

# How to protect yourself from Spyware



*A good defense starts with a thorough understanding of your opponent's offense. How to protect yourself from spyware teaches you what is spyware, how is it being distributed and installed and how to protect from it. Our leading experts in information security show you not only how to discover spyware on your computer but what you can do to protect yourself against them. When it comes to securing your privacy, knowledge is power. This book gives you the knowledge to build a proper defense against spyware.*

\*\*\*

A good defense starts with a thorough understanding of your opponent's offense. *How to protect yourself from spyware* teaches you what is spyware, how is it being distributed and installed and how to protect from it. Our leading experts in information security show you not only how to discover spyware on your computer but what you can do to protect yourself against them. When it comes to securing your privacy, knowledge is power. This book gives you the knowledge to build a proper defense against spyware.

\*\*\*

# Table of Contents

<b>TABLE OF CONTENTS</b> .....	<b>3</b>
Warning .....	4
<b>CHAPTER 1 – INTRODUCTION</b> .....	<b>5</b>
<b>CHAPTER 2 – WHAT IS SPYWARE?</b> .....	<b>6</b>
Spyware .....	6
Adware.....	6
Legitimate software.....	7
<b>CHAPTER 3 – WHAT DO SPYWARE AND ADWARE APPLICATIONS DO?</b> .....	<b>8</b>
Examples of spyware.....	9
<b>CHAPTER 4 – HOW CAN I GET “INFECTED” WITH SPYWARE?</b> .....	<b>12</b>
Users’ unintentional permission.....	12
P2P file transfer or software download.....	12
Deceptive or confusing pop-ups.....	13
Shareware – freeware – P2P software .....	13
Opening insecure e-mails.....	14
Visit to certain Web sites.....	14
Accepting files while chatting on-line.....	15
<b>CHAPTER 5 – HOW CAN I KNOW THAT SPYWARE IS INSTALLED ON MY COMPUTER?</b> .....	<b>16</b>
<b>CHAPTER 6 – HOW CAN I PROTECT MYSELF FROM SPYWARE?</b> .....	<b>18</b>
<b>CHAPTER 7 – FINAL WORDS</b> .....	<b>20</b>

## **Warning**

This book is written to provide information about ever growing security problem - spyware. Unfortunately, many legitimate programs are being presented as spyware and therefore every effort has been made to make this book as accurate as possible, but no warranty is implied. The information is provided on an as-is basis. Any actions and / or activities related to the material contained within this book are solely your responsibility. The authors will not be held responsible for any individuals misusing the information in this book. (Please note that this book was created for Information purposes only.)

# CHAPTER 1 – Introduction

The Internet is ever growing and you and we are truly pebbles in a vast ocean of information. They say what you don't know can't hurt you. When it comes to the Internet believe quite the opposite. On the Internet there are millions and millions of computer users logging on and off on a daily basis. Information is transferred from one point to another in milliseconds. Amongst those millions upon millions of users, there are you.

In past few years, one of the major threats were surely hackers and computer viruses. Huge effort was made to fight these problems – it took almost whole decade and problem is still not solved completely, but today we can freely say that viruses do not pose such huge threat as they once did. We learned how to discover them, stop them, destroy them... Almost every company has Anti-virus systems scanning all incoming and outgoing data, all mail servers are also checking all incoming and outgoing messages... But, what is most important, general public is aware of this threat and each person possessing PC knows what has to be done to protect from these threats.

Unfortunately, we can't rest – new security threat is emerging and each day more and more analysts warn us that spyware will be major security problem in years to come. Over the last several years, a loosely defined collection of computer software known as “spyware” has become the subject of growing public alarm. Computer users are increasingly finding programs on their computers that they did not know were installed and that they cannot uninstall, that create privacy problems and open security holes that can hurt the performance and stability of their systems, and that can lead them to mistakenly believe that these problems are the fault of another application or their Internet provider. What is even worse, general public is not informed enough on this issue, companies are still not taking this problem seriously enough, and, finally, only few know how to fight it.

