COMPUTER PROTECTION
ESSENTIALS

JEFF LONG

Computer Protection Essentials

by Jeff Long

ABOUT THE AUTHOR

Jeff Long owns WizzDom PC Computer Repair which offers low rates, experienced staff and convenient same-day service. WizzDom PC Computer Repair is the fastest growing in-home computer repair and small business IT service providers at http://wizzdompc.com

Jeff Long does high-quality low-priced cell phone repair, computer repair, and website design at http://Wizzdompc.com

Jeff Long specializes in high quality web design at a low cost and top-notch SEO services and graphic design at http://97webdesign.com

Jada IT
https://jadait.com/

RichardTong
https://richardtong.com.au/

SURPRISE GIFT!
Click the Gift Box to Open...

Legal Notices

This book is supplied for information purposes only and the content inside does not constitute professional advice. It is sold with the understanding that the authors/publishers/resellers are not engaged in giving any accounting, legal or any other professional advice. If legal/accounting or any other professional assistance is required, the services of a professional should be used.

The authors and publishers of this book have used every effort to ensure that it has been prepared in the best possible way – however the authors & publisher make no representation or warranties with respect to the accuracy, applicability or completeness of this book's contents. They disclaim any warranties, accountabilities or fitness for any particular purpose. The authors/publishers/resellers do not accept any responsibility for any liabilities resulting from the decisions made by the readers of this book.

All Legal Terms at http://Member.ws/legal/ also apply.

Editors:
Jennifer Dawson
Lori Chambers
Ashley Miller
Amanda Wells
Jimmy Wilson

Cover Design:
Jake Radaza

Publishers:
Jennifer Dawson
Jimmy Wilson

Consultant:
Ian del Carmen

Please register your copy of this book at
http://iBookWholesaler.com/register/

Click Here for Related Information

https://jadait.com/

https://richardtong.com.au/

Protecting Your Computer's System

Today, more and more people are using their computers for everything from communication to online banking and investing to shopping.

As we do these things on a more regular basis, we open ourselves up to potential hackers, attackers and crackers. While some may be looking to *phish* your personal information and identity for resale, others simply just want to use your computer as a platform from which to attack other unknowing targets.

Below are a few easy, cost-effective steps you can take to make your computer more secure to begin with:

1.   Always make backups of important information and store in a safe place separate from your computer.

2.   Update and patch your operating system, web browser and software frequently. If you have a Windows operating system, start by going to www.windowsupdate.microsoft.com and running the update wizard. This program will help you find the latest patches for your Windows computer. Also go to www.officeupdate.microsoft.com and locate possible patches for your Office programs.

3.   Install a firewall. Without a good firewall, viruses, worms, Trojans, malware and adware can all easily access your computer

Jada IT
https://jadait.com/

RT Richard Tong
https://richardtong.com.au/

from the Internet. Consideration should be given to the benefits and differences between hardware and software based firewall programs.

4. Review your browser and email settings for optimum security. Why should you do this? Active-X and JavaScript are often used by hackers to plant malicious programs into your computers. While cookies are relatively harmless in terms of security concerns, they do still track your movements on the Internet to build a profile of you. At a minimum set your security setting for the "Internet zone" to High, and your "trusted sites zone" to Medium Low.

5. Install anti-virus software and set for automatic updates so that you receive the most current versions.

6. Do not open unknown email attachments. It is simply not enough that you may recognize the address from which it originates because many viruses can spread from a familiar address.

7. Do not run programs from unknown origins. Also, do not send these types of programs to friends and coworkers because they contain funny or amusing stories or jokes. They may contain a Trojans horse waiting to infect a computer.

8. Disable hidden filename extensions. By default, the Windows operating system is set to "hide file extensions for known file types". Disable this option so that file extensions display in Windows. Some file extensions will, by default, continue to

remain hidden, but you are more likely to see any unusual file extensions that do not belong.

9. Turn off your computer and disconnect from the network when not using the computer. A hacker cannot attack your computer when you are disconnected from the network or the computer is off.

10. Consider making a boot disk on a floppy disk in case your computer is damaged or compromised by a malicious program. Obviously, you need to take this step before you experience a hostile breach of your system.

