

KEEP YOUR PC SAFE FROM VIRUS AND DATA LOSS

SELECTED TIPS - 88 PAGES!

Keep Your PC Safe From Virus And Data Loss!



88 Pages!

Brought to you by Chools

Contents

Spyware Can Destroy	9
Is Adware/Spyware Legal	10
How Does Adware/Spyware Spread?	12
How To Remove Adware/Spyware?	13
What Programs Help Prevent Adware/Spyware?	14
Why Stop Spam?	15
How File Sharing Causes Spam	16
Anti-Spam Filters	17
How Spammers Get Your Email Address	18
Choosing The Right Anti-Spam Program	19
PC Performance: Increasing Speed	20
PC Performance: Time For A New CPU?	22
PC Performance: Use Free Registry Repair	24
PC Performance: Microsoft Cleaning Systems	26
PC Performance: Solutions For Slow Computers	28
Antivirus Protection: Worms – The Most Dangerous Computer Virus	30
Adware: The Underlying Truth Revealed.....	32
Antivirus Prevention: Keeping Computers Free From A Virus	34
Spyware Scan	36
What's The Snag Behind The Spyware.....	38
Free Spyware Killers: The Only Resort For You Vs. Spyware Battle Victory	40
Hunting Down Spyware And Adware	42
The Need For Adware And Spyware Blocker	44
The Solution To Your Spyware And Adware Problem	46
The Difference Of Adware, Spyware And Anti-Virus	48
Totally Free Spyware Removal: Tips That You Can Follow.....	50
How To Remove Spyware	51
What Is Malware?	52
Why Free Spyware Removal Tools Are Offered	54
The Spyware Threat	56
ZoneAlarm Internet Security Suite For Antivirus Protection.....	58
Data Recovery - What Is It?	60
Data Recovery - Viruses And Malware.....	62
Data Recovery - Restoring Deleted Files.....	64

Keep Your PC Safe From Virus And Data Loss

Data Recovery Software	66
Data Recovery In Windows	68
Data Recovery Services	70
Data Recovery - Insurance And Disasters.....	72
Data Recovery - Evidence Recovery	74
Data Recovery - The Importance Of Backing Up Data	76
Data Recovery - Continuous Backup.....	78
Data Recovery	80
Types Of Data Loss.....	81
Data Recovery Software	82
Data Recovery Services	83
Data Recovery Services	84
Backing Up Your Data	85

Spyware Can Destroy

Spyware and adware are two different animals. Each has the ability to make your life a mess. If you rely on the internet for anything or you rely on your computer for anything, it is a must that you fully understand what these things are and how they work.

The first key to protecting yourself from these things is to fully understand what they are. That will allow you to know how to not make common mistakes that cause spyware to get into your computer.

Unfortunately, many people have been lead to believe that all types of this software are bad and should be avoided. But, that's not always the case. The fact is you may want to have certain types of this software to use.

Remember, to make it spyware it has to be downloaded to your computer without your consent.

Why would you want to have spyware that tracks your personal information? Why would you want those advertisements? You may actually sign up for a service online and when you do you may also agree to receive targeted ads.

Companies like this find it helpful to track where you go online and what you do in order to provide you with ads that are targeted to your interests. Instead of seeing ads that don't have anything to do with you, you'll see ads that are based on the places you've visited online.

Is Adware/Spyware Legal

A common question that is asked is whether spyware and adware is actually legal. The fact is that in most cases the answer is, no, its not. But, that doesn't always stop all crime.

What is illegal is being able to get into anyone's computer without their authorization for any reason. In the United States, the law that covers this is the Computer Fraud and Abuse Act.

Since part of the definition of spyware and adware is that the process itself requires that a user download the program without the knowledge and/or consent of the user then it is quite illegal in itself. It is a tricky law, though, that is very open to consideration.

It is so difficult to prosecute those that make and distribute spyware and adware that it is, in fact, something rarely done. In some cases, many of these companies operate as standard businesses. It's not a hidden trade in any way, in many situations.

Why is it so difficult? One of the reasons this is the case is the fact that they have to prove that you didn't want to download the software in the first place.

Let's say that you were using shareware and the process included spyware. Some spyware providers claim that you signed up for the spyware as part of the bundle of applications.

Another consideration is just how you give your consent. Be honest, how many times have you read through those long, "Read me" agreements before purchasing or downloading some type of software?

If you don't read the End User License Agreement, as they are called, and click "yes, you agree" and continue, guess who's legally responsible for whatever happens?

To make this even worse, many of the spyware and adware companies will make these agreements excessively long and difficult to read and understand. You get frustrated and just hit that button.

Keep Your PC Safe From Virus And Data Loss

Of course, in most cases of spyware and adware, there is no agreement to sign anyway. The fact is that many of these are drive by downloads that you'll never know the program is there. In this case, there is no contract at all and therefore nothing to hold you to them.

The good news is that throughout the United States and in countries such as Australia, there is much law making happening to provide some protection from spyware and adware to the public.

In Iowa and Washington, within the United States, there have been laws passed that offer some protection. In these laws, specific types of spyware are targeted and made to be criminalizing acts.

How Does Adware/Spyware Spread?

One of the most important things for you to understand is just how spyware spreads. How does it get from its source to your computer?

By understanding this fact, you'll know how to better protect yourself from future invasion.

It's Not A Virus

One thing to know is that spyware and adware are not viruses and don't spread in the same way as a virus would. With a virus, the infected computer system is used to spread the virus from one system to the next. It is actively looking for the next victim. Spyware gets into your system by deception. In most cases, you download it to your computer.

You've Installed It

Most commonly, spyware enters the computer when the computer user installs it. Of course, you wouldn't know that you are doing that. What happens is quite a bit more worrisome.

You visit a website and find a piece of software that you would like to have. You download it. Little did you know that the software that you just downloaded had spyware piggybacked onto it and now you've got both the desirable software and the spyware lurking on your computer. You may not even know it's there for months!

Or, you may have the spyware trick you into downloading it. In this case, you may be asked to perform an operation that is "required" to complete the download. When you do, you are actually downloading the spyware or adware onto your computer.

How To Remove Adware/Spyware?

There are several ways to remove spyware from your computer. If you have knowledge of viruses, then you can easily understand most of these methods and how they are potentially beneficial to you.

Spyware can be detected in many of the same ways as a virus can. A scan of your computer can relieve many types of spyware and adware and help you to safely remove them from your computer.

The worst case scenario for the computer user that has a large amount of spyware and adware on their computer is to have to have their computer's system reinstalled. In this case, it will take professional help, in many cases, to back up the data on the computer and then to fully reinstall the operating system for the unit.

But, that's not the normal case and it's not the first step for you to take, either. There are several other things that you should do first. There is much help out there but it takes a bit more help and knowledge to get you to the point of knowing what program is a potential benefit and which is likely not to be.

It's Gotten Bad

It's important to realize that spyware is no longer something that happens to the other guy. You have to consider this a strong risk as you would a virus. You don't have to make a mistake in downloading it to your computer to be a victim to it. It can just happen.

In that, there are countless products on the market that claim to be able to provide you with the very best resource for removing spyware and adware from your computer. Some are very much capable while others can even be spyware programs lurking themselves.

What Programs Help Prevent Adware/Spyware?

Anti spyware programs are going to be the most effective and beneficial tool for you to use in your fight against all things spyware. In most cases, it will remove most of the spyware and adware from your computer.

Some types of spyware can pose a larger problem and often be difficult to remove. Nevertheless, there are some excellent tools available to help most computer users to combat the threat of spyware.

Programs Available

There are many programs on the market that can be helpful in removing spyware. While we are not advocating for any one program here, there are several that must be mentioned in order to learn what these are, what they can do and just where they came from.

One such program is that of OptOut. This program was designed by Steve Gibson and really became one of the founding tools in the fight against spyware. It was one of the first tools to do this and therefore was the foundation for other programs that were to come along.

Some of the most popular tools include Ad-Aware which was designed by Lavasoft. Another program is that of Spybot-Search and Destroy which was created by Patrick Kolla.

These programs have helped many to fight. In fact, they not only removed spyware but they worked at helping to stop the download of them, too.

You can also look at Microsoft for some help. Just months ago, they began working on a program to help with this type of protection. The program was for Windows XP, Windows 2000 or Windows 2003, and was a free downloadable program that expired in July in its beta version. It was called Windows AntiSpyware beta.

Why Stop Spam?

When it comes to the safety of your computer, one of the best ways to ensure that you don't get one is to avoid getting and opening spam emails. Spam emails often contain viruses, worms, Trojans, and spyware that can potentially damage your computer to no ends or simply make using your computer extremely frustrating. There are however many different ways that you can combat spam and that is what this article is about.

If you are interested in stopping spasm from ripping your computer to shreds, you can start by getting some general information on spam in the first place. You should also realize that there is more than one way that you can get trapped by spam. You can get much information about spam on the internet. This makes sense since it is through the internet that spam attacks you.

Peer to peer file sharing is probably one of the best ways to obtain any song you could ever want quickly and for FREE or cheap and it is also a great way to get a lot of spam. When thousands of people are connected to one file sharing program, the odds of finding any song are extraordinarily high. The music lover within you won't be disappointed nor will the movie lover either. Of course, the spasm that can come with registering for these programs is astounding. If this is something that you are interested in using any of the peer to peer programs you should do a lot of research on them first. Ares, and lime wire are relatively good programs that do not include much spam.

How File Sharing Causes Spam

File sharing has become an epidemic of its own in the past few years. The idea of getting something for nothing is simply too appealing to most of us. File sharing programs like Kazaa, Morpheus, and Ares are very popular as means of getting just about any music CD and DVD that is out there. Of course, you are basically just waiting to get stuck with some spam when you sign up with these. It's a very simple process.

These free file sharing programs often make their profits and provide these services because they make trades or sell their registration lists (which include email addresses) to other companies etc. this is how they are able to provide you with all of that stuff you so like to download from them. Not to mention the fact that they do not monitor the programs that are being shared which may also contain problems in them.

Every time you register with the free file sharing programs your email address is sent to any number of people. The next thing that you know, you are getting thousands of spam in your inbox and have no idea how these people got your email address in the first place. Well, now you know. That is just the tip of the iceberg when it comes to these programs. They are chalk full of things that can ruin your computer. And it all begins the moment that you register for them.

Anti-Spam Filters

There are so many anti spam programs on the market today that it can be nearly impossible for you to choose the right one for you. Many people are opting to use spam filters. These days, there are few tools that are more important to an efficient workplace than an excellent spam filtering service.

The down side here is that online junk-mail marketers are becoming more numerous and insidious by the day. Because of this, it is more important than ever to stop e-mail spam.

Did you know that the average employee who spends only a few minutes a day reading and removing spam email will waste more than 20 billable hours a year? If you actually multiply that by the number of employees who receive these emails and you have yourself a major productivity problem on your hands. It is time to fight back, and reclaim your employees' time.