In this book, we will cover this growing problem. We will explain what spyware is, how it works, what is it's purpose... We will also show you how to fight spyware – how to discover it, how to remove it and how to protect yourself from it. By no means we are going to make a ludicrous claim that this book will protect you from all spyware. What we say is that by reading this book hopefully you will be in a better situation to protect yourself from having your information compromised and spyware installed.

## CHAPTER 2 – What is spyware?

The term “spyware” has been applied to everything from keystroke loggers, advertising applications that track users’ web browsing, web cookies, to programs designed to help provide security patches directly to users. More recently, there has been particular attention paid to a variety of applications that piggyback on peer-to-peer file-sharing software and other free downloads as a way to gain access to people’s computers. This book focuses primarily on these so-called “spyware” and “adware” and other similar applications, which have increasingly been the focus of legislative and regulatory proposals. Many of these applications represent a significant privacy threat.

There are at least three general categories of applications that are described as spyware. They are:

- Spyware - key stroke loggers and screen capture utilities, which are installed by a third party to monitor work habits, observe online behavior, or capture passwords and other information;
- Adware - applications that install themselves surreptitiously through “drive-by downloads” or by piggybacking on other applications and track users’ behaviors and take advantage of their Internet connection;
- Legitimate software - legitimate applications that have faulty or weak user-privacy protections.

It is in the first two cases that the spyware label is the most appropriate. In the third case, it is not.

### Spyware

Programs in the first category, which are sometimes called “snoopware”, are typically stand-alone programs installed intentionally by one user onto a computer used by others. Some capture all keystrokes and record periodic screen shots, while others are more focused, just grabbing websites visited or suspected passwords. These programs have legal uses (e.g. for certain narrow kinds of employee monitoring) as well as many clearly illegal ones. The best known spyware programs are Trojans which are mostly used by hackers. They enable them to capture important data from victims’ computer – keystrokes, e-mail addresses, screenshots, passwords, download files...

### Adware

Software in the second category installs itself covertly, generally by piggybacking on another, unrelated application or by deceptive download practices. These programs start-up on their own and make unauthorized use of users’ computers and Internet connections, in many cases transmitting information about the user or it’s computer back to a central location. They often resist uninstallation.

They usually do not capture keystrokes or screenshots. In part because applications in this second category fall into a legal grey-zone, they have recently been the focus of a great deal of attention and concern.

## **Legitimate software**

Legitimate software which includes programs based on legitimate business models that incorporate features with flawed user privacy protections. Generally the problem relates to the unnecessary inclusion or inappropriate use of a unique program ID, which creates the potential for user tracking.

Of course, the lines between the three categories we present here can be fuzzy and it is sometimes difficult to tell which group any given application rightfully belongs in. Our concerns about the security and privacy is one basis for our preference for general baseline privacy legislation as a response to spyware. Also, until such legislation arrives, we wish to alarm general public to become more aware of this ever growing security and privacy threat.

## **CHAPTER 3 – What do spyware and adware applications do?**

The vast majority of writing about the spyware problem has focused on the privacy dimension of the issue. Privacy is one of the major concerns raised by spyware, but large issues are transparency and control too. Users are typically unaware that spyware programs are being installed on their computers and often are unable to uninstall them. They may not even know that their computers have been infected until they find ads popping up all over their desktops or one day they may notice that their computers are working slower than usual, which usually happens when spyware programs are uploading information to a remote server or are downloading new ads. These are only few of the symptoms of what can be a very serious problem because these programs can change the appearance of websites, modify users' "start" and "search" pages in their browsers or change low level system settings. They are often responsible for significant reductions in computer performance and system stability. In many cases, consumers are mistakenly led to believe that the problem is with another application or with their Internet provider, placing a substantial burden on the support departments of providers of those legitimate applications and services. Even in cases where these programs transmit no personally identifiable information, their hidden, unauthorized use of users' computers and Internet connections threatens the security of computers and the integrity of online communications.