Fighting Spam

How prevalent is Spam? According to Scott McAdams, OMA Public Affairs and Communications Department (www.oma.org):

> *"Studies show unsolicited or "junk" e-mail, known as spam, accounts for roughly half of all e-mail messages received. Although once regarded as little more than a nuisance, the prevalence of spam has increased to the point where many users have begun to express a general lack of confidence in the effectiveness of e-mail transmissions, and increased concern over the spread of computer viruses via unsolicited messages."*

In 2003, President Bush signed the "Can Spam" bill, in December of 2003 which is the first national standards around bulk unsolicited commercial e-mail. The bill, approved by the Senate by a vote of 97 to 0, prohibits senders of unsolicited commercial e-mail from using false return addresses to disguise their identity (spoofing) and the use of dictionaries to generate such mailers.

In addition, it prohibits the use of misleading subject lines and requires that emails include and opt-out mechanism. The legislation also prohibits senders from harvesting addresses off Web sites.

Violations constitute a misdemeanor crime subject to up to one year in jail.

One major point that needs to be discussed about this: *spam is now coming from other countries in ever-greater numbers*. These emails are

Click Here for Related Information

harder to fight, because they come from outside our country's laws and regulations. Because the Internet opens borders and thinks globally, these laws are fine and good, but do not stop the problem.

So what do you do about this?

Here are the top 5 rules to do to protect from spam:

Number 1: Do what you can to avoid having your email address out on the net.

> There are products called "*spam spiders*" that search the Internet for email addresses to send email to. If you are interested, do a search on "*spam spider*" and you will be amazed at what you get back. Interestingly, there is a site, WebPoison.org, which is an open source project geared to fight Internet "*spambots*" and "*spam spiders*", by giving them bogus HTML web pages, which contain bogus email addresses.

> A couple suggestions for you:

> A) Use form emails, which can hide addresses or also
> B) Use addresses like sales@company.com instead of your full address to help battle the problem.
> C) There are also programs that encode your email, like jsGuard, which encodes your email address on web pages so that while spam spiders find it difficult or impossible to read your email address.

Number 2: Get a spam blocking software.

> There are many programs out there for this. (Go to www.cloudmark.com or www.mailwasher.net for example). You may also buy a professional version. Whatever you do, get the software. It will save you time. The software is not foolproof, but they really do help. You usually have to do some manual set up to block certain types of email.

Number 3: Use the multiple email address approach.

> There are a lot of free email addresses to be had. If you must subscribe to newsletters, then have a "back-up" email address. It would be like giving your sell phone number to your best friends and the business number to everyone else.

Number 4: Attachments from people you don't know are BAD, BAD, BAD.

> A common problem with spam is that they have attachments and attachments can have viruses. Corporations often have filters that don't let such things pass to you. Personal email is far more "open country" for spamers. General rule of thumb: if you do not know who is sending you something, DO NOT OPEN THE ATTACHMENT. Secondly, look for services that offer filtering. Firewall vendors offer this type of service as well.

Number 5: Email services now have "bulk-mail" baskets.

If what you use currently does not support this, think about moving to a new vender. The concept is simple. If you know someone, they can send you emails. If you don't know them, put them in the bulk email pile and then "choose" to allow them into your circle. Spam Blocking software has this concept as well, but having extra layers seems critical these days, so it is worth looking into.

Spyware & Adware

Spyware and Adware are not only an ever-increasing nuisance for computer users everywhere, but also a booming industry.

According to Webroot Software, Inc., the distribution of online advertisements through spyware and adware has become a whopping $2 billion industry.

The aggressive advertising and spying tactics demonstrated by some of these programs, require an equally aggressive response from a seasoned eradicator. Sunbelt Software is such a company. A leader in Anti-Spyware, Anti-Spam, Network Security and System Management tools, they gave consistently remained on the cutting-edge of anti-spyware programming since 1994.

So you might be asking:

"Why do I feel as if somebody's watching me?"

According to the National Cyber Security Alliance, spyware infects more than 90% of all PCs today. These unobtrusive, malicious programs are designed to silently bypass firewalls and anti-virus software without the user's knowledge.