Of course, with the ever-growing sophistication and available technology of today's spammers, anti-spam programs have often become so complicated that they're almost not worth the time it takes to install them. A few of the top companies, however, have managed to solve that problem.

They do this by simply sending all of your email through these companies' filters; spam can be pre-filtered so that your server never has to deal with it in the first place. That would certainly be easier.

How Spammers Get Your Email Address

E-mail spammers don't get your address because you're on the distribution list of legitimate e-mail publications. These days, it is a very rare mailing list that is completely open. That is not to say that there aren't any secure mailing lists, but it is very easy to get a hold of email addresses these days.

So where do these spammers get your address you may be wondering? The number one place that people used to use were posts on internet forums, and message boards. Newsgroups are "publicly" readable; whether you post your message on your local ISP or on a major service of some other kind, your message is typically spread worldwide by Usenet in a matter of hours, and it; as well as your email is quickly picked up by advertisers.

The current most-common place to get your address is from actual web pages. If your e-mail address is listed on a web page anywhere on the internet at all, such as from a contact section especially if that page is listed in a search engine or directory, spammers will find it. To know if this is possible all that you have to do is trying searching for your own e-mail address in Google. If you can find it there, spammers can too. Spammers get a hold of fresh addresses by going to web sites and scanning for e-mail addresses anywhere on the site.

Choosing The Right Anti-Spam Program

When it comes to anti spam programs and the general war against spam, there are many different programs types to choose from. When it comes to the safety of your computer, one of the best ways to ensure that you don't get one is to avoid getting and opening spam emails. Spam emails often contain viruses, worms, Trojans, and spyware that can potentially damage your computer to no ends or simply make using your computer extremely frustrating. There are however many different ways that you can combat spam and that is what this article is about.

If you are interested in stopping spam from ripping your computer to shreds, you can start by getting some general information on spam in the first place. You should also realize that there is more than one way that you can get trapped by spam. You can get much information about spam on the internet. This makes sense since it is through the internet that spam attacks you.

You can use just about any anti spam program when it comes to your home personal computer. However, if you are running a business you may need a bit more protection. Spam filters alone will not help you as you will likely be getting hundreds of emails a day. It helps to post your email as a direct link on your website rather than posting it because that is how spammer's software will find you. You can also use various anti spam software programs that will sift through them for you so that you don't have to.

PC Performance: Increasing Speed

Newly bought computers are excellent with their speed. However, with their increasing usage and with ongoing time, their performance starts getting affected. Most PC users register complaints related to their decreasing speed and deteriorating output. However, this problem can be tackled just by exercising little more care. The speed of your PC can be improved and the performance can be boosted.

Low Cost Solutions

Various low-cost and high-cost solutions are available depending upon which one you would like to choose.

These can be self performed and installed to increase the efficiency of your machines

1. Adding Random Access Memory to Computer

This is all about the mother board of your system. Adding RAM can increase the memory of your motherboard. Different memory options of 256MB, 728 MB or 1GB etc are available

2. Switching to SCSI Drives

This option talks about switching over to SCSI drive from your IDE hard drives in the computer. SCSI drives solve the problem of slow communication speed which is normally faced with the installed IDE hard drives.

Free of Cost Solutions

Speed of computer can also be increased without spending any extra money. Various methods are available:

- Regular disk cleaning and de-fragmentation of the computer. This can free up unnecessary space used by the temporary files
- Cleaning the registry is another option. This eliminates all the regular and routine entries done by your system. Care should be exercised here as one should not delete some internal

Keep Your PC Safe From Virus And Data Loss

software related registries. Help of internet can be taken and some basic research can be done

- Disable the applications which are unnecessary and not required. Whenever you do not use any application, it is better to turn it off. This reduces the program uploading and increases the speed. Unnecessary services provided by Windows can be turned off as well
- Automatic start load can be turned off and unnecessary options can be removed
- Reducing the font size can also help. Fonts also slow down the system. Therefore getting excused from excessive large font can also be a solution. System fonts should however be left the way they are
- Deleting the history of searches on the system is another option. Delete the cookies as well. (this can be done by going to the internet browser and then to internet options from tool menus)

However, one should note that some background is necessary for this. Without having basic knowledge and research such options should not be explored and if explored, care should be taken.

PC Performance: Time For A New CPU?

The efficient and accurate functioning of your personal computer relies on the speed of CPU mainly. The latest CPUs are extremely faster than the aged ones.

Switching over to a new CPU is therefore; the way adopted by many users to maintain the proficiency and smooth working of the computers. Here are some useful guidelines that can assist you to choose a new CPU.

A little survey will facilitate. Start with a survey around you to find out everything about the CPUs existing in the market. Keep in mind the model and features of your computer. Visit a few computer dealers nearby and gather some good opinions by letting them know the requirements of your computer.

Work out for yourself. Are you thinking of hiring a professional to fix it up? Just drop the idea as you can do it yourself.

- Before buying a new CPU, it will be helpful to be on familiar terms with the old one serving the computer. Make an effort to explore the CPU by unscrewing the computer. A number of tools may aid you in the process. Don't be impatient in touching the hardware.
- A word of precaution. Keep in mind not to rub your hands with your clothes. A static hand could be the result of this and touching any hardware with it could make your hardware loose life. This could be simply avoided by touching something made of metal, the computer cartridge for instance.
- Now, carry out a careful comparison between the two processors. You need to examine the way the old CPU is installed. Make an impression of all the settings, including the various locks and clips, in your mind. Learn to remove the locks, with no wear and tear. Take away the old CPU.
- Now reverse the process with new CPU. Place the new CPU at the right spot, put the locks and seal the computer.

Keep Your PC Safe From Virus And Data Loss

Congratulations. You have saved the money

The whole process is not only simple and trouble-free, but carrying it out for yourself could save you from spending some extra bucks. It is very easy for some professionals to make a good amount of money by just convincing you that this whole process requires some special skills. Be happy! No need to trust the false stories anymore. You have managed everything in a perfect way.

Well! You can make a fair amount of money by fixing this up for others. There are many people who appoint a professional to repair the minor computer problems. It's a good way to earn money by being such a professional.

PC Performance: Use Free Registry Repair

Are the applications taking time to process on your computer desktop? Do you have to wait long between the two mouse clicks? If yes, it's time to manage the speed of your computer. You need not to be aware of the computer software for doing this. Just introduce yourself to free registry repair software.

What makes the computer slow?

It must be surprising for you to know that there is a bulk of files accumulated in the memory that are useless for the system. Many of us try to get rid of them by clearing the browser history and disk clean but many more are generated by the application like java cache files, ad ware, installers and ant virus programs. This marks the entry of free registry repair that take care of computer's routine operations without letting it slow down.

Let the registry repair software fix it

- A large number of unwanted files are stored in your computer on a daily basis. It could be during installation or removal of any hardware or software from the machine. This repair software identifies them and eradicates them from the memory.
- If you try to do it manually, you will find it cumbersome to locate these files and delete them. This software saves a fair amount of time and finally enhances the proficiency of the machine.
- If you are a beginner, then it is not easy for you to identify the files that are not required to stay on your machine. The registry repair helps you in keeping the track of such files.

Quality overview

One such free registry repair available these days is Tune UP Utilities. It removes the useless files, thereby improving the booting speed of computer. Just experience the remarkable difference before and after running the repair. Not only this, it provides support to the novice users through its support area and online forums to solve all the queries of users regarding the

Keep Your PC Safe From Virus And Data Loss

services of this particular software. This software makes the computer immune from viruses.

Tune UP Utilities has earned praise from a number of sites and magazines for its reliable services and superior outputs. The high ranking among the most popular websites proves that this software is really excellent as it is a fact that these expert websites don't offer good ranking to any ordinary software.

Don't worry about cost.

This software is available absolutely free for you. You can express your gratitude in the form of donations that will aid the process of this software to develop further in future.

PC Performance: Microsoft Cleaning Systems

The daily use of a PC can create many temporary files and undue load on your system space. Mainly these unnecessary documents will occupy lot of MB space and tend to make your system slow. Therefore, an efficient window cleaning system is required for such problems. This will improve the computer speed and will also remove any sort of virus or bugs present in the computer hardware programming.

But, regular cleaning of the system is required to avoid major data loss or computer crash down. It will save you a lot of trouble and inconvenience, or else you may have to call a computer expert or technician. That means unnecessary wastage of money and time. To avoid all these problems, windows registry cleaner is the cheapest and the best way out. This software is freely available on net or any computer store. This disk cleaner increases the lifespan and speed of your computer. There are numerous types of windows registry cleaners, which can be easily accessed from the Internet. Some cleaner software is typically designed for your type of operating system.

The windows operating system is equipped with a central database that keeps track of the entire computer system including temporary files and cookies. Any thing you do on the computer is automatically added to the registry. This database system is called the registry, and it is basically a Microsoft product. It not only keeps a check but also co-ordinates all the software systems to network and work in unison, thereby delivering the perfect package that you always enjoy, albeit for a price.

But then is it not worth paying a small price for such a lucrative deal?

Windows operating system is designed to suit most of the computer systems. It's simple to use, but with a complex programming. It enables even a novice user to handle it with ease and confidence. But this designing genius system has often been criticized for taking an easy way of maintenance and repair. Microsoft has been criticized for taking an easy route of maintenance and regular repair to keep the PC running at its best performance. The hassles of ongoing maintenance have been ignored completely by the computer giants.

Keep Your PC Safe From Virus And Data Loss

But many kind of software are available in the market for performing ongoing maintenance checks on your system. Maintaining a windows registry cleaner is simple and hassle-free, provided you have the minimum tools required for its successful operation. Therefore, it's an easy task to maintain your PC in a perfect condition with effective use of disk cleaners and fixers

PC Performance: Solutions For Slow Computers

Is your computer slow? How often do you bang your keyboard hoping for a faster search results? Well, these are definitely not the right ways to handle a slow PC.

While it may be funny to watch a frustrated colleague in tussle with the computer, wait till you are in a similar position, in a vain attempt to get the system working fast. You might end up tearing your hair in frustration!

A complete rational and logical approach is the key to such problems. As we require doctors and medical experts for our body disorders, the computer also needs an expert human or software for its normal functioning, once in a while. If the computer is giving a slow output, maybe numerous files in your PC have become scrappy or fragmented. Basically, the data stored in the hard disk of your computer, over a period of time becomes diced and tends to spread out all over the system. When newer files are added to existing data files, in increasingly large numbers, they are difficult to maintain in the same block or folder, thus the computer starts looking out for fresher options or space to store the data. And the resultant files are literally adjusted into various folders.

