COMPUTER VIRUS

Terms and Conditions

LEGAL NOTICE

The Publisher has strived to be as accurate and complete as possible in the creation of this report, notwithstanding the fact that he does not warrant or represent at any time that the contents within are accurate due to the rapidly changing nature of the Internet.

While all attempts have been made to verify information provided in this publication, the Publisher assumes no responsibility for errors, omissions, or contrary interpretation of the subject matter herein. Any perceived slights of specific persons, peoples, or organizations are unintentional.

In practical advice books, like anything else in life, there are no guarantees of income made. Readers are cautioned to reply on their own judgment about their individual circumstances to act accordingly.

This book is not intended for use as a source of legal, business, accounting or financial advice. All readers are advised to seek services of competent professionals in legal, business, accounting and finance fields.

You are encouraged to print this book for easy reading.

Table Of Contents

Foreword

As its title seems to imply, a virus is indeed a very damaging element which is certainly capable of causing enough chaos to a system to render it helpless, at least for a time.

Computer Virus

Chapter 1:

What Is A Computer Virus?

Synopsis

A virus will function as an element that will constitute damage to the hard disk contents or interfere with the normal operational executions of the computer system. This will cause the computer to be unable to function properly until the virus is eliminated and the overall system is overhauled and rebooted.

The Basics

A virus program is usually able to replicate itself and this too is an added problem once the virus latches on to a system. Progressively getting out of control, the virus will attempt to cause as much damage as possible before it can be detected and eliminated. The replication is usually intentional and designed to act just like a Trojan, thus causing the unsuspecting user being caught off guard. If a file that contains a virus is opened, or copied onto another computer, then the other computer will also become infected and this process is repeated every time the file is opened and downloaded onto other systems.

A virus can easily be introduced into a computer system along with any software program and this is bad news for the users of FTP otherwise referred to as file transfer protocol. The viruses can also become a problem when there is referencing done and email attachments are being used. When the virus enters the computer system, it can attach itself to, or even replace an existing program. This of course is not good for the user, who will ultimately open the attachment or file and cause the virus to be activated.

Chapter 2:

How Are Viruses Spread?

Synopsis

Having a virus unleash itself within a computer system can be a nightmare for the user, as this is most often done unintentionally but with no less detrimental effects. There is no real way to detect how a virus really attacks and spreads but a lot of effort is put into how to ensure the damage done is as minimal as possible.

How They Get Around

The following are some of the more frequent ways that viruses can spread form computer system to another effectively until detection is almost too late to save the infected material:

- Email attachments are by far the most popular way that viruses find their way into the user's computer system. When the Microsoft's Outlook Express automatically opens attachments to emails received, the virus in automatically unleashed on the system. However, most users now tend to avoid opening attachments they are unfamiliar with and instead resort to immediately deleting them to ensure the virus does not gain access into the system.

- Rogue websites are another problem area for unleashing viruses. Sometimes the virus is introduced into the system by simply visiting websites without knowing the possibility of the virus being embedded in the site's content. Thus when the site is downloaded, so will be the virus too.

- Networks are also another popular way the virus is able to gain some momentum, as any user on the same server opening a site where there is a virus will unleash the virus onto other user's systems too. It usually takes only one party to accidently open an infected site and all the other users on the network will be exposed to the virus infecting their systems too.

- Infected disks are sometimes the cause of the virus spreading, as the user of the infected disk is the source of the hard drive being infected and thus corrupting all the material on the hard drive itself.

Chapter 3:

How Bad Can A Virus Attack Be?

Synopsis

A viruses in itself, is a very damaging program and when unleashed on a computer system, the damage can be quite devastating to say the least. Even in the mildest form, viruses can and usually do, cause a lot of damage to the user's system.

Viruses Are Serious

It would seem that the virus is able to show the vulnerability of the user and the tools being used, while at the same time these viruses are able to display just how innovative the inventor can be if there is a need to inflict online damage, without any actual physical intervention. Phenomenal numbers have been documented within the very small window of time that it takes to cause devastating damage to a computer system. Some of the damage done will not be able to be rectified, thus causing the user to lose all the data permanently. Applications can also be lost but usually it is fairly simple to download again but this is not so possible when it comes to data lost.

Viruses are usually designed to represent a small piece of software that latches onto existing programs until it is activated and then launches into damage mode. An example of such would be the almost unavoidable use of spreadsheet software, as this particular application is bound to be open often thus making it an ideal place to attach the virus to.

Email viruses are also another area where there are usually devastating results from the invasion of a virus. This is especially so if the user tends to open attachments without proper care or scrutiny.