In some cases, these invasive applications closely resemble more traditional viruses. While many spyware programs piggyback on other applications or trick users into authorizing installations through deceptive browser pop-ups, some spread themselves by exploiting security vulnerabilities in email attachments or browsers. In addition, many of these programs create major new security vulnerabilities by including capabilities to automatically download and install additional pieces of code without notifying users or asking for their consent and typically with minimal security safeguards. This capability is often part of an "auto-update" component, and it opens up a world of concerns on top of those posed by objectionable behaviors in the originally installed application itself.

Users must have control over what programs are installed on their computers and over how their Internet connections are used. They must be able to count on a predictable web-browsing experience and they must have the ability to remove it for any reason and at any point programs they don't want. A growing body of invasive applications takes away this control.

Unfortunately, the story doesn't end here. Even though the problems described above are cause for general security concern, what is more alarming is illegal use of these programs. What is even worse, many of these programs are intentionally created for that purpose only. For example, the most popular Trojan horse, SubSeven, is made only for one purpose – gathering information from victims'

computer. Once installed on your machine, it gives hacker almost unlimited access of your computer. Not only that it captures keystrokes and screenshots but it gives hacker full access to all your drives and files, e-mails, ability to use your computer as a bridge to other hacking activities, disable your keyboard and mouse... All personal data is compromised. But, the story doesn't end there either – once hacker has all your friends' e-mail addresses, he can easily spread his spyware software to them too! All he has to do is send an e-mail signed by you to them from your own account (he has access to that too) and attach Trojan to it. This is the most commonly used way to spread spyware, adware and viruses. Beside hackers, many companies are also gathering private information from users using their software. These information are usually used for advertising but for general trade as well.

All mentioned above is clear indicator that spyware is a serious privacy and security threat that we will have to deal with in time to come. The sooner we alarm and inform general public on this matter, the better results we will have and we will avoid greater damage.

## **Examples of spyware**

### **Example 1**

Queens resident Ju Ju Jiang admitted to installing a keylogger called Invisible KeyLogger Stealth (IKS) on public computers at 13 Kinko's stores in New York. Using the keylogger, Jiang acquired over 450 banking passwords and usernames from customers who used the public computers. Jiang used the stolen financial information to open new bank accounts and then siphon money from legitimate accounts into the new, fraudulent accounts. Although IKS markets its products to IT administrators and parents, Jiang's exploits illustrate how it and other similar programs can easily be used for illegal purposes.

### **Example 2 –nCase**

One category of spyware includes programs that collect information from a user's computer – in some cases including personally identifiable information such as a name or email address. This can compromise both a user's control over his computer and Internet connection and his privacy. Of course, the most egregious forms of keystroke logging or screen capturing spyware, for which the primary advertised purpose is monitoring or spying, clearly fall into this category, but so do many applications which piggyback on free downloads as a vehicle to serve advertising. One notable example of spyware of this variety is nCase, produced by 180Solutions.

nCase is bundled with an array of free products, including some peer-to-peer applications. Once installed, it registers a unique identifier and tracks websites viewed, including monitoring search terms. In some cases, this information is reportedly aggregated with registration data collected by the affiliate application. There have also been reports that newer versions of the software attempt to read an email address, real name, or ZIP code from other applications' data in the registry, and to associate this information with the user's unique ID. 180Solutions reports that it keeps track of demographic

information for at least 40% of its user base. This information can include age, sex, home and work location, and household income. nCase uses the information it collects to deliver targeted pop-up ads and sells the data to third parties. The company advertises the ability to “see a 360-degree view of the user's behavior—24 hours a day, 7 days a week.” On top of these substantial privacy problems, nCase raises significant user control issues. In addition to bundling with other applications, nCase has been accused of deceiving users into granting permission to download and install the application by presenting potentially deceptive or confusing pop-ups on various websites or by taking advantage of poorly configured security settings in users’ browsers (a practice known as “drive by downloads”). In addition, there have been reports of other spyware programs installing nCase in the background once they have gained access to a user’s computer. Although nCase does appear in the Add/Remove programs menu in Windows, its uninstallation process is notoriously long and complicated, and in instances where nCase is installed alongside another application, nCase generally remains on a user’s computer even after the original host application is uninstalled. On top of everything else, nCase has been reported to open up back doors into users’ computers, creating a significant security hazard.