And when you try to retrieve these fragmented data, the computer starts searching the bits and pieces and it may take a lot of time to assemble these pieces and present it on the display. And that's when you seek godly intervention for quicker results! But a very practical solution like a defragmentation process can go unnoticed, yes a defrag software can restore faster speed by cleaning up the mess that is the main cause for a slow speed of the computer. A defrag software mainly restructures the hard disk and puts together the fragmented data as close as possible for faster computer access. Another important utility of defrag software is that it manages to create free space by deleting useless data, with prior permission to store files in its entirety, thereby reducing fragmentation.

Usually such software are added at the time of installation of an assembled or branded computer, but these software programs can also be downloaded through the Internet, or brought from any computer store.

Keep Your PC Safe From Virus And Data Loss

Praying to the Almighty may help in a way as to showing you the right path for a correct solution in the form of defrag software! So don't fret, next time when your computer slows down, you know what to do to keep it going at its fastest best speed.

Antivirus Protection: Worms – The Most Dangerous Computer Virus

Get the idea on the Worms

Among the three widespread malwares or rather the malicious software, of Viruses, Trojans and Worms, Worms are the most lethal of all as they can carry out devoid of any human intervention. They replicate just as the viruses do, however they are more self contained as they don't require host program for proliferation unlike the viruses. Networks with several routers, servers and clients are usually affected by worms. However, Worms cause around the same damage like viruses do ranging from files deletion to corruption of programs. In the view of the fact, that internet is more of a knot of networks; it is quite vulnerable to worm attacks.

How do they affect Servers and Routers?

Servers are controlling computers having massive storage capacity and stock up generic resources which are usually shared by other depending PCs or clients within the network. On the other hand, routers route the traffic within the network and are more like dedicated servers having customized operating systems. When worms are unconstrained on the network, they proliferate all by themselves gobbling up the CPU time parting little or no time for the remaining programs to execute. This makes the network endlessly busy slowing down the network traffic.

Noteworthy worms

Payload is malicious software often carried along by worms. It could always be a spyware which would sneakily monitor activities and actions of your PC or the hidden access points of the network which is the backdoor installation program and could be used to steal data or spam programs from your PC by hackers. Another fast scattering worm was discovered in 2004 namely, MyDoom. Emails stretched this by enclosing the message "Andy, I'm just doing my job, nothing personal, sorry". The creator of MyDoom was by no means notorious; however, it is supposed to be directed towards the company website SCO, i.e., Santa Cruz Operation, so that the traffic of the website could be slowed down. Subsequently, this soon broadened to further

Keep Your PC Safe From Virus And Data Loss

internet sites, shoddily slowing down the different networks which were part of internet as a whole.

Ensure to keep your antivirus program running

The malicious Payloads accompanying with worms can lead to substantial breakdown in a PC in any network. Hence, it is always mandatory for you to switch on the antivirus programs within the network. If this is not followed, it is possible that data is transferred external to the network or files are deleted cautiously.

De-Worming

There are various firewalls designed to organize and control network traffic which acts as a shield to various PCs within the network by cloaking them well. They are rationally successful in saving the PC from worm attacks. Worms are mainly scattered to networks with the help of emails. Hence one should be extra cautious when opening emails from unknown senders or getting hold of mysterious files as attachments, as the distribution is by means of this source. No matter whatever precautions you take, at times your PC may be attacked by worms. If you think your computer is showing symptoms of being sluggish slowing down the internet speed, or re-boots often then it is high-time you scan the system with some antivirus software right away. If your confined software doesn't help in de-worming, then you can always refer the internet for the wide range of options available.

Adware: The Underlying Truth Revealed

The Adware is a special software used for advertising and is very popular on the internet, if you have ever been online, then you must have come in contact with the word adware. This unique software is used as a support for advertising online.

It helps programmers all around the globe to set adverts based on their desired result. Every programmer working for any of the internet advertisement companies really appreciates the adware because of the ease with which it passes information across the internet from one system to another, allowing the advert programmer to send adverts around the globe through the internet.

The Adware is used to play adverts, and also to download favorable adverts on the computer system. It can be used along with other applications which makes it very favorable to uses and that is the source of its popularity. The fact that it is highly lucrative to programmer is an alluring factor which makes it a best bet for all those programming adverts.

The adware has some similarities in function with the spyware. The reason behind the pop-up menus you see whenever you visit a new website is the function of adware.

Whenever you put an adware on a computer system it begins to trail every operation made on that system, it gives details of any one using the system and all the activities carried out. It is a special tracking device that might gather the necessary information of the user and transfer it to a different system or to an advertising firm.

The Advertising company by this device sends adverts to users using the pop-up menus, it is not compulsory though for one to view these sites, since he or she may shut it down.

Because of the public sharing of vital personal information, many users have decided to purchase other software applications that help to regulate, reduce or even remove the functions of the adware. This becomes important because of the risk of users sharing their vital information with advert companies and others on the internet. This software will monitor the level of information transferred from that particular system.

Keep Your PC Safe From Virus And Data Loss

There are different types of adware in use today such as: 123 messenger, 180 Search Assistant, Direct Revenue, just to mention a few.

It is good to protect ones private information, by the use of Adware; this will save you from all types of fraudulent activities going on around the internet. Once you install the adware on your system it makes it open to all, most especially, to the programmers at the advertisement companies. Due to this fact, there will be a surging in of adverts on your system, causing you to visit the sites of all these companies.

But the adware erasing or protecting software gives an answer to this problem, if you do not like the insurging of Advertisements to your system without restrictions. With this removing adware software your system with all its vital information are protected making it safe and also preventing all forms of theft that may occur. Care should be taken to get the removing software from the right source.

Finally, you should know that the adware is a good software that aids internet advertisement, without it, it is difficult to carry adverts from one system to the other. It is a necessary tool of all internet advertising firms.

Antivirus Prevention: Keeping Computers Free From A Virus

Computer criminals are out there producing virus every day, in fact it was reported that about three hundred fresh virus are created each day by these computer hackers. Eugene Kaspersky, a well known computer guru in terms of computer security affirms this fact. From this one can only see how desperate these criminals are and the need for the continual protection of computers all around the world.

Various kinds of viruses exist, just as there are various creators of these viruses. A virus type is known by the way it functions, there are some of them that are very deadly, some are gentle and some gradually destroy the computer system without revealing themselves until the end of their duty of destruction. It is our duty to always look for the way to uncover them before they finish the work of destruction, it not always good to allow the virus in the system for long, because of their ability to completely bring down the computer if left there for a long time.

To avoid the dangers of the virus, we need to exercise the greatest level of carefulness in our online activities, since the internet is the breeding down of all computer virus these days. When you are trying to download any software or file on the internet, always scan the program first with the use of the right mouse button, that way you will be sure it does not contain any virus. Do this also whenever you want to open an email attachment or any other file attachment on the web. Another way will be copy these files to a CD or disk and then run a scan on them, before using it. Better be careful than trying to cure damages after the harm has been done.

Do leave all the work for the antivirus software programs without putting in your effort to run scans periodically. Always be careful in your dealings online and make sure to scan before use, because as they say prevention is better than cure. Even the firewalls can only block away some viruses and warn you of some, but it can not be a hundred percent perfect in combating all forms of virus without human intervention. Do your best and the antivirus software program will do the rest.

It is advisable to back up all your important files, putting them in an external drive or on the drive D of your system. You should be careful to scan your C drive and D Drive periodically to avoid any threat of virus.

Keep Your PC Safe From Virus And Data Loss

With all these prevention steps taken from time to time you will be sure to have a virus free computer system with the use of the best antivirus system.

Please, feel free to use the instructions before as a way to get a good antivirus software program:

1. Make sure the antivirus software program offers both online and offline protection. Every good antivirus guarantees protection for the computer system while the user is browsing the internet and while the computer is not connected to the internet. There should be a two - fold protection offered.
2. Consult any of the independence testing agencies for advice or update on the best antivirus software program available. This update will help you make an informed decision at to what antivirus to buy.
3. Always make sure you update your antivirus software periodically so as to curb and track down every current virus around.

When these steps are followed, you will always have a Virus FREE computer system with the help of an antivirus.

Spyware Scan

The reason behind the production of spyware scanning programs was to stop the computer criminals who want to make use of the internet to commit a lot of crimes. They put the spyware into your system without your permission or notice and all needed information is carried away for use by the programmers that developed the deadly spyware.

There are some things you should know about the spyware:

1. The Computer is a Zombie

You should know that the computer system works more like the zombie, it is the exact thing to input that will come in the output. When it is affected in any area, it will definitely be evident.

This is characterized when your system is affected by a spyware, instantly there will be signs showing the infection. When a spyware gets into any system, it begins to damage all the files and programs contained in the system. The Adware will begin to show numerous adverts, one after another, disturbing the work you are doing on the system. Once any little thing enters the computer system it affects it absolutely, this is why, care should be taken to ensure the proper operation of the computer since it is a very sensitive machine.

We really do not have absolute control of the computer system, if that was the case, we would have physically stopped the transfer of spyware, adware and malware into our system.

2. Stop Identity Theft

It is not funny to fall into the arms of those who commit identity theft, this can even lead someone into bankruptcy and dent your credit report. But, the spyware makes it very easy for this criminal act to be carried out. Once the spyware forces its way into your system, it immediately observes, records and sends the private information contained in your system, like the number of the credit card and only that is enough to steal as much money as possible, leaving you with the debt to repay. One should be very careful.

Keep Your PC Safe From Virus And Data Loss

To stop this identity theft you need to stop the spywares from getting into your system. That will stop every form of identity theft from occurring. This is the reason why all those producing the spyware are making it seriously in terms of finances, these criminals make a lot of money through this means.

The best way to put an end to this is to get an anti-spyware program that will remove all types of spywares from your system and protect it from further attacks. This will go a long way to curb the identity theft problem.

3. Do not Allow it Destroy your Program Files

When the spyware gets into your system it begins to destroy most of the files found in the system. It has a special pattern which it uses to carry out this work, but this special destruction pattern is only known to the software and its developer. It moves from one program file to another causing a lot of havoc to the computer system.

There are times when the spyware proves so hard to be eliminated from the system, especially if you are using an anti-spyware that is not so effective. In that case, you will discover that the spyware relocates whenever it senses danger, proving to be difficult. But, when a powerful spyware remover comes on board, it will be easily eliminated no matter where it hides in the computer system.

What's The Snag Behind The Spyware

The spyware was developed by programmers with advertisement companies with the intent of reaching targeted audiences if specific adverts that will meet the needs represented in all areas of their lives. This works by programming the spyware, getting it into the user's computer system without the knowledge of the user. The spyware now begins to work as a tracking device on the user's computer, monitoring, recording and reporting all the activities carried out in the computer.

Information derived from the user's computer system is analyzed to know the user's areas of interest and need, and the adware is used to bombard the user with the adverts fitting to his or her areas of need and interest. That is how the spyware works with the adware.