Trojan horses are also another simple computer programs that claim to perform with one objective, but usually comes with the intention of infecting the user's system with a virus.

Chapter 4:

What Is A Malware?

Synopsis

Having to deal with the possible onslaught of viruses attacking a computer is already quite a challenge and when malware is added to the equation, the frustration builds. Malware is a huge threat to the computer system being used as its damaging capabilities are quite extensive.

All About Malware

Basically, any malware presence within a system will cause the user's browser to be hijacked, the search attempts to be redirected, while having to contend with unnecessary pop up adds and also the sites you visit tracked.

In most cases the malware is able to reactivate itself into the system, even though the user is thought to have eradiated its presence. This is mainly because the malware is able to embed itself deep into programs and is rather difficult to detect until it surfaces in the form of trouble for the user. However, it is possible to follow a variety of basic preventive measures to help remove the malware through a series of spyware removals. Other viruses, which are sometime categorized within the malware platform would include worms, Trojans and everything that generally attacks the software of the user.

The invasion by malware can take on several different forms, and these are usually hard to detect in the initial stages until considerable damage is done. Malware often comes hidden within other programs such as Kazaa, iMesh and other file sharing programs. The popular contribution of the malware would be to provide revenue for the pop up ads where income is generated when the user opens these. Others would include websites being presented under the disguise of being full of informative content, thus encouraging the user to open such files.

Chapter 5:

Getting The Right Anti-Virus For Pc

Synopsis

Having a good and reliable antivirus program is very important to maintaining the integrity of the user's system at all times. With a suitable antivirus program in place, the user is less likely, or at least in a position to minimize the possibility of having to deal with negatives such as malware.

Choosing The Right Protection

As there are a lot of different antivirus programs available in the market today, the user may find it confusing and overwhelming when it comes to trying to choose one suited to his or her needs. However, based on the following points, the user should be able to be make a fairly informed decision on what would be best for the needs of the moment.

Effectiveness of the antivirus programs should be considered as there are programs that will deal with only certain aspects or types of viruses and not be able to handle others. This is ok if the use of the online download is limited and the user is not in the habit of surfing for anything and everything. The user should ideally get as much information as possible on the antivirus intended for purchase and only then should the choice be made according to its suitability.

Choosing an antivirus program that is easy and simple to use is also something that needs consideration. If the program is difficult to install, it would be rather frustrating indeed to actually get it to perform at its optimal capacity. The programs should be either self-explanatory or at the very least simple, even for the most simple minded user.

The virus definitions and the engine updates should also be another consideration, as these will eventually effect the integrity of the programs it is meant to monitor.

Chapter 6:

Removing The Computer Virus Automatically

Synopsis

Having to deal with virus invasions is part of everyday computer system usage. It is almost impossible to eradicate the problem completely but the good news is, this it is certainly controllable.

Get Rid Of That Bug

The user will have to explore all the various antivirus applications available to identify one that is most suitable for the current needs when going online. This exercise is very important as it will give the user a fighting chance of ensuring damage, if any, is considerably minimal.

Removing viruses does not necessarily mean that the user will have to erase all the material on the system and start all over again, as in most cases the virus can be dealt with, without having to resort to such drastic measures. Therefore, the user will first have to identify the particular virus in question and then go about finding the suitable counter active antivirus program that can be used to tackle the unpleasant task of eradicating the virus and stopping it from causing further damage. However, it should be noted that in almost all cases, some percentage of data is usually lost.

Perhaps the first step will be to identify the kinds of work and online activities the user intends to participate in. If this is found to be fairly consistent in choice, then at the very onset of use, the individual can have some suitable antivirus programs installed into the system to detect, control or minimize any invasion that manages to pass through the antivirus programs in place. These programs will run automatically whenever the system is activated and are perhaps a very good form of preventive measures that can be taken.

Chapter 7:

Deleting The Computer Virus Manually

Synopsis

Though rather difficult in some cases, it is not altogether impossible to find ways to counter act the negativity of a virus invasion. There are several ways that can be easily adopted to help in manually deleting viruses.

Do It Yourself

Identifying and understanding the particular virus that has taken root in the user's computer system will help the user to take further measures to deal with the virus before it goes out of control and the damage done becomes uncontrollable. For those who are pressed for time or are simply not capable of tackling this task themselves, the alternative of sending it to the nearest service center usually presents an ideal option. However, it is possible to deal with the virus problem manually by following a few steps provided within the system.

The first step would have to be backing up the data on a hard drive dock. This is by far the safest method of backing up files and is comparatively better than the more traditional method of backing up files on an external hard drive which does have a higher chance of the viruses copying themselves onto the external tool. For those who don't possess a hard drive dock, uploading the files to a cloud based storage system such as Dropbox should be considered.