### **Example 3 —Altnet**

Another category of spyware consists of programs that do not represent an immediate privacy threat because they do not collect user information, but still hijack the user’s computer and Internet connection for their own purposes. The most prominent recent example is “Altnet.”

In April 2003, it was discovered that software with undisclosed networking capabilities was being bundled with the popular Kazaa Media Desktop. Installing the Kazaa file-sharing program also installed a companion program, “Altnet,” created by a company called Brilliant Digital Entertainment (BDE). Through Altnet, BDE had the ability to activate the user’s computer as a node in a distributed storage and computing network distinct from Kazaa’s existing peer-to-peer network. Users were never clearly told that software with the capability to use their computers and network connections in this way was being installed. Since the discovery of BDE’s intentions in a securities filing, the company has acknowledged its intent to launch the Altnet network, publishing the following description on its website:

*“Altnet is giving you the opportunity to opt in to making certain parts of your computing power, disk space and bandwidth available to Altnet business partners. You will know exactly how a business would use your source at the time of use. You choose what jobs can use your machine and which ones cannot. Altnet will charge its business partners for this service and pass on benefits to you. All this will be conducted with absolute respect for your privacy and your choices.”*

However, the section of the Kazaa/Brilliant end user license agreement (EULA) dealing with Altnet paints a somewhat different picture:

*“You hereby grant BDE the right to access and use the unused computing power and storage space on your computer/s and/or internet access or bandwidth for the aggregation of content and use in distributed computing. The user acknowledges and authorizes this use without the right of compensation. Notwithstanding the above, in the event usage of your computer is initiated by a party other than you, BDE will grant you the ability to deny access.”*

There are several major problems with Altnet from the perspective of user control. Although BDE included a statement of the purposes of the Altnet program buried in the EULA that comes with Kazaa, this hardly represents the kind of clear, conspicuous notice that should accompany requests to access a user's Internet connection. The widespread dismay that accompanied the disclosure of BDE's intentions to construct a distributed computing network demonstrates that the consent BDE was receiving from users of Kazaa was not, by any stretch of the imagination, well-informed.

Moreover, the terms BDE set forth in the EULA provide for substantially more permissive access to users' computers than what BDE now claims on its website will be done with the Altnet network. Whereas BDE now claims that the service will be "opt-in," the EULA reserved the right to make it "opt-out." Whereas BDE says it will "pass on benefits" to users in exchange for use of their computers, in the EULA, BDE reserved the right to make use of user's processing power and bandwidth "without ... compensation."

Finally, while Brilliant points out that it is possible to uninstall BDE/Altnet without disabling Kazaa, it is an extended process that involves at least twelve steps, including tracking down and deleting files scattered across Windows' "System" folders. Additionally, although the BDE application piggybacked on Kazaa during installation, uninstalling Kazaa generally does not uninstall Altnet.

Of course, there are other types of spyware/adware applications but making whole list would take too much time and space. Purpose of this e-book is to give you general knowledge, and we believe that examples we included will provide you enough information to sense threat spyware/adware pose.

# CHAPTER 4 – How can I get “infected” with spyware?

There are many ways for you to get infected with spyware. Spyware and adware can be acquired

- when you unknowingly give your permission while downloading/installing applications
- during a peer-to-peer (P2P) file transfer or software download
- when you click on a deceptive or confusing pop-up
- when you install insecure shareware/freeware and P2P applications
- when you open e-mails you're not sure are legitimate (spam mail)
- when simply visiting certain Web sites
- when you accept and receive files when chatting on-line with persons you personally do not know

## Users' unintentional permission

Many legitimate applications installation packages include other, but spyware applications, too. Usually, during the installation process you are asked to choose whether you wish to install those additional software as well. Features of such additional software are usually not completely described or their real purpose is hidden somewhere in long description, usually in form of a note. In some cases, option to install (or not to install) is simply presented in form of a single checkbox with explanation similar to “include free *nnnnn* software”. But, no matter what the case is, creators of such installation packages count on your thoughtless and unawareness, and hope that you will not pay necessary attention to such notices or will not notice them at all) and will permit installation of additional spyware software. In such way producers of such packages are legally backed up and all responsibility is switched off to you. Moreover, those additionally installed applications are not presented in Add/Remove Programs and have no visible screens while running (usually running in background) and user may never know about them. Also, when uninstalling main applications, these additional applications remain on users' computer what is another security and control threat.