But, the fact remains that all these puts the user at risks, because in the process of monitoring, recording and reporting the user's personal activities on the computer, the information is not secured and is open to any one. This means that a criminal can get hold of this information and commit a lot of internet crimes at the detriment of the innocent user.

The spyware and adware can not be separated since they function together, one depending on the other to succeed. But, the spyware can operate on its own without the intervention of the adware sometimes, like the case mentioned above in the explanation above. When a spyware gets into your system, the computer's processing speed becomes unnecessarily slow, thus delaying the work of the user on the computer system, this can be very annoying.

There are many establishments looking for a way out of this predicament, in their search an answer was found, a solution was discovered and a way out was located to finally put an end to the menacing problem of spyware, adware and malware.

The product of these research was the invention, creation and provision of anti-spyware, anti-adware, and anti-malware software programs to fight this problem and provide a permanent solution to the problem. Today there are a lot of brand names of anti-spyware software program in the market. It will be wise to go for the best after carefully analyzing all the available options.

Keep Your PC Safe From Virus And Data Loss

Spyware is very dangerous and should be avoided, it is dangerous because of the following reasons, which are:

1. It is very deceptive, it comes into your system without your knowledge, causing a lot of havoc to your system.
2. It comes into your computer to pollute the whole system while carrying out its own functions.
3. It spies on your activities on the internet, knowing every move you make, every information you store or give out, hence making your system unsecured.
4. It is the easiest way to fall for those committing the crime of identity theft. The innocent user can lose a lot if this happens.
5. It disturbs the user by always showing up numerous adverts, making it hard to concentrate on the work at hand.
6. Most times it forces its way into the computer using various trickish means to accomplish this task. When anything enters your system without your permission, it is very bad and is a security risk,

Since the Spyware is known to be very dangerous and is considered a high risk on the computer system and on the funds of the computer user. You should put all hands on deck to see that this poison is out of your system permanently. The only way out is to use an anti-spyware on your computer.

Free Spyware Killers: The Only Resort For You Vs. Spyware Battle Victory

Whenever you have a spyware installed on the computer system it is always a serious problem, since it becomes almost impossible to get rid of it. In practice, no matter how hard you try to remove the spyware, it will not be completely eradicated since it has a way of hiding itself perfectly to avoid detection.

The only way out in removing the spyware from your computer system is through the use of a spyware removing software known as spyware destroyer or killer. When this is used, it becomes very easy to detect and destroy any spyware in the system and also block the spyware from the system so that it can no longer gain access to the computer system.

Before proceeding, it is necessary to explain the meaning of the spyware for those that do not know what it means. The spyware is a software programmed by some criminal developers to spy on the activities of computer systems. Once they gain entrance into the computer, they begin to monitor all the activities carried out on the system, these are recorded and transmitted by to the programmer that sent it. This tool is used for most internet crime.

This calls for the need to protect your system since all your valuable information are at risk of loss or damage with this dangerous spyware in your computer system. Take a step towards the right direction by locating a spyware destroyer to track down the spyware in your system before it tracks down and destroys both you and your computer.

The importance of the spyware destroyer can not be overstated, since without it you will be incapacitated, unable to tackle the problem of spyware, you should also know that a good spyware destroying software program performs the following functions:

All spyware destroying software removes spywares from the system, once installed into the system it searches through all the files and programs to detect the presence of spyware, once it tracks down any spyware, it immediately destroys. This program kills at sight, once it see any spyware it destroys it instantly, leaving the computer system free of all spyware threat.

Keep Your PC Safe From Virus And Data Loss

The spyware destroyer also goes ahead to provide a perfect protection for the computer system from further attacks of the spyware, by blocking the computer from all these problems in the future. With this absolute protection the user of the computer can be at rest, knowing all is well with his or her computer.

With any of the spyware destroyer on your system, there will be freedom for you to browse the web without restriction, knowing that your system is safe and protected from any kind of attack from spyware. You are free to easily download things from the internet, log on to any site of your choice and carry out all the transactions you so desire on the internet without fear. Once you notice a threat of a spyware a scan of the computer system will immediately get rid of it.

The most interesting thing about the spyware destroyers on line is the fact that most of them offer a free trail period, this will give you an opportunity to use it for a period of time to know if it is suitable for your system and if the trial convinces you, then the purchase is made. This method is very good because one will be able to test the quality of the product before buying it, to avoid buying something of less quality.

Finally, it is refreshing to know that one is not limited to only one brand of the spyware destroyer software programs. There are majority of spyware destroyers in the market to choose from. Many of them are free, while some are paid for. The very best one is the one that works better with you and your system. Make the right choice and destroy every attack of spyware on you computer system today.

Hunting Down Spyware And Adware

The Adware and spyware is avoided by many because of its disadvantages, since it has a way of negatively affecting the computer system. If the adware gets into one's computer system, it begins to cause unnecessary adverts to pop up denying the user the opportunity to concentrate on the work at hand. The spyware should be avoided too, because it monitors all the activities carried out on the computer system without the knowledge of the user. This is the reason many people avoid these software programs, doing every thing possible to remove it completely from their computers.

Many ways abound to rid our computers of these deadly programs, but incase the spyware and adware has spread to a large extent on the system, there will be no need to use any other means but to completely clear it out of the computer system through the formatting of the hard disk. To do this you will need to do a back up of all the files and programs in your system, so that you can still have them available to use.

But, if you discover that the spread of the adware and spyware is not much, you can get an adware and spyware remover or blocker software from the internet. There are some products that offer protection from adware, spyware and antivirus all in one, an example of this is the popular McAfee antivirus which gives an all round protection from antivirus and every other wicked software products.

The issue of virus, spyware and adware development in relation with anti-virus, anti-adware and anti-spyware has become a vicious cycle. The whole process is revolving without an end in view. More viruses are created each day and more anti-virus to combat them are also created. Sometimes, one might want to think that the same programmers develop the virus and then go ahead to create the anti-virus in order to make more money - I think that is exactly what happens.

Well, whatever the case is, all we are interested in is keeping our computer system as safe as possible so as to work without the fear of insecurity or of losing your valuable documents. The right thing to do will be to get an adware, spyware blocker, this will definitely keep these liches

Keep Your PC Safe From Virus And Data Loss

at bay, and ensure that your work on the computer and on the internet is not in any way disrupted.

Talking about working on the internet, it has been discovered that most of the adware and spyware transferred are through the internet that makes it very necessary to be extremely careful while browsing the web. Always make sure you run a scan on every attachment file to your email or instant messages, it is very easy to do that now, because this scanning feature is provided freely by Yahoo and the other servers. Another tip will be for you to also run a quick scan on every download link by right clicking first.

If you avoid pornographic sites you will do well, because it has been observed that these sites contain a lot of virus, adware and spyware programs, when you visit such sites you will discover that your computer has contacted any of the damaging software programs. It is always safe to stay away from such website, when you do well to avoid all these spyware, adware etc. you will not need to spend your valuable resources repairing the damage done.

Incase you need the best adware, spyware remover you can choose either McAfee, SpyBot or even Adaware. Which ever one you choose, make sure you continue to update to keep it current.

The Need For Adware And Spyware Blocker

Since 1995 there have been some software products available that has even become very popular in recent times. These are the Adware, Malware and Spyware, the spyware is the most dangerous among the group just mentioned, because it can be installed in your computer system without your knowledge that is a great danger. This is the reason why many do not like these software products, because they expose your system to unnecessary hazards.

The original intent for the production of Spyware is for the monitoring of the activities online, so as to easily detect criminals and curb fraudulent activities online. But, these software products are now used for fraudulent activities by scams and this has become a serious security risk.

This software is used to monitor criminals on the internet, so as to reduce the level of crime on the web, if that was the only way it is used, it would have been very good, because there will be no reason to fear since you are not one. But, in recent times, it has been discovered that even criminals can use this spyware to spy on other systems on the internet to commit internet crimes - this is exactly where the problem is, it is not safe in this sense. We might have experienced the spyware activity on the web, it is really not an interesting experience at all.

I had an experience online with these, I was searching the web for a particular keyword for a very long time, initially, when the search began, it was smooth and with the passage of time I started experiencing some complexities in the research that once was very easy. I discovered to my amazement that the sites provided were totally different from the site I needed and used to receive when that keyword was searched for in the past.

The issue here was that my system was suspected and was then monitored by the spyware software that was secretly installed on the computer I used and was the reason my searches were redirected no matter the search engine I used. This can be very annoying, just the fact that someone is watching you without your knowledge is not acceptable, but there is a way out of this.

Keep Your PC Safe From Virus And Data Loss

Most of the software product enumerated previously can be used to monitor and gain information entered into your computer, it is not safe, since your personal credit data can be accessed by anyone and a crime can be committed, most probably identity theft can be committed, where your credit account information is used to access credit facilities that will be charged into your credit account.

To avoid the misfortunes attached to these software products, you will need to block your computer system from the spyware, spyware and even malware, when this is used, ones system is totally protected from these external factors.

It is also necessary to block the spyware, adware and malware, because your system becomes unnecessarily slow with the spyware on it. To always work at the fastest speed protect your system from spyware and the others.

In Conclusion, the spyware and adware exposes you to a lot of dangers. The adware is an advertisement software that opens the system up for different adverts from the internet, the spyware on the other hand is a software secretly installed that monitors by opening your system up with all your files and operations available to any one. For this very reason, the adware and spyware should be blocked to avoid unsecured access to the information in your computer.

The Solution To Your Spyware And Adware Problem

How much do you know about spyware and adware programs? Did you know that they can cause some serious problems inside your computer? These malicious software are a widespread problem that if not taken care of will only get worse

With the world keeping in touch more often and the world getting smaller all thanks to the Internet, a large number of malicious software programs and applications have made and found their way to individuals' personal computer, doing their damage in an array of ways.

No one is an exception to the threats of spyware and adware programs especially if you are a user who is constantly online. Users, whether or not they are at the computer, are always online if they are using a high speed Internet access.

Since you are always open to this kind of attack by software programs, it is necessary for people to know that the problems you suffer can be happen in more than one way. Should you be surfing the Internet, randomly doing things online, and a window pops up on the desktop, this is likely to be adware hard at work.

Legit Adware

Did you know that Adware programs are actually legitimate programs? These programs are designed to promote certain inventions or perhaps a service online users are liable to use. Some of these "safe" adware advertising products may not do much else other than open a second window for a few seconds. The hassle behind this is you will have to close it to continue with what you were doing.

However, other adware programs go to far in their advertisements and bombard the user continuously with the advertisements. With that being said, it is then converted into more of an annoyance instead of just grabbing your interest for a few seconds at a time.

Keep Your PC Safe From Virus And Data Loss

These programs can be so bad that they will put themselves on things inside your computer so you may find yourself constantly bearing witness to the exasperating and disturbing work they bring.

Even with the annoyance of these adware popups, there are even more dangerous and malicious programs that you may mistakenly download onto your computer.