Once embedded in a computer, it can wreak havoc on the system's performance while gathering your personal information. Fortunately, unlike viruses and worms, spyware programs do not usually self-replicate.

Where Does It Come From?

Typically, spyware originates in three ways. The first and most common way is when the user installs it. In this scenario, spyware is embedded,

attached, or bundled with a freeware or shareware program without the user's knowledge. The user downloads the program to their computer.

Once downloaded, the spyware program goes to work collecting data for the spyware author's personal use or to sell to a third-party. Beware of many P2P file-sharing programs. They are notorious for downloads that posses spyware programs.
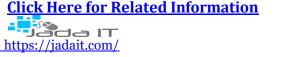
The user of a downloadable program should pay extra attention to the accompanying licensing agreement. Often the software publisher will warn the user that a spyware program will be installed along with the requested program.

Unfortunately, we do not always take the time to read the fine print.

Some agreements may provide special "opt-out" boxes that the user can click to stop the spyware from being included in the download. Be sure to review the document before signing off on the download.

Another way that spyware can access your computer is by tricking you into manipulating the security features designed to prevent any unwanted installations. The Internet Explorer Web browser was designed not to allow websites to start any unwanted downloads. That is why the user has to initiate a download by clicking on a link. These links can prove deceptive.

For example: a pop-up modeled after a standard Windows dialog box, may appear on your screen. The message may ask you if you would like to optimize your Internet access. It provides yes or no answer buttons, but, no matter which button you push, a download containing the spyware

program will commence. Newer versions of Internet Explorer are now making this spyware pathway a little more difficult.

Finally, some spyware applications infect a system by attacking security holes in the Web browser or other software. When the user navigates a webpage controlled by a spyware author, the page contains code designed to attack the browser, and force the installation of the spyware program.

What Can Spyware Programs Do?

Spyware programs can accomplish a multitude of malicious tasks. Some of their deeds are simply annoying for the user; others can become downright aggressive in nature.

Spyware can:

- ⇒ Monitor your keystrokes for reporting purposes.
- ⇒ Scan files located on your hard drive.
- ⇒ Snoop through applications on our desktop.
- ⇒ Install other spyware programs into your computer.
- ⇒ Read your cookies.
- ⇒ Steal credit card numbers, passwords, and other personal information.
- ⇒ Change the default settings on your home page web browser.
- ⇒ Mutate into a second generation of spyware thus making it more difficult to eradicate.
- ⇒ Cause your computer to run slower.

Click Here for Related Information

https://jadait.com/

https://richardtong.com.au/

⇒ Deliver annoying pop up advertisements.

⇒ Add advertising links to web pages for which the author does not get paid. Instead, payment is directed to the spyware programmer that changed the original affiliate's settings.

⇒ Provide the user with no uninstall option and places itself in unexpected or hidden places within your computer making it difficult to remove.

Examples of Spyware

Here are a few examples of commonly seen spyware programs:

(Please note that while researchers will often give names to spyware programs, they may not match the names the spyware-writers use.)

CoolWebSearch, a group of programs, that install through "holes" found in Internet Explorer. These programs direct traffic to advertisements on Web sites including *coolwebsearch.com*. This spyware nuisance displays pop-up ads, rewrites search engine results, and alters the computer host file to direct the Domain Name System (DNS) to lookup preselected sites.

Internet Optimizer (a/k/a DyFuCa), likes to redirect Internet Explorer error pages to advertisements. When the user follows the broken link or enters an erroneous URL, a page of advertisements pop up.

180 Solutions reports extensive information to advertisers about the Web sites which you visit. It also alters HTTP requests for affiliate advertisements linked from a Web site. Therefore the 180 Solutions Company makes an unearned profit off of the click through advertisements they've altered.

HuntBar (a/k/a WinTools) or Adware.Websearch, is distributed by Traffic Syndicate and is installed by ActiveX drive-by downloading at affiliate websites or by advertisements displayed by other spyware programs. It's a prime example of how spyware can install more spyware. These programs will add toolbars to Internet Explorer, track Web browsing behavior, and display advertisements.

How Can I Prevent or Combat Spyware?