## P2P file transfer or software download

By using P2P software, you already crossed half the way to get infected by adware/spyware application. You can never know the real content of the files you download, especially if you're downloading executables. There is no guarantee that downloaded .exe file will do only what its' description says. In many cases, executables available on P2P contain spyware/adware which are installed on your machine first time you run it. Some applications only carry spyware/adware

applications, while other are altered and are spyware/adware itself. If you are using P2P application, just think how many times you downloaded some files named and described in English (filename also in English) only to discover that whole content is in some other, foreign language (this is the most obvious when downloading e-books or other similar publications).

### **Deceptive or confusing pop-ups**

Some pop-up screens don't actually deliver advertisements but attempt to install unwanted software on your system and change your system configurations. These pop-ups can be very clever. Instead of "To install this program, click Yes," the prompt unexpectedly reads, "To install this program, click No." After clicking on these pop-ups, you may find that the computer now displays new bookmarks and a different home page as well as having unwanted software installed.

### **Shareware – freeware – P2P software**

It is important to say that currently there are well over 800 shareware-freeware which also **include adware and spyware** and the numbers of web sites that include these types of installers is impossible to calculate (we described those under "Users' unintentional permission"). These Freeware and Shareware applications are located all over the internet as easy downloads. They can be found on CNet, Tucows and hundreds of other locations offering free & low cost bargains. **Most of these products make no real statement that they include adware or spyware and if they do it is buried in the "terms of use" or at best they might make a vague reference that they are ad supported.** Some developers might include a vague privacy statement which does not fully explain what information will be gathered or give a full explanation regarding what will be done with the information.

As an example of the scope and extent of the number consumers effected, consider that an estimated 260 MILLION computer users have downloaded at least one of the five most popular Gnutella File sharing applications just from CNet.com in the United States alone (Sept. 2002).

KaZaA Media Desktop	119,021,166
Morpheus	102,253,332
BearShare	17,651,773
LimeWire	14,528,779
Grokster	4,307,827
Total Downloads from CNet.com	257,762,877

The known third-party applications bundled with these downloads include Cydoor, TopText, Onflow, Webhancer, BonziBuddy, ClickTillUWin, and New.net in addition to trojans and viruses such as the self replicating Nimda virus. These add on spyware/adware applications can deliver on line

advertisements, collect information, assign computers user's a GUID for user tracking, overlay content or graphics on the Web site they are viewing, or modify their system settings.

What is even more alarming is that these estimates do not include the numbers from the many other download locations scattered across the internet nor do these figures include estimates of the various other Gnutella file sharing programs that are available or any of the 900 freeware or shareware programs that are downloaded each let a long the number of the "drive-by" "backdoor" installations. If these additional numbers were able to be calculated the total number of effected computers would be staggering and well be well over 600 million infected computers!

### **Opening insecure e-mails**

Many spyware / adware applications are being distributed through e-mail. Content of such mails can vary – from the ones informing you that you won a free trip to some famous tourist destination to those that contain no text at all but only suspicious attachment. When you open such e-mail, usually silent installation process that installs spyware on your computer is started.

Other type includes e-mails whose purpose is to collect your private information. For example, you can receive an e-mail informing you that you have received a free gift. If you accept to receive that gift, you will be asked to enter valid information (name, surname, address, etc...) in order to receive that gift. Just after you enter these information you will be informed that gift was indeed free but that you are obliged to pay shipping (be sure that in this shipping price, price of the gift is included too). No matter whether you choose to pay shipping and receive free gift or to simply abort, result is same – all personal information you entered in screen before are already sent to central location and will be used for some other purpose (advertising, reselling...)