The spyware programs are problematic in a variety of ways.

- Spyware programs will monitor a user's habits and computer use.
- Keeps an eye on the Internet sites the user frequently visits and what the user does on their own computer.

Whatever information is being monitored, it is being recorded and sent to someone else who has been online that may be engrossed for such data.

Even worse spyware software programs exist. These programs are able to record the keystrokes and send that data back to the spyware creator. The keystrokes that get recorded can include your numerous passwords, e-mail addresses whether it is yours or not and even your credit card number(s).

This spyware program makes it an effortless task for hackers to possess such private personal data that "will" be used at the user's expense.

Other spyware programs will scan the hard drive and attach themselves to files and other spyware software on the computer. It could even install things on its own while changing the user's web browser homepage among many of the malicious things it can do. There is just so many of them.

In order to get rid of these spyware programs, the user should get spyware and adware removers that can delete these troublemakers and keep them from coming back. The applications are very helpful to users bombarded by spyware. These tools help keep private information just that... private.

The Difference Of Adware, Spyware And Anti-Virus

Anyone who uses a computer whether it be for professional use or personal use knows that there is a real threat from spyware, adware and computer viruses. All three are similar in that all of them are complete nuisances for users. Yet, they are different but how?

Spyware Rundown

Did you know that spyware is not designed to intentionally harm a computer? However, what it does is open pathways for someone besides the owner of the computer to communicate with it. Typically spyware will record the types of web sites the owner visits which then get sent to web advertisers which allows them to give you unwanted e-mails and annoying pop-ups.

No wonder spyware is looked upon as such a bad thing, ranked to the top with viruses and Trojan horses. It is actually more intrusive than adware is. Adware does not have the capabilities to like spyware to have their own executable programs that monitor and record keystrokes. It will also scan hard drives and look at the computer's applications that a user would normally use. These include chat programs, cookies and the web browser's settings.

Once spyware has all the information it needs, it will send it back to the spyware creator. This data can be then used for various things including marketing and advertising purposes and even sell the information to other parties.

Adware Overview

Although it is annoying, adware is a legitimate form of freeware. Much similar in spyware's original design for advertising, it comes packaged as a software or program. Once these programs are installed, the adware is also installed. Sometimes though, some adware forms, comes from downloading advertising pieces that go with a particular application. Once it is utilized, so is the adware. No doubt, adware is like spyware in that it tracks and records user information for its program authors.

Computer Infection Signs

So how do you know if you have spyware on your computer? One big sign is pop-ups. If you are visiting a site and a pop-up occurs not related to the site you are visiting, a bulb should flash over your head as a wake up call. More times than not, spyware advertisements will have adult oriented themes to it. Should you notice your computer taking longer to load or its really going slow, then spyware and other components related to it, have made their way in. Make sure to have a spyware remover program that will scan and remove said infected files.

Computer Virus Infections

Many people are quite aware of the danger that proceeds with having virus on their computer. They know the destruction these little buggers can do. They were created for only one purpose in mind - to create mayhem on your computer. Viruses will destroy what they come into contact with and then begin to self-replicate. They will touch as many components of your computer software including the operating system as it can before it is detected.

How To Be Rid of Annoying and Destructive Items

There are plenty of anti-virus software in the market, many of which provide spyware and adware scan and remove utilities. Others centrally focus on locating and then deleting or destroying these two programs. Whether you have an all-in-one anti-virus program or a dedicated scanning program, have them search your computer on a regular basis by setting up a timer so they can do a search, find and destroy. Remember to update your products often.

Also download a firewall protection such as ZoneAlarm to keep out most of these destroyers.

Totally Free Spyware Removal: Tips That You Can Follow

Did you know that spyware, more often times than not, are incorporated as freeware? Did you know these "freewares" can cause serious problems for your computer?

What are freewares? It refers to a series of software programs that can be downloaded at any time for free. Most often, they come grouped together like a package with the buy one, take one promo seen in stores. Start off, by reading the program's user agreement to find out how you can uninstall unwanted malicious programs.

Your browser's security holes on certain websites can allow spyware to filter in. What does this mean exactly? It means that a website can attack your computer through flaws of Internet Explorer and other programs that allow access to the Internet.

What is the best way to handle this? Though, almost never done, people should really look into the website they want to visit. Doing so may avoid those unwanted spyware to be placed onto your computer.

Signs of Unwanted Spyware

So how do you know you have been a victim of spyware especially since it is not easy to recognize and often times, not seen until the effects start taking hold on your computer? Keep a watchful eye out for the following signs.

- Your computer begins to freeze, hang up, or slows down. This is a general sign that spyware software is the culprit in taking up your computer's memory resources.

- Annoying popups tend to be uncontrollable, which come in persistently. Even if you ignore them, they still popup onto your computer screen.

- You find that your set homepage has been changed and not by you. It is usually a website you have never visited and never heard of before. You start to leave and you get sent to, yet, another link.

How To Remove Spyware

So what do you need to do in order to remove malicious spyware. Listed below are some steps to keep havoc happening to your computer.

- **Start by looking at your computer's tasks list.** This section of the computer allows you to see what type of programs are running and taking up valuable resources. It is important to get familiar with this list. Eventually, you will be able to recognize what does and does not constitute spyware. This can be done by pressing the CTRL + ALT + DEL buttons on your keyboard at the same time.

- **Your start up list could take a cleaning.** Some spyware programs will integrate themselves to being when the computer is started up. To clean it... do the following step: run the msconfig. This can be done by typing msconfig in the Run Command window.

- **Look at your computer's Programs listing.** This is where programs that have been installed onto your computer will be listed at. To do this, go to the Control Panel under Start and check the Programs Menu and look at the Add/Remove programs section. Anything that looks oddly unfamiliar, get rid of immediately.

- **As soon as you can, if you haven't got one already, obtain an anti-virus program.** Getting more than one of these can also be done and works wonders. The best program is the program that removes it as well as blocks it completely.

- For those that are caught by Spyware Finder programs but are unable to be deleted need to be deleted manually.

Following these tips will save you from the headache that comes with it and dangers that Spyware poses. Anyone can do this! You don't have to be a computer guru (genius) to figure out to remove the Spyware and protect your computer.

What Is Malware?

The most common things that people recognize for malicious software programs are spyware and adware. While these may be more commonly known, there is another just as vicious. Introducing another "ware" program that is a big culprit of computer viruses by hackers... malware.

What exactly is malware?

The name goes from the combination of "malicious" and "software". How does malware get its name? It actually gets it because it focuses more on intent rather than the software itself. A program cannot be thought of malicious on its own unless it is being used for those purposes. As most people know, a software's purpose is all dependent on the person who created it.

There are three types of malware that people who connect to the Internet need to be concerned about and watching out for. They are:

1. Infectious - This malware type mainly virus and worms in it. These are the more common known malware. When the word virus is used this day in age, most people think immediately computer rather than a physiological virus. Virus and worms will differ in how they operate and distribute themselves.

- How does a virus get spread? Usually by going through floppy drives disks. The virus will replicate and attach itself to a executable file and will run whenever the program is activated or the disk is opened.

- When was the worm introduced? This computer malware was first seen when the Internet was first used. The malware scans many networks for those vulnerable, unprotected systems and then it will copy itself to them. From there, it starts the process all over again, except it uses the new network.

Though the two are distinct in nature, they are often times used to describe one or the other to explain malware.

2. Concealers - This type of malware is designed to "conceal" itself from the user. There are two concealers used. They are:

- Trojan Horse - Today's Trojan horses have various appearances. It can disguise itself as a computer utility and can "encourage" a person to use it to improve computer systems. When the person downloads the program, it then makes way for other malware and software to be "installed" onto the computer.

Creators of viruses use the Trojan horse to cause a widespread virus outbreak. When a computer has a Trojan horse on it, it is subsequent to spread the virus to many other networks.

- Backdoors - This is used to create another way to get into your computer system. Typically used by hackers, it helps them to avoid security systems that people have installed onto their computer. Hackers can then "hijack" a computer to do with what they please.

3. Profit Malware - Some companies use malware to increase their profit margins. How they do this comes in the form of a dialer. What is a dialer and exactly how does it affect your computer? A dialer is the type of malware that will mess with your computer's Internet speed connection by rerouting your existing line through an even more expensive phone line, which then increases the bill you would not have normally paid.

When a person is infected with this malware, it forces them to pay a larger amount of money for a service they have no real need for. Should a person be infected with this malware, they should go flush the wallet in the toilet because this is essentially what you are doing until this malware is removed.

Why Free Spyware Removal Tools Are Offered

Most people in society today are under the impression that there is nothing in life that is free. They believe that everything has a price. That no matter what the deal is, a free something comes with some kind of payment. In some ways, this is not far from the truth.

Why is this? It is because the products available today are offered with little or no financial costs. No payments or cash up front. Yet, there is a catch. They do require something from people in return for the free software. Remember, that life has purpose and even nothing has a purpose. Should a company offer up free software removal tools, there must be something they have in mind to be doing this.

Why would a company offer removal software for free?

- Promotional purposes - Companies will entice customers with free items for a way to boost their profit. Companies think that by offering the free removal tools to the public, it will accomplish two things:

A. *Promote spyware tools* - Companies use a common tactic called beta testing. They will release a new piece of software commercially in order to promote it by releasing a free version of it. Those who enjoy the product are liable to purchase the full version once it has been released.

B. *Promotes another product* - Some companies will entice people to buy their products as they include the spyware removal software as a freebie. Doing this, can and does attract customers to the company. A manufacturer's intention is for the customers to see the virtues in the product. When enough people are enticed to sit up and take notice, the company could then start to charge for it.

- Education purposes - the spyware removal tools are distributed as the purpose to increase a person's knowledge. Whose knowledge? It can be either the manufacturer's or the user's increase in knowledge. How can their knowledge be different?

Keep Your PC Safe From Virus And Data Loss

A. Manufacturer - they release the tools to find out more about the people who would use them. They want to learn more about the kinds of things people look for in a great spyware removal tool. Sometimes, these companies will offer the software in exchange for an user evaluation. By letting the user test it free, manufacturers can always find kinks in the software.

B. Users - By sampling a free spyware removal tools, users can learn many things too. By using the free software, the user can learn just how much spyware was able to get into their computer. Through this, they can learn the importance of the protection by using the free spyware removal software. This will also allow them to be educated in the various ways hackers scam into their computer by installing spyware in their system.

- Spyware Introduction - Some spyware moderators will disguise their software as a software "removal" tool but when people download this "program", they are indeed downloading a spyware program that can do harm and not good. Hackers prey on these people who want to get rid of spyware by making them have more spyware. People become an unwilling victim of these hackers.

People should understand and hopefully this article will teach the reality behind the costs of free spyware removal. Is there anything in life that is free? Maybe, maybe not. But maybe understanding what the companies are offering in the beginning will persuade people to be more aware about getting something for free.