There are a couple things you can do to prevent spyware from infecting your computer system. First, invest in a reliable commercial anti-spyware program. There are several currently on the market including stand alone

Click Here for Related Information

software packages such as Lavasoft's Ad-Aware or Windows Antispyware. Other options provide the anti-spyware software as part of an anti-virus package.

This type of option is offered by companies such as Sophos, Symantec, and McAfee. Anti-spyware programs can combat spyware by providing real-time protection, scanning, and removal of any found spyware software. As with most programs, update your anti virus software frequently.

As discussed, the Internet Explorer (IE) is often a contributor to the spyware problem because spyware programs like to attach themselves to its functionality. Spyware enjoys penetrating the IE's weaknesses.

Because of this, many users have switched to non-IE browsers. However, if you prefer to stick with Internet Explorer, be sure to update the security patches regularly, and only download programs from reputable sources. This will help reduce your chances of a spyware infiltration.

.

And, When All Else Fails?

Noticed I said "when" and not "if"? As spyware is growing in destruction and it covers easily more than 90% of the computers (that's you and me, 9 in 10!), the only solution you may have is backing up your data, and performing a complete reinstall of the operating system!

Click Here for Related Information

Phishing & Identity Theft

Who hasn't received an email directing them to visit a familiar website where they are being asked to update their personal information? The website needs you to verify or update your passwords, credit card numbers, social security number, or even your bank account number. You recognize the business name as one that you've conducted business with in the past.

So, you click on the convenient "take me there" link and proceed to provide all the information they have requested. Unfortunately, you find out much later that the website is bogus. It was created with the sole intent to steal your personal information.

You, my friend, have just been "phished".

Phishing (pronounced as "*fishing*") is defined as the act of sending an email to a recipient falsely claiming to have an established, legitimate business. The intent of the phisher is to scam the recipient into surrendering their private information, and ultimately steal your identity.

It is not at easy as you think to spot an email phishing for information. At first glance, the email may look like it is from a legitimate company. The "From" field of the e-mail may have the .com address of the company mentioned in the e-mail. The clickable link even appears to take you to the

company's website, when in fact, it is a fake website built to replicate the legitimate site.

Many of these people are professional criminals. They have spent a lot of time in creating emails that look authentic. Users need to review all emails requesting personal information carefully. When reviewing your email remember that the "From Field" can be easily changed by the sender. While it may look like it is coming from a .com you do business with, looks can be deceiving.

Also keep in mind that the phisher will go all out in trying to make their email look as legitimate as possible. They will even copy logos or images from the official site to use in their emails. Finally, they like to include a clickable link that the recipient can follow to conveniently update their information.

A great way to check the legitimacy of the link is to point at the link with your mouse. Then, look in the bottom left hand screen of your computer. The actual website address to which you are being directed will show up for you to view. It is a very quick and easy way to check if you are being directed to a legitimate site.

Follow the golden rule: never, ever, click the links within the text of the e-mail, and always delete the e-mail immediately. Once you have deleted the e-mail, empty the trash box in your e-mail accounts as well. If you are truly concerned that you are missing an important notice regarding one of your accounts, then type the full URL address of the website into your browser. At least then you can be confident that you are, in fact, being directed to the true and legitimate website.

Click Here for Related Information

The Advancement of the Keyloggers

A keylogger is a program that runs in your computer's background secretly recording all your keystrokes. Once your keystrokes are logged, they are hidden away for later retrieval by the attacker. The attacker then carefully reviews the information in hopes of finding passwords or other information that would prove useful to them.

For example, a keylogger can easily obtain confidential emails and reveal them to any interested outside party willing to pay for the information.

Keyloggers can be either software or hardware based.

Software-based keyloggers are easy to distribute and infect, but at the same time are more easily detectable.

Hardware-based keyloggers are more complex and harder to detect. For all that you know, your keyboard could have a keylogger chip attached and anything being typed is recorded into a flash memory sitting inside your keyboard. Keyloggers have become one of the most powerful applications used for gathering information in a world where encrypted traffic is becoming more and more common.