### **Visit to certain Web sites**

Some spyware is secretly downloaded when you launch a program acquired from a Web site. For example, a pop-up may notify you that a special plug-in is required to run a video or movie file. In this case, what appears to be a legitimate plug-in could actually be spyware. Some spyware takes advantage of known vulnerabilities in the Microsoft® Windows operating system and Internet Explorer browser to secretly place spyware your computer. For example, one such method involves pushing malicious JavaScript and VBScript code to the user's Web browsers when they visit a seemingly ordinary Web page. If the user's Internet Explorer security preferences are set to the lowest levels, the code can install spyware programs on the user's hard drive and even set them so that they launch automatically the next time the user reboots. It can also insert toolbars and other objects into the browser itself, essentially changing the way the browser works in the future—all without the user's permission.

Another method bypasses the security settings altogether by exploiting a bug in Internet Explorer versions 4 and 5. These versions allow Web scripts to gain access to a hard drive by overflowing the browser with data. Malicious webmasters use this exploit to install spyware or modify the way the

browser works.

### **Accepting files while chatting on-line**

Chat sites are probably one of the primary places that hackers' activity takes place. In many cases, when chatting with persons you don't know face to face, be sure to double check all files received. You would be amazed with number of users that got infected simply by accepting and running files from persons they met in chatroom. For example, if your "friend" offers you to send his photo, be sure that file you received doesn't have double extensions (like .jpg.exe or similar) – in such cases you can be sure that file is spyware.

# **CHAPTER 5 – How can I know that spyware is installed on my computer?**

There are many ways to notice that spyware is actually installed on your machine. Generally, if you notice anything strange going on with your computer (strange pop-ups, different home page in your Web browser, new icons...) it is highly possible that your computer is infected with spyware/adware application. Here we give short list of the most common signs that you can notice if you have spyware application installed on your computer.

- 1.** You find a new finger-size hardware device connected between your keyboard cable's plug and the corresponding socket on the back of your computer. Or maybe someone recently offered you "a better keyboard."
- 2.** Your phone bill includes expensive calls to 900 numbers that you never made—probably at an outrageous per-minute rate.
- 3.** You enter a search term in Internet Explorer's address bar and press Enter to start the search. Instead of your usual search site, an unfamiliar site handles the search.
- 4.** Your antispware program or another protective program stops working correctly. It may warn you that certain necessary support files are missing, but if you restore the files they go missing again. It may appear to launch normally and then spontaneously shut down, or it may simply crash whenever you try to run it.
- 5.** A new item appears in your Favorites list without you putting it there. No matter how many times you delete it, the item always reappears there later.
- 6.** Your system runs noticeably slower than it did before. If you're a Windows 2000/XP user, launching the Task Manager and clicking the Processes tab reveals that an unfamiliar process is using nearly 100 percent of available CPU cycles.
- 7.** At a time when you're not doing anything online, the send or receive lights on your dial-up or broadband modem blink just as wildly as when you're downloading a file or surfing the Web. Or the network/modem icon in your system tray flashes rapidly even when you're not using the connection.
- 8.** A search toolbar or other browser toolbar appears even though you didn't request or install it. Your

attempts to remove it fail, or it comes back after removal.

**9.** You get pop-up advertisements when your browser is not running or when your system is not even connected to the Internet, or you get pop-up ads that address you by name.

**10.** When you start your browser, the home page has changed to something undesirable. You change it back manually, but soon you find that it has changed back again.

**11.** And the final sign is: Everything appears to be normal. The most devious spyware doesn't leave traces you'd notice, so scan your system anyway.