The Spyware Threat

There are many threats to computer users nowadays. Worms, viruses, Trojan horses among many other things. Yet, two threats that are known but not well known are Spyware and Adware. These two programs are thorns in the side of computer users.

Spyware and Adware programs strike at any computer that is online at any time. They become a huge hassle, leaving a big mess behind and damages computers in many ways. For this reason, there are removal tools designed to guard computers from these kinds of threats and then keeping it protected from additional damage.

Often times, people use the words synonymously but there is a line to be drawn when describing a malicious program as adware or spyware.

With adware, this is typically a legit alternative that is accessible by software businesses to users who generally do not want to shell out for a software product... Zonealarm, AVG AntiVirus Software among some of the many others. Adware is capable of being circulated in game or software utility programs as freeware.

In certain cases and some programs, there are those that although freeware still have features that are blocked until you pay for the full version. most freeware allow for all the features to work but user will have to deal with the sponsored ads that can come along with the program.

These ads will run in a smaller part of the software or it comes as a popup ad box. Should you stop using the software, either for a bit or for good, the ads "should" wane.

When you least anticipate it to, some ads will popup even when you are doing vital work on your computer. This is usually when people will get upset becomes it is a pain and a major hassle. No matter how hard you try, there is no way to stop them and keep them from bothering you.

One of the worst parts of this is that fact adware programs will try to overrun your computer with the ads even though you do not want their products. It seems you have lost control of your computer to these ads and may not be able to do the job you need to do on the computer

Keep Your PC Safe From Virus And Data Loss

because of it. This is what makes adware such a nuisance. It is just this reason that a removal tool is necessary.

Spyware is similar to adware only it is typically a separate software program. Functions of the spyware software are no doubt malicious and is done without the user's knowledge. It can wreak all kinds of problems by posing as something the user sees as useful. Once the program is downloaded, it will then find its way through your computer and start its disaster deeds.

Spyware typically watches your online activity, transmitting it to the "end user". Some programs will be forced onto your computer without your consent. Some even go as far as recording the "keystrokes" so the criminals can find out your sensitive data like passwords, e-mail addresses and credit card numbers.

The worst kind of spyware is so malicious it can cause severe damage to a computer's hard drive. They can snoop around the contents, spread into other computers, damage the computer's internal system and even change software or download software.

A computer should always have an effective removal tool for spyware just to get rid of these sneaky, pesky and malicious programs.

ZoneAlarm Internet Security Suite For Antivirus Protection

When the Internet first made its launch, no one really could know the magnitude of viruses that would be created to infect a person's hard drive. Viruses were only one part of the equation. Now there are: Trojans, worms, spyware and adware to add to that list. They are grouped together and singled out as malware software meaning it is malicious software.

According to an article in Computer Economics, financial losses due to malware worldwide were \$14.2 billion in 2005, a decline since 2002. Even though this news is a blessing to computer users, it only means that attacks were covert. They focused on being overt in the beginning. Why does this worry some? Because malware can cause unexpected amounts of damage and with the change could make it harder to find.

To keep malware at a "safe" distance away from a computer system is no doubt a difficult task. There must be a strong security system in place along with an antivirus program to achieve minimal "hacks" in the computer system.

One such protection is from Checkpoint Software Technologies Ltd called ZoneAlarm Internet Security Suite 7.0. This software has proven itself time and again, receiving numerous certifications from independent testers and computer publications. This software has got the most number of recommendations from reviews than any other suite that provides Internet security.

What does ZoneAlarm do?

ZoneAlarm provides the ultimate PC protection as a firewall, antivirus software, spyware, instant messages and home network protection.

The firewall capabilities have full stealth mode features which makes the computer completely invisible to outsiders. It protects both the inbound and outbound information and it stops any suspicious activity before it can do damage.

Keep Your PC Safe From Virus And Data Loss

The antivirus and anti spyware technology can recognize new virus within two hours. The spy spite blocking features will halt any programs from visiting a spyware site. People will be alerted by the identity theft protection when their credit card number appears online.

Layers upon layers of security can block cookies and scripts and clear out the computer's cache. There is also anti - spam and phishing features as well as parental control measures. Norton's Internet Security software puts a load on a computer system. For this reason, ZoneAlarm out beats Norton.

ZoneAlarm's newest version 7.0 adds the following features to its product:

- Antivirus engine with signature updates done on an every hour basis. It has expanded coverage and detects viruses quicker.
- There is an AutoLearn feature, which ZoneAlarm can configure the computer's security system and deals with threats by way the damage that can do.
- There are network and program firewalls with added layers of security.
- Improved firewall for the operating system.
- Protects person's identity by stopping pre approved credit offers and detects thefts by monitoring the person's credit card lists.
- Antispyware improvements lead to harder to find spyware and persistent spyware to be removed.

Even though it has a lot of features, ZoneAlarm is very easy to use and install. It is the best software solution for security and antivirus programs. It can protect a computer form the cyber threat facing users today.

Data Recovery - What Is It?

Data recovery is the process by which information that cannot be accessed normally is retrieved. This includes files that have been deleted or lost in partitioning changes. It also includes recovering data from storage devices that have been damaged, either electronically by corruption or viruses, or mechanically through break down or disaster. There are many techniques for data recovery. The correct one will depend on the reason for the data loss.

Perhaps the most common cause of data loss is through the accidental deletion of files. This is correspondingly the easiest problem to fix. Most deleted files are not actually removed from the hard drive. The space they occupy is simply marked as being able to be written to by new data. Given the size of modern hard drives, it can be a considerable length of time before new data is written to that space. This is how recovery software works. They are able to track down what data is stored in sectors labeled as blank and recover the desired information.

There are numerous types of mechanical failures that can cause physical damage to storage media. Old style floppy disks and CD-ROMs are susceptible to damage – floppy disks through magnetic fields and CD-ROM's by having their metallic substrate scratched off. Hard drives are complicated pieces of machinery with moving parts that operate at speeds like 7200 rpm. Physical damage always causes at least some data loss. Often the logical structures of the file system can be damaged. Before any data can be recovered, the logical structure must be rebuilt.

Unfortunately, most of us are incapable of repairing any physical damage to our hard drives. Thus a number of companies have been formed that specialize in the recovery of data from damaged or destroyed hard drives and other storage devices. A hard drive is a sealed system. If any dust is allowed to settle on the disk surface, it can cause more damage. Clean room facilities are needed to reliably repair damaged drives. A reputable data recovery service will have onsite a Class 100 clean room. They will also have all the specialized tools and experience necessary to recover lost data. It can be surprising the amount of data that can be recovered from a drive that would appear to most of us to be destroyed. There are data recovery companies out there that can salvage disks that have been through fire and the subsequent water damage.

Keep Your PC Safe From Virus And Data Loss

Data recovery is not limited to hard drives. With the proliferation of digital recording equipment, from cameras to PDA's to MP3 players, the use of data recovery techniques on such things as Flash cards is growing. Also, many organizations find that they have important information stored on older technologies like tape drives or zip disks. These forms of media may have been damaged over the years, and most companies probably do not have the skills or equipment to recover data from them. There are data recovery services out there that specialize in this type of work.

Data Recovery - Viruses And Malware

If the specter of fire, floods and just plain computer failure is not enough for you to consider how to protect your data, you should also be aware of the potential for malicious destruction of your data caused by viruses and other malware.

A computer virus is a self-replicating computer program that can copy itself and then transmit these copies to other files, programs or computers. It is called a virus because it behaves similarly to a biological virus. Viruses are one of the several types of malware, or malicious software. Viruses can be destructive in that they can contain overtake the computer system and use up valuable resources. They can also be designed to delete files and affect partition tables.

Other types of malware include worms and Trojan horses. A worm is similar to a virus in its effects. The difference is that a worm is self contained, and does not need another program for propagation. A Trojan horse is a piece on malware that is hidden inside a legitimate program.

Some malware can be very dangerous as they can delete files, or steal personal information and transmit it to the programmer. Malware has the potential of wiping out complete file systems, beyond the reach of data recovery software.

In order to protect your data from viruses and worms you will want to install anti-virus software that can detect and eliminate known viruses. These programs work by examining the contents of the computer's memory and checking for known viruses. Some anti-virus programs will also scan all files as they are downloaded to help ensure that no virus has the chance to enter your computer. You will also want to regularly update your anti-virus software and operating system. Microsoft Windows, because of its dominant position in the market, is often the target of attacks by viruses. Microsoft frequently issues patches and updates to fix any vulnerabilities found by malware.

In addition to anti-virus software, common sense can be a useful tool when combating viruses. So not download anything from the internet from sites that you do not have confidence in. Do not open attachments on emails from people you have never heard of. In fact, it is usually a good idea to avoid opening any unexpected emails, as some viruses can access your colleague's computers and email themselves from their accounts.

Keep Your PC Safe From Virus And Data Loss

And finally, the best way to protect your data from viruses is simply to back it up. A malware attack, like a fire or natural disaster, can occur despite all your precautions. By backing up your data you can recover it in case your originals are lost completely.

Data Recovery - Restoring Deleted Files

So you have accidentally deleted those pictures from your vacation last summer, and the recycle bin has been emptied. Are your files gone for good? They may not be. While Microsoft tries to tell you that emptying the recycling bin permanently deletes your files, the truth is that Windows simply marks the file as deleted, and treats the space that it occupies as free. The data is not actually removed from the drive at this time. Thus until a new file is written onto that space, you have the chance to recover the deleted files.

It is important to differentiate between steps for recovering deleted files and partitions and the steps you need to take if there is physical damage to your drive. If your hard drive has is making strange noises, shaking, rattling or smoking, then there is no software fix that will resolve your problems. You need to turn your computer off immediately, remove the hard drive and call a data recovery service if your files are vital.

Whenever you realize that you have lost data, the first thing to remember is not write anything more to the hard drive. The more data that is written to the hard drive after the accidental deletion of files means that there is a greater probability that the lost data will be gone forever.

The first step is to visit the recycling bin to see if the missing files are there. If that is the case, it is a simple procedure to move the files from the recycling bin to the main portion of your file system. If you were careful with your computer set up, you may have installed a program like Norton SystemWorks to protect yourself from viruses. Programs like this often include automatic backups. You will need to check with the software documentation to see how to recover any files from the backup archive.

If Windows cannot help you find your missing files, you will want to consider using data recovery software. There are many packages out there. Some are shareware, and a couple are even freeware. At this time we will not begin to review the many data recovery software solutions that exist. Suffice it to say that quality data recovery software can retrieve at least part of your missing data with a comparatively high frequency. It will also include utilities for searching for and organize the missing data, so that you do not need to wade through a list of everything that has been deleted from your computer since you purchased it.