As keyloggers become more advanced, the ability to detect them becomes more difficult. They can violate a user's privacy for months, or even years, without being noticed. During that time frame, a keylogger can collect a lot of information about the user it is monitoring. A keylogger can potential

Click Here for Related Information

obtain not only passwords and log-in names, but credit [card](#) numbers, bank account details, contacts, interests, web browsing habits, and much more. All this collected information can be used to steal user's personal [documents](#), [money](#), or even their identity.

A keylogger might be as simple as an *.exe and a .dll* that is placed in a computer and activated upon boot up via an entry in the registry. Or, the more sophisticated keyloggers, such as the Perfect Keylogger or ProBot Activity Monitor have developed a full line of nasty abilities including:

⇒ Undetectable in the process list and invisible in operation

⇒ A kernel keylogger driver that captures keystrokes even when the user is logged off

⇒ A remote deployment wizard

⇒ The ability to create text snapshots of active applications

⇒ The ability to capture http post [data](#) (including log-ins/passwords)

⇒ The ability to timestamp record workstation usage

⇒ HTML and text log file export

⇒ Automatic e-mail log file delivery

All keyloggers are NOT used for illegal purposes. A variety of other uses have surfaced. Keyloggers have been used to monitor web sites visited as a means of parental control over [children](#). They have been actively used to prevent child pornography and avoid children coming in contact with dangerous elements on the web.

What are Intrusion Detection Systems?

Intrusion Detection System (IDS) are a necessary part of any strategy for enterprise security. What are Intrusion Detection systems? CERIAS, The Center for Education and Research in Information Assurance and Security, defines it this way:

"The purpose of an intrusion detection system (or IDS) is to detect unauthorized access or misuse of a computer system. Intrusion detection systems are kind of like burglar alarms for computers. They sound alarms and sometimes even take corrective action when an intruder or abuser is detected.

Many different intrusion detection systems have been developed but the detection schemes generally fall into one of two categories, anomaly detection or misuse detection.

Anomaly detectors look for behavior that deviates from normal system use. Misuse detectors look for behavior that matches a known attack scenario. A great deal of time and effort has been invested in intrusion detection, and this list provides links to many sites that discuss some of these efforts"

(http://www.cerias.purdue.edu/about/history/coast_resources/intrusion_detection/)

There is a sub-category of intrusion detection systems called network intrusion detection systems (NIDS). These systems monitors packets on the network wire and looks for suspicious activity. Network intrusion

Click Here for Related Information

detection systems can monitor many computers at a time over a network, while other intrusion detection systems may monitor only one.

Who is Breaking Into Your System?

One common misconception of software hackers is that it is usually people outside your network who break into your systems and cause mayhem. The reality, especially for corporate workers, is that insiders can and usually do cause the majority of security breaches. Insiders often impersonate people with more privileges then themselves to gain access to sensitive information.

How Do Intruders Break into Your System?

The simplest and easiest way to break in is to let someone have physical access to a system. Despite the best of efforts, it is often impossible to stop someone once they have physical access to a machine.

Also, if someone has an account on a system already, at a low permission level, another way to break in is to use tricks of the trade to be granted higher-level privileges through holes in your system. Finally, there are many ways to gain access to systems even if one is working remotely. Remote intrusion techniques have become harder and more complex to fight.

How Does One Stop Intrusions?

There are several Freeware/shareware Intrusion Detection Systems as well as commercial intrusion detection systems.

Open Source Intrusion Detection Systems

Below are a few of the open source intrusion detection systems:

- AIDE (http://sourceforge.net/projects/aide) - Self-described as "AIDE (Advanced Intrusion Detection Environment) is a free replacement for Tripwire. It does the same things as the semi-free Tripwire and more. There are other free replacements available so why build a new one? All the other replacements do not achieve the level of Tripwire. And I wanted a program that would exceed the limitations of Tripwire."

- File System Saint (http://sourceforge.net/projects/fss) - Self-described as, "File System Saint is a lightweight host-based intrusion detection system with primary focus on speed and ease of use."

- Snort (www.snort.org) - Self-described as "Snort® is an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines the benefits of signature, protocol and anomaly based inspection methods. With millions of downloads to date, Snort is the most widely deployed intrusion detection and

Click Here for Related Information

https://jadait.com/

https://richardtong.com.au/

prevention [technology](#) worldwide and has become the de facto standard for the industry."