# CHAPTER 6 – How can I protect myself from spyware?

As we've already mentioned the more you know about spyware and adware the better protection you have – knowledge is power. We already explained what spyware and adware are, what those applications do on your machine and how you can get infected. Therefore, even without us telling you, now you can think of the best way to protect yourself from spyware. Still, here we give few steps that you should follow in order to protect yourself from spyware (you can check whether you came up with good solution and what you might have had overlooked):

- 1.** Make sure to install and run an antispymware application (any of the [Lavasoftware's AdAware](#), [H-Desk's Disspy](#) or [eTrust's PestPatrol](#) should do). Perform on-demand scans regularly to root out spyware that slips through the cracks. Reboot after removal and rescan to make sure no ticklers, which are designed to reinstall spyware, have resurrected any deleted applications. Additionally, be sure to activate real-time blocking abilities of your antispymware application. Hopefully, antispymware application will prevent great number of spyware applications from ever being installed on your computer. Finally, regularly update your antispymware application – check for available updates at least once a week.
- 2.** Give your antispymware application some backup. In addition to an antispymware application, make sure to run both software and hardware firewalls and antivirus applications to protect yourself against Trojan horses and viruses ([Zone Labs' ZoneAlarm](#) or [Symantec AntiVirus and Internet security](#) should do. Some antispymware applications, such as [H-Desk's Disspy](#), have Trojan protection included).
- 3.** Beware of peer-to-peer file-sharing services. Many of the most popular applications include spyware in their installation procedures. Also, never download any executables via P2P, because you can't be absolutely certain what they are. Actually, it's a good idea to avoid downloading executables from anywhere but vendors or major, well-checked sites.
- 4.** Watch out for cookies. While they may not be the worst form of spyware, information gathered via cookies can sometimes be matched with information gathered elsewhere (via Web bugs, for example) to provide surprisingly detailed profiles of you and your browsing habits.
- 5.** Squash bugs. Web bugs are spies that are activated when you open contaminated HTML e-mail. Get rid of unsolicited e-mail without reading it when you can; turn off the preview pane to delete messages without opening them. In Outlook 2003, Tools > Options, click on the Security tab and select Change Automatic Download Settings. Make sure "Don't download pictures or other content automatically in HTML e-mail" is checked.

- 6.** Don't install anything without knowing exactly what it is. This means reading the end-user license agreement (EULA) carefully, as some EULAs will actually tell you that if you install the app in question, you've also decided to install some spyware with the software. Check independent sources as well, as some EULAs won't tell you about spyware.
  
- 7.** Protect yourself against drive-by downloads. Make sure your browser settings are stringent enough to protect you. In IE, this means your security settings for the Internet Zone should be at least medium. Deny the browser permission to install any ActiveX control you haven't requested.
  
- 8.** Do not open e-mails whose senders you don't know. Even if you open such e-mail, be sure not to download (or open) any attachments and be sure to thoroughly read all information included.
  
- 9.** When receiving files from someone (even if you know the person) run antispymware and ativirus check on those files.
  
- 10.** Keep up to date on the ever-changing world of spyware. Knowing the threat will help you defeat it. There are several great sites you can visit to keep abreast of this issue. [PestPatrol's Research Center](#) has one of the most comprehensive lists of spyware and related threats we've seen. [Spyware info](#) is another good online source of information. Finally, [best spyware remover](#) is also great site where you can get informed on this matter.

## **CHAPTER 7 – Final words**

“A good defense starts with a thorough understanding of your opponent’s offense. *How to protect yourself from spyware* teaches you what is spyware, how is it being distributed and installed and how to protect from it. Our leading experts in information security show you not only how to discover spyware on your computer but what you can do to protect yourself against them. When it comes to securing your privacy, knowledge is power. This book gives you the knowledge to build a proper defense against spyware.”

We intentionally repeated words from foreword. Now, at the end of this book, we truly hope that we succeeded. We hope that we supplied enough information to give you proper knowledge to build a good defense against spyware. We explained you why spyware pose huge security and privacy threat, what does spyware do on your computer, how can you get infected with it and, finally, how you can successfully fight against it. Knowledge is power and by reading this book you made first step. But do not stop here. This book cannot give you whole knowledge nor teach you how to protect yourself from all spyware / adware. Keep informing yourself in time to come – only that way you will guarantee your own privacy.