Keep Your PC Safe From Virus And Data Loss

A more serious problem results when a partition containing needed files has been deleted. You do not want to attempt to create a new partition. Your data is probably still there. Creating a new partition will wipe it out completely. Data recovery software may be able to recover files lost when a partition was deleted. You can either run the software on another partition, or in the case of a complete hard drive wipeout, you will want to either install another hard drive or remove the problem drive and reinstall it in another computer.

Data Recovery Software

Data recovery software can be used to correct errors in hard drives that result in data loss.

There are many brands of data recovery software on the market today. Some are simple shareware utilities, while others are full commercial products.

It should be noted that you should never attempt to use a data recovery program if you suspect your drive is broken. If there are unusual noises coming from the drive, you will want to take it to a professional to attempt data recovery. The more you use a malfunctioning drive, the more damage you can do to it.

Data recovery software typically uses two main techniques to repair errors to file systems that cause files to be inaccessible. The first is known as consistency checking. Here the program will scan the logical structure of the file system for missing or unexpected results. Examples of utilities that follow this reasoning are the Linux fsck and the Microsoft equivalent chkdsk and scandisk. Fsck refers to file system consistency check, and generally runs when the system is booting up in order to detect errors caused by an incorrect shutdown. Consistency checking does not work if the file system is too badly damaged.

In the case of severe file system damage, another type of data recovery software can be used. These programs ignore the file system structure and attempt to read whatever data they can from the drive. The program then attempts to recreate files using a set of preprogrammed rules. This type of data recovery does not attempt to repair the file system. Instead, it tries to recover any files that it can, and then save them to a functioning drive. The damaged drive can then be either reformatted or replaced, depending on the cause of the damage. This technique is noticeably slower than consistency checking, can recover data even when the logical structures are badly damaged.

If your boot drive has crashed, you may be unable to start up your operating system in order to run your data recovery software. In this case you have a couple of options. You can try booting up your computer from a CD-ROM, you can purchase a new hard drive and install your operating system on it, or you can remove the hard drive and install it in a different, functioning computer. All three options have their advantages and disadvantages.

Keep Your PC Safe From Virus And Data Loss

One thing to consider when selecting data recovery software is whether it has an undo option. You should never perform data recovery on a drive without the ability to undo any changes you are making. If you are unable to retrieve the missing data with this software, you want the ability to try again with another program or to use a professional data recovery service. By following these tips hopefully you will be able to safely recover your missing files, and hopefully next time you will have backed up all your essential data.

Data Recovery In Windows

With Microsoft Windows being, in one incarnation or another, the most dominant operating system on PC's today, data recovery solutions for it have been well developed. There is a myriad of software packages out there that can recover lost files. However, there are quite a few steps that one can take without having to find and install third party software. If the files have simply been deleted, the obvious solution is to visit the Recycling Bin to recover them. However, if there has been a drive failure, more drastic steps must be taken.

More often than not, the cause of the apparent disk failure is due to a corrupt Master Boot Record (MBR) or Partition Table, which often results in a non-booting drive. The most common response to this is to panic and purchase a new drive, or even a new PC in some cases!

With Windows XP, you can check the partitions and file systems by running the Computer Management program. To run this utility, select the My Computer icon, and then right click. From the list of options select manage. This will open the Computer Management window.

On the list on the left side of the window select Disk Management. Windows will display a list of the hard drives and CD or DVD drives on your computer. For each hard drive, Windows will specify the file system and the partition structure, as well as the status of the drive. The file system is how the data and free space are organized so that it the computer can read and write data to the drive. The primary file systems used by windows are FAT-32 and NTFS. FAT stands for File Allocation Table, and FAT-32 refers to the use of 32 bit storage elements. Older versions of Windows, from 95 and earlier, used FAT-16. NTFS, or NT File System, is now the most common Windows file system, as it is the one primarily used by Windows NT and Windows XP. Operating systems can generally use older file systems when necessary, meaning you can install that old hard drive from your Windows 3.11 machine into your new, Windows XP machine in order to recover any data from it.

Both FAT and NTFS use a master boot record, or MBR, and a partition table in their file structure. These are always located in the first sector of the drive. An error in the MBR or partition table will cause Windows to not be able to read any of the files located on that drive.

There are some utilities included in Windows that can sometime fix problems with the partition table. These are scandisk and chkdsk. The former is used on older Windows platforms, while

Keep Your PC Safe From Virus And Data Loss

the latter is used on Windows NT and XP systems. These applications usually run while Windows is booting up in order to detect problems caused by an abrupt shutdown. They can also be run from a floppy disk or your Windows installation CD if your computer is unable to boot up. You should always start with these utilities when trying to repair errors to your file systems.

Data Recovery Services

A data recovery service is a company that specializes in retrieving files and information, especially from computers that have been damaged or destroyed. While data recovery software can be used to recover information that has been deleted or from hard drives that have been corrupted, if there is physical damage to the drive, you will probably need to call a data recovery service. There is most likely physical damage to your drive if there are unusual sounds coming from it, especially clicking, buzzing or scraping noises. Data recovery software will probably not be able to recover information lost to a damaged drive, and may make it harder for a data recovery service.

All hard drives contain both mechanical and electronic parts. The mechanical parts can wear out over time, rendering the drive inoperable. The information is still on the drive, but is inaccessible to you. It takes a professional technician to recover the data. A hard drive cannot be opened in a regular environment, because any dust can damage the surface of the disk. A reputable data recovery service will operate a clean room where they can safely disassemble your drive, free from dust or electrostatic discharge.

Data recovery services are also needed if the drive has been severely damaged by fire or water. The skills needed to coax data from such a drive are beyond those of a typical computer technician. There are techniques for retrieving files in these cases, however, and a data recovery service should be able to help you.

There are many companies out there that offer data recovery services. Just do a Google search for data recovery to find one near you. Different companies will offer different levels of service, with a corresponding difference in price.

When shipping your drive to a data recovery service, you will want to wrap it in an anti-static material. A freezer bag is sufficient if there is nothing better. If you still have the original packaging you should use that, otherwise find a sturdy box about twice as large as the drive. Use foam padding or bubble wrap to protect the drive inside the box. Do not use Styrofoam peanuts as they attract static electricity. If your drive has suffered water damage, it is important that you do not attempt to dry it. The drive needs to be dried under sealed conditions within a clean room. You should include a damp sponge with the package in order to keep the drive from drying out enroute.

Keep Your PC Safe From Virus And Data Loss

When looking for a data recovery service try to find one that can offer some levels of guarantee about their work. Some firms will first try to clone your drive and repair the clone, leaving your damaged drive untouched. It is also nice when the data recovery company will store your data for a period after recovery to ensure that a backup exists until you are confident you have replaced the data on your system.

Data Recovery - Insurance And Disasters

When your business is hit by fire or flood, insurance should be able to handle the monetary costs of resuming operations. However, damage to your computers can result in the loss of critical information that money alone cannot replace. Rebuilding customer files and financial records can be extremely time-consuming, if not down right impossible. If in the unfortunate case that you have not backed up your data in an offsite storage facility, you may still be able to recover your data from damaged or destroyed equipment. Recovery of data from a hard drive can be critical after a fire or flood. Data can be recovered from many drives even if all of the plastic components have melted.

Many drives that have been completely blackened by fire still have intact insides. A data recovery service may be able to rebuild any damaged electronics to read the data stored on the drive. However, if the fire was too intense, and the platters within the head assembly have begun to melt, then there is no chance that a successful data recovery can occur. This will not be known until a data recovery company has the chance to open the drive within a clean room and inspect the damage.

If the hard drive has been submerged for a relatively short period of time, it is possible that the water has not made its way inside the drive. However, if water has penetrated the drive, it is important to act as quickly as possible. The drive should be kept wet, as the process of drying it out, when not done carefully, can cause more damage. This is because the water will probably not be pure, and will leave behind dirt and other minerals that can prohibit data recovery.

Whatever you do, do not attempt to run computer equipment that has been damaged by fire or water without a computer technician checking it out first. Running power to a damaged drive can completely erase any chance in being able to recover the data from it. What you need to do is ship it to a data recovery service in its current condition as quickly as possible. Any delay can decrease the probability that your data can be salvaged.

Make sure you select a data recovery service that has experience dealing with hard drives that have been damaged by fire or water. While some of the techniques for disaster recovery are the same as for other data recovery, the chances of successfully recovering your data are usually less after a disaster. By selecting an inexperienced company to handle your recovery needs, you run the risk of losing data that a more experienced company may have been able to

Keep Your PC Safe From Virus And Data Loss

save. Data recovery is usually a one time shot. If you make a mistake, you do not get a second chance.

Insurance will usually cover the cost of data recovery services in the case of fire or a natural disaster. This is done as data recovery may be the quickest way to get the company up and running normally. And the faster your company is back to normal, the happier everyone, from the insurance company, to your clients, to yourself, will be.

Data Recovery - Evidence Recovery

The use of computers to commit crimes, has given rise to the field of forensic computing. Here experts analyze computers and other forms of digital communications in order to find evidence of a crime. This consists of identifying, preserving, analyzing and presenting digital evidence.

It has been estimated by experts in the legal industry that between 30 and 40 percent of all documents used in the process of litigation were found through forensic investigations of the relevant computers. If you suspect your company's computers have been tampered with or used in the commission of a criminal offense, then you need to protect the integrity of your computer system. Whether the cause is a disgruntled employee who wiped out his computer before leaving or individuals trying to hide evidence of fraud or embezzlement you will want to do as little as possible to those computers until an expert can determine when information is on them.

The first step in forensic computing is to find and recover any evidence that may be useful for law enforcement or for prosecutors. The techniques for evidence recovery are similar to those for data recovery. One difference is that the data may have been deliberately deleted, and criminals with varying degrees of sophistication can be more successful at removing tracing of incriminating evidence.

If you believe that you have a computer that contains electronic evidence of a crime, do not use it any further. Attempting to access the computer in any way may change the data contained in the drive. Continuing to use the computer can overwrite the evidence making it permanently unavailable.

A forensic computing expert is needed to properly analyze a computer and check for evidence on it. An untrained user may accidentally delete important evidence. A trained and certified expert can ensure that the data remains intact, and thus applicable to a court of law.

There are many crimes for which evidence may be found on the computer. Besides the usual white collar crimes of money laundering, embezzlement, fraud and stock manipulation, there can also be email records indicating sexual harassment or threats preceding a violent crime. By mishandling a computer that you suspect to contain evidence of a crime, you could even be found guilty of hindering prosecution.

Keep Your PC Safe From Virus And Data Loss

Besides evidence of criminal offences, there may be evidence of professional misconduct on your office computers. A forensic computer expert can help you determine whether an employee is stealing from the company, or using company resources in an improper manner. They may be able to hide their activities from you, but they will not be able to hide them from a forensic expert.

There are many companies offering computer forensic expertise and evidence recovery. A search on the internet should be able to find one near you.