Commercial Intrusion Detection Systems

If you are looking for Commercial Intrusion Detection Systems, here are a few of these as well:

Tripwire

http://www.tripwire.com

Touch Technology Inc (POLYCENTER Security Intrusion Detector)

http://www.ttinet.com

Internet Security Systems (Real Secure Server Sensor)

http://www.iss.net

eEye Digital Security (SecureIIS Web Server Protection)

http://www.eeye.com

Surfing the Web Anonymously – Questions to Ask

When you surf the web it is possible to learn information about you even when you don't want to [advertise](#) who you are. This is true even if your system contains no virus or malware software.

Specifically information that is easily available online includes your IP address, your country (and often more location information based on IP address), what computer system you are on, what browser you use, your browser history, and other information. It gets worse.

People can get your computer's name and even find out your name if your machine supports programs like finger or identd. Also, cookies can track your habits as you move from machine to machine.

How do people get this basic information about you?

When you visit another web site, information about you can be retrieved. Basically, information is intercepted and used by others to track your Internet activities.

How do you stop this from happening?

First of all, it is possible to serf the web anonymously and thereby stop leaving a trail for others to find. Note that this is not fool-proof, but it makes it much harder for people to know who you are. There are products called anonymous proxy servers that help protect you. The anonymous proxy server replaces your Internet address for its own. This has the effect of hiding your IP address and making it much harder for people to track you.

How do I get an anonymous proxy server?

There are many vendors who sell anonymous proxy servers. There are also free proxy servers available to you. Two such products are ShadowSurf and Guardster. Guardster (http://www.guardster.com/) offers various services for anonymous and secure access to the web, some paid as well as a free service. ShadowSurf (http://www.shadowsurf.com/) ShadowSurf provides anonymous surfing at their site for free. Go to it and you will find a box to enter a URL that you want no one to track. There are many others, but here are two that are frequently used.

Another interesting product, given the recent news about the Google search engine filtering its findings for the Chinese government, is Anonymizer (http://www.anonymizer.com). This company, among others, recently (Feb 1st, 2006) pressed that it "is developing a new anti-censorship solution that will enable Chinese citizens to safely access the entire Internet filter-free" (http://www.anonymizer.com/consumer/media/press_releases/02 012006.html).

Does an anonymous proxy server make you 100% safe?

No. Still, you are much better off if you use such technology.

What other things should I be concerned about when trying to keep my private information private?

Three other items come to mind when trying to keep your information private. First, you can use an encrypted connection to hide your surfing. This article does not go into detail on this, but

search the [web](#) and you will find a lot of information on this. Secondly, delete cookies after each session. Third, you can configure your browser to remove JavaScript, [Java](#), and active [content](#). This actually [leads](#) to limitations, so you need to think about the cost/benefit of this [course](#) of action.

Computer Viruses... And Anti-Viruses

Every day new computer viruses are created to annoy us and to wreck havoc on our computer systems. Below are ten viruses currently cited as

being the most prevalent in terms of being seen the most or in their ability to potentially cause damage.

New viruses are created daily. This is by no means an all inclusive list. The best thing you can do is to remain vigilant, keep your anti-virus software updated, and stay aware of the current computer virus threats.

Virus: Trojan.Lodear

A Trojan horse that attempts to download remote files. It will inject a .dll file into the EXPLORER.EXE process causing system instability.

Virus: W32.Beagle.CO@mm

A mass-mailing worm that lowers security settings. It can delete security-related registry sub keys and may block access to security-related websites.

Virus: Backdoor.Zagaban

A Trojan horse that allows the compromised computer to be used as a covert proxy and which may degrade network performance.

Virus:W32/Netsky-P

A mass-mailing worm which spreads by emailing itself to addresses produced from files on the local drives.

Virus: W32/Mytob-GH

A mass-mailing worm and IRC backdoor Trojan for the Windows platform. Messages sent by this worm will have the subject chosen randomly from a list including titles such as: Notice of account limitation, Email Account Suspension, Security measures, Members Support, Important Notification.

