.

This allows ample time for anyone to prepare their system and thereby prevent unnecessary crashes and problems brought about by malicious and threatening viruses, worms or scams.

Believe it or not, luck has little to do with this. The meeting of opportunity and preparation does much to make safe computing a reality that is possible and livable, now.