Data Recovery - The Importance Of Backing Up Data

It is important any computer user to remember to always back up their data. Although technology is continuously improving, hard drives still fail and data is still lost. Hard drives are an amazing piece of mechanical engineering. They operate at high speeds spinning at around 7200 rpm. Although they have been engineered to withstand considerable levels of jarring and vibration, problems can still occur that result in irreparable damage to the drive.

Because of the nature of all storage devices, you should back up any important data you may have. There are many ways you can unintentionally lose information on a computer. A power surge, lightning, fire, equipment failure and malicious or innocent tampering with your computer can all cause data loss.

If you regularly make backup copies of your files and keep them in a separate place, you can easily get at least of your information back in the event something happens to the originals on your computer.

Deciding what to back up is highly personal. Anything you cannot replace easily should be at the top of your list. Before you get started, make a checklist of files to back up. This will help you determine what to back up, and also give you a reference list in the event you need to retrieve a backed-up file.

Things to back up include the following:

- Digital photos
- Personal documents
- School or work projects
- Music collection
- Address book
- Email archive
- Downloaded software

There are many ways to back up your personal computer. The cheapest is often just to purchase a CD or DVD burner and a collection of blank disks. Another way, which can add

Keep Your PC Safe From Virus And Data Loss

another level of security to your data, is to purchase storage space on an offsite server, and update your files there on a regular basis.

You can individually select the files you want to back up each time, or you can use a back up utility. There are several programs out there that are suitable for regularly copying the essential portions of your hard drive. Windows XP includes its own Backup Wizard. It comes preinstalled on Windows XP Professional, but you will have to install it yourself of the Home edition. Once it is installed, you can find it by going to the system tools folder in the start menu.

Backing up your data regularly can prevent the need of a difficult data recovery process in the event of a system failure. When you consider the time and the effort you have spent acquiring or producing the data and programs on your computer, it makes sense to spend just a little bit of time each week ensuring that you do not lose it

Data Recovery - Continuous Backup

With the increasing reliance on computer based systems to manage all aspects of our lives, more emphasis is being placed on the development of backup systems as a necessary tool to promote rapid and reliable data recovery. All computers and systems have the possibility of failure. Planning for that failure can reduce the impact it may have on your business operations.

Traditional backups have usually consisted of tape-based systems that backup data and transactions on a daily basis. For applications that require a higher degree of security, like credit card transactions or systems that process a large amount of data each hour, a daily backup may not be sufficient protection in the case of disaster. Fortunately, continuous backup solutions exist. Here data is automatically copied to a backup system every time a change is made to that data. This is in essence how the Unix file system works by saving multiple versions of the same document. Continuous backup allows the user or a system administrator to restore the data to any point in time.

There are many technologies that are designed for continuous backup. There is considerable effort being done right now to create some sets of standards for continuous backups. The key to continuous backup is the ability to record all data changes as occur, and to time-stamp them. This means that one can reset the file to any point in time, rejecting any changes made after that. Windows XP implements a form of continuous backup with their system restore function. However the idea of full continuous backup is a much more powerful concept.

It is important to differentiate between continuous backup and what is known as taking snapshots. Unlike snapshots, continuous backup does not store complete images of the drive taken at given intervals. It just records the changes made to files. Snapshots generally require far more storage space than a continuous backup solution.

Continuous backups are quite a bit different from traditional backups. Traditional backups can only restore data to the point at which the backup was taken. With continuous backups, there are no schedules. When data is written to disk, it is also written to a second location. This eliminates the need for nightly scheduled backups.

Near continuous backup is a variation of continuous backup where the data is backed up on regular, those discreet, intervals. A typical length of time for a near continuous backup interval

Keep Your PC Safe From Virus And Data Loss

is a couple of minutes. This reduces the demand that a continuous backup system requires, while still providing a high level of data protection against unforeseen occurrences.

It is important to note that some backup systems are called continuous even though they only perform the backup every hour or so. In essence, they are actually a snapshot system, and do not offer the full flexibility of a continuous backup system.

Data Recovery

It seems that all of the work we do these days is stored on computers. For a business, the files that we create can have a real, monetary value. For the individual, their computer may be filled with pictures, correspondence and other personal memories. Occasionally this data can be lost, either through a computer malfunction or the accidental deletion of files. The techniques used to find missing files are known as data recovery.

Data recovery does cover a wide variety of services, depending on the cause of the data loss. Microsoft's Recycle Bin and Apple's Garbage Bin can be thought of as the first step in the recovery of deleted files. For bins that have been emptied, and Linux systems, there are various utilities such as undelete which can retrieve deleted files.

Another reason for data loss occurs when something damages the file system, causing incomplete data to be written to the drive. This can be a result of a power surge or failure, or some types of computer crashes. In this case, the logical structure of the file system is damaged, and must be rebuilt before the files can be accessed.

When data recovery software cannot retrieve the missing files, a data recovery service may be the only solution. These companies specialize in the recovery of data from damaged storage devices.

Data recovery can often be incomplete. It is usually done in an emergency situation. Complete data recovery can often only occur when a back up copy has been made. By storing all of your important data in multiple locations on different storage devices, you can best protect yourself against data loss.

Types Of Data Loss

Perhaps the most common cause of data loss is through the accidental deletion of files. This is correspondingly the easiest problem to fix. Most deleted files are not actually removed from the hard drive. The space they occupy is simply marked as being able to be written to by new data. Given the size of modern hard drives, it can be a considerable length of time before new data is written to that space. This is how recovery software works. They are able to track down what data is stored in sectors labeled as blank and recover the desired information.

There are numerous types of mechanical failures that can cause physical damage to storage media. Old style floppy disks and CD-ROMs are susceptible to damage – floppy disks through magnetic fields and CD-ROM's by having their metallic substrate scratched off. Hard drives are complicated pieces of machinery with moving parts that operate at speeds like 7200 rpm. Physical damage always causes at least some data loss. Often the logical structures of the file system can be damaged. Before any data can be recovered, the logical structure must be rebuilt. Unfortunately, most of us are incapable of repairing any physical damage to our hard drives, and thus must consult with a data recovery service

Data recovery is not limited to hard drives. With the proliferation of digital recording equipment, from cameras to PDA's to MP3 players, the use of data recovery techniques on such things as Flash cards is growing. Also, many organizations find that they have important information stored on older technologies like tape drives or zip disks. These forms of media may have been damaged over the years, and most companies probably do not have the skills or equipment to recover data from them. There are data recovery services out there that specialize in this type of work.

Data Recovery Software

There are many data recovery software packages out there. Some are shareware, and some are even freeware, but the majority of quality programs do have a price attached. Some commercial packages will offer to attempt to recover your data for free, but then you need to purchase the software if it is successful. At this point you need to determine how much your data is worth to you. It makes sense to spend a certain amount of money of data recovery software if it means your business is not disrupted or your precious holiday photos are not lost forever.

Two main techniques are used by data recovery software to retrieve files. These are consistency checking and surface scanning. Consistency checking involves scanning the logical structure of the disk and checking for any errors or missing data. It then tries to repair the logical structure so that the data can be retrieved. Examples of programs that use consistency checking include scandisk and chkdsk for Windows, disk utility for Macs, and fsck for Linux. Surface scanning is slower, but works for drives with more heavily damaged logical structures. Here the software attempts to recreate any data it can find. It uses a system of rules to determine which data is part of which file, and then writes the collected files to a new drive. Surface scanning does not repair a damaged file structure, but it can recover the data that is on it so that the drive can be reformatted.

Before you try running data recovery software, you should make sure that the program will not attempt to do any changes to your drive without being able to undo them. The last thing you need is for your data recovery software to make matters worse by permanently erasing the data you are trying to recover.

Data Recovery Services

When the mechanical portions of your hard drive fail, it is impossible for you to operate the drive in order to recover your data. In this case you may need to contact a professional data recovery service. If you were careful, you would have made backups of your important data. In this case it becomes simple to replace the data on a new drive. If you do not have any backups then you may be in trouble.

A data recovery service is a company that retrieves files from hard drives that have been damaged. While data recovery software can be used to recover information that has been deleted or from hard drives that have been corrupted, if there is physical damage to the drive, you will probably need to call a data recovery service. One way to tell if there is physical damage to your drive is if there are unusual sounds coming from it, especially clicking, buzzing or scraping noises.

For a non-functioning drive, the information may still be on the drive, but just inaccessible to you. A technician may be able to recover the data. There are many companies out there that offer data recovery services.

How such companies usually operate is that you send your drive to them via courier. They will then try to repair the drive in their clean room, which will prevent dust and other contaminants from further damaging your drive. If successful, they will either send the now functioning drive back to you, or in the case of data recovery from a completely inoperable drive, they can send just the data in any form you desire.

When looking online for a data recovery service, you will want to be wary of companies who cannot offer some guarantee about their work. Check to see if company can store your data after recovery, in order to give you a chance to make sure that it is properly and completely installed on your own system.

Data Recovery Services

When the mechanical portions of your hard drive fail, it is impossible for you to operate the drive in order to recover your data. In this case you may need to contact a professional data recovery service. If you were careful, you would have made backups of your important data. In this case it becomes simple to replace the data on a new drive. If you do not have any backups then you may be in trouble.

A data recovery service is a company that retrieves files from hard drives that have been damaged. While data recovery software can be used to recover information that has been deleted or from hard drives that have been corrupted, if there is physical damage to the drive, you will probably need to call a data recovery service. One way to tell if there is physical damage to your drive is if there are unusual sounds coming from it, especially clicking, buzzing or scraping noises.

For a non-functioning drive, the information may still be on the drive, but just inaccessible to you. A technician may be able to recover the data. There are many companies out there that offer data recovery services.

How such companies usually operate is that you send your drive to them via courier. They will then try to repair the drive in their clean room, which will prevent dust and other contaminants from further damaging your drive. If successful, they will either send the now functioning drive back to you, or in the case of data recovery from a completely inoperable drive, they can send just the data in any form you desire.

When looking online for a data recovery service, you will want to be wary of companies who cannot offer some guarantee about their work. Check to see if company can store your data after recovery, in order to give you a chance to make sure that it is properly and completely installed on your own system.

Backing Up Your Data

It is important any computer user to remember to always back up their data. Although technology is continuously improving, hard drives still fail and data is still lost. They operate at high speeds, spinning at around 7200 rpm. There are many things that can happen to a hard drive that can result in irreparable damage.

Because of the nature of all storage devices, it is important to back up any important data you may have. There are many ways you can unintentionally lose information on a computer. A power surge, lightning, fire or equipment failure can all cause data loss.

If you regularly make backup copies of your files and keep them in a separate place, you can easily get at least of your information back in the event something happens to the originals on your computer.

There are several programs that handle regular backups of your hard drive. Windows XP includes its own Backup Wizard. Whatever program you choose, you should be able to set it to copy the essential portions of your hard drive at a set time, usually in the middle of the night when nobody is using the computer.