Virus: W32/Mytob-EX

A mass-mailing worm and IRC backdoor Trojan similar in nature to W32-Mytob-GH. W32/Mytob-EX runs continuously in the background, providing a backdoor server which allows a remote intruder to gain access and control over the computer via IRC channels. This virus spreads by sending itself to email attachments harvested from your email addresses.

Virus: W32/Mytob-AS, Mytob-BE, Mytob-C, and Mytob-ER

This family of worm variations possesses similar characteristics in terms of what they can do. They are mass-mailing worms with backdoor functionality that can be controlled through the Internet Relay Chat (IRC) network. Additionally, they can spread through email and through various operating system vulnerabilities such as the LSASS (MS04-011).

Virus: Zafi-D

A mass mailing worm and a peer-to-peer worm which copies itself to the Windows system folder with the filename Norton Update.exe. It

can then create a number of files in the Windows system folder with filenames consisting of 8 random characters and a DLL extension. W32/Zafi-D copies itself to folders with names containing share, upload, or music as ICQ 2005a new!.exe or winamp 5.7 new!.exe. W32/Zafi-D will also display a fake error message box with the caption "CRC: 04F6Bh" and the text "Error in packed file!".

Virus: W32/Netsky-D

A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the LSASS (MS04-011) exploit.

Virus:W32/Zafi-B

A peer-to-peer (P2P) and email worm that will copy itself to the Windows system folder as a randomly named EXE file. This worm will test for the presence of an Internet connection by attempting to connect to www.google.com or www.microsoft.com. A bilingual, worm with an attached Hungarian political text message box which translates to "We demand that the government accommodates the homeless, tightens up the penal code and VOTES FOR THE DEATH PENALTY to cut down the increasing crime. Jun. 2004, Pécs (SNAF Team)"

Trojan Horse – Greek Myth or Computer Nemesis?

We have all heard the term Trojan Horse, but what exactly is it? A Trojan Horse is a destructive program that masquerades as a harmless

application. Unlike viruses, Trojan Horses do not replicate themselves, but they can be just as destructive. One of the most dangerous examples of a Trojan is a program that promises to rid your computer of viruses but instead introduces viruses into your computer.

The Trojan can be tricky. Who hasn't been online and had an advertisement pop up claiming to be able to rid your computer of some nasty virus? Or, even more frightening, you receive an email that claims to be alerting you to a new virus that can threaten your computer. The sender promises to quickly eradicate, or protect, your computer from viruses if you simply download their "free", attached software into your computer. You may be skeptical but the software looks legitimate and the company sounds reputable. You proceed to take them up on their offer and download the software. In doing so, you have just potentially exposed yourself to a massive headache and your computer to a laundry list of ailments.

When a Trojan is activated, numerous things can happen. Some Trojans are more annoying than malicious. Some of the less annoying Trojans may choose to change your desktop settings or add silly desktop icons. The more serious Trojans can erase or overwrite data on your computer, corrupt files, spread other malware such as viruses, spy on the user of a computer and secretly report data like browsing habits to other people, log keystrokes to steal information such as passwords and credit card numbers, phish for bank account details (which can be used for criminal activities), and even install a backdoor into your computer system so that they can come and go as they please.

Click Here for Related Information

To increase your odds of not encountering a Trojan, follow these guidelines:

Remain diligent.

Trojans can infect your computer through rogue websites, instant messaging, and emails with attachments. Do not download anything into your computer unless you are 100 percent sure of its sender or source.

Ensure that your operating system is always up-to-date. If you are running a Microsoft Windows operating system, this is essential.

Install reliable anti-virus software. It is also important that you download any updates frequently to catch all new Trojan Horses, viruses, and worms. Be sure that the anti-virus program that you choose can also scan e-mails and files downloaded through the Internet.

Consider installing a firewall.

A firewall is a system that prevents unauthorized use and access to your computer. A firewall is not going to eliminate your computer virus problems, but when used in conjunction with regular operating system updates and reliable anti-virus software, it can provide additional security and protection for your computer.

Nothing can guarantee the security of your computer 100 percent. However, you can continue to improve your computer's security and

decrease the possibility of infection by consistently following these guidelines.