Once the data has been backed up, the process of running virus scans cannot be launched. Booting the computer into a safe mode would be the first step to commence which would involve the use of the F key where the most common is F8. A Google search will inform the user on the best key option suitable for the particular system in place. The selection should include the safe mode with networking as the exercise will involve both online and software scans.

Chapter 8:

Enhance Security With A firewall

Synopsis

Having a system in place does not necessarily mean all the possibilities of a virus invasion is taken care of effectively and consistently. It simply means for that particular period the chances of a virus invasion is minimized but over time this will not be as effective as when it was first installed. Therefore it is important to ensure the firewall administration is constantly searching for ways to improve and guard against any onslaught of a potential virus invasion.

Protect Yourself!

The firewall administration would ideally increase the firewall performance and remove network security threats. There will be the need to keep the firewall properly configured and operating at peak to ensure efficiency as there is always the presence of viruses to challenge the network administrators, thus with the right kind of firewall, it is possible to rid any clutter and improve the performance levels of the application. Popularly known as the first and continual line of defense for any online usage, it is capable of handling vast amounts of traffic across the networks. The firewalls act as filters to a phenomenal amount of packets daily, where an equally phenomenal amount of rules and objects are scrutinized and passed for use.

Since most usage of the online platform is in need of dynamic action plans, the firewall policies are constantly undergoing changes and modifications to accommodate any newer designs of viruses. This will ensure the continuous flux will help to increase the firewall configuration to grow equally dramatically over time. This often huge and subsequently complex situation will cause the firewall configuration to become hard to manage and may require some lengthy research in order to add or change any particular existing condition. Care must be given to this particular aspect of the overall firewall platform as the complexity could apparently decrease the firewall's performance and this could lead to potential security breaches.

Chapter 9:

Tips For Protecting Your Computer From Viruses

Synopsis

In order to use the computer system without having to constantly contend with glitches cause predominantly by viruses, the user will have to ensure adequate measures are taken to protect the computer system from possible virus invasion.

Helpful Hints

The following are some practical and easy ways to help the user keep the treat of viruses at bay:

- The simple and most effective way to keep the possibility of a virus invasion from taking root within the software would be to be constantly updating the software in use. This would include the Operating System where regular check for updates and set up automation updates are practiced.

- Using higher quality antivirus software for reputable manufactures is also something to be encouraged. Taking the time to check the manufacturer's recommendations for information such as set up guides and configurations is important. A complicated style would not be helpful to the user and instead probably cause a lot of frustration when trying to install the application.

- The user should ideally avoid any sites that are questionable in nature, especially those that offer commercial software downloads for free. There are usually hidden agendas and the software are mostly below the performance levels expected, when it comes to thoroughly addressing the virus eradication or blocking exercise.

- The most popular recommendation would be to never open emails from unknown sources. Most would advise simply deleting the email if in doubt, as it would not be worth the effort of eradication, if it does contain viruses.

- The user should be aware of anything that appears either too good to be true or simply seems to be free. It is a common thought process to note that nothing is free, thus online elements should be no different.

Chapter 10:

How To Identify A Dangerous Website

Synopsis

Being weary of opening just any site would be a good practice to incorporate into the browsing exercise whenever one is participating in online activities. However, curiosity tends to get the best of the individual and the attraction to indulge in opening the site becomes just too much to resist. In the event of this predicament unfolding, the individual should first take some precautionary measures to ensure the action does not become regrettable.

What To Look Out For

The following are some preventive measure that can be applied to help limit the possibility of a virus infection from opening an unsuspectingly dangerous site:

- Before actually viewing a link, the user should first conduct an analysis on the site and this is done by right clicking on the site and selecting the option to “copy link address”. If the link appears to have a shortened URL, then this would be unshortened before the testing is done. This can be done by simply pasting the shortened URL to the site and this action will provide the user with the actual whole URL link thus enabling the complete URL to be keyed in for testing.

- Using URL Void is also another option as this will allow the system to run a check on the site against the databases of many reputable engines and domain blacklists. However even this is not a full proof deterrent as there are some sites that contain viruses but have not been detected thus the certification given is positive based on the no adverse reports filed or documented by users.

- Using the Comodo Site Inspector is also another recommendation as this is able to provide effective identifying exploits and also queries from a huge list of sites already known and noted to be dangerous. Although this method does take a little longer than the user may be comfortable with, it is certainly worth the wait.

Wrapping Up

It is very important to ensure that your computer is protected while using it. This is especially true if you have important documents stored on it. SO take some time to implement some of the above strategies and keep your PC protected.