Who are the Players in the Anti-virus Industry?

Everyone in the United States has heard of the leading anti-virus vendors Symantec, Mcafee, Computer Associates, and Trend Micro. These companies have market-leading presence in the United States.

Microsoft, as well, has plans become a key player in this market. Microsoft acquired intellectual property and [technology](#) from GeCad software in 2003, a company based in Bucharest, Romania. They also acquired Pelican Software, which had a behavior based security as well as Giant Company [Software](#) for spyware and Sybari Software, which manages virus, spam, and phishing filtering.

A lot of discussion has centered on whether Microsoft with come to own a dominant position in the anti-virus market by simply bundling its technologies with its operating systems at no charge. This is a similar technique applied in other markets such as word processing and [Internet](#) browsers.

Of course there are a number of anti-virus vendors who also play in this [market](#). There are many companies with great market presence in other countries that are beginning to become more widely known. These vendors include GriSoft out of the Czech Republic, Sophos in the united Kingdom, Panda Software out of Spain, Kaspersky in Russia, SoftWin in Romania, F-

Secure in Finland, Norman in Norway, Arcabit in Poland, VirusBuster out of Hungary, and AhnLab in South Korea.

It is not clear where the industry is heading and everyone in this market faces a rapidly changing landscape. The amount of effort to find and provide fixes for viruses is staggering. Malicious programs are getting more complex and the number of them is increasing. Many companies may find themselves without the resources to match the efforts of those truly bent on creating havoc.

Some virus companies are getting of hundreds of new samples a day! Moreover, the new viruses are getting "smarter" in that they propagate themselves quickly and they often hide themselves and are smart enough to move around in a system by renaming themselves in an effort to make it hard to remove them.

Protection You Can Afford

All in all, there are <u>numerous</u> ways you can lose the information on your computer. Your <u>child</u> decides to play Chopin on your keyboard, a <u>power</u> surge, lightening, a virus, or even simple equipment failure. Therefore, backing up the contents of your hard drive is an absolute MUST. By regularly making backup copies of your files and storing them in a separate location, you can typically get some, if not all, of your information back in the event your computer crashes.

While a regular backup to floppy, CD, or zip drive will save your files, wouldn't it be great if you could create an exact copy (a drive image) of your hard disk? That means backups of all your files, <u>programs</u>, and user settings. This would definitely save you time when it came to reloading. Acronis may be able to help.

Acronis True <u>Image</u> 9.0 is a robust disk-imaging utility <u>software</u> that copies the entire <u>contents</u> of your hard drive including data and operating system files, personalized settings, and more, onto another disk or disk partition. Its layout is easy to use and navigate. It also includes wizards which can walk you through both backing up and restoring your computer. Highlighted features include:

Secure Zone — allows you to save data to a special hidden partition located on your hard drive which would eliminate the need to purchase an extra hard drive.

Jada IT
https://jadait.com/

RichardTong
https://richardtong.com.au/

PC Cloning — you can upgrade to a new system disk without needing to reinstall the operating system and applications, or configure user settings.

Acronis Snap Restore – lightening-speed restore of your PC from an image. You can start working in seconds while your system is still being restored. Acronis provides a free test-drive of its product and a 30-day money back guarantee. When you are ready to purchase, you can either download for $49.99, or if you so desire, order a boxed version for $59.99. With Acronis True Image Home 9.0, you can rest easy that your family pictures, personal documents, tax returns, resumes, and other important information will not be lost forever.

Resources & Links

Download Ian del Carmen's International bestselling book worth $97! "Rags to Dot Com Riches" is NOW for **FREE** at

http://RagsToDotComRiches.com

Learn Internet Marketing at The Internet Business Academy –

http://TheInternetBusinessAcademy.com

Domain names – http://idcibc.com/go/?domain

Web hosting - http://idcibc.com/go/?webhost

Website creation - http://idcibc.com/go/?outsource

Website traffic - http://idcibc.com/go/?traffic

Link Tracker - http://idcibc.com/go/?linktracker

Click Here for Related Information

More Unadvertised Gifts

Click Here To Download
http://iBookWholesaler.com/gifts/