Spy Proofing Your Computer In 4 Easy Steps!

NOTICE: You Are Free To Give Away or Share this Content. You may also post it to Your Website, Providing You Don't Alter, Edit, or Change The Content In Any Way Shape or Form.

You May Not Charge For This Report!

Spy Proofing Your Computer In 4 Easy Steps

TABLE OF CONTENTS

1. Do I Need To Spy Proof My Computer?

I think the question should be, “do I use my computer for anything that would best remain private and confidential?”

With over 500 "invisible" surveillance spy programs available for anybody to download and install on any computer they choose to, privacy invasion and information theft have become big business.

Add to that the hundreds, if not thousands, of advertising spyware programs in use by companies who want to sell you something. **Chances are that if you haven't been infected with spyware yet, you will be.**

My goal in this report is to show you how protect your privacy using **PROVEN** products that are, in most cases, freely available at no cost to you.

I will back up my research with documented evidence and easy to follow instructions.

So let’s get started by looking at Internet scams in the headlines and why you should protect your computer and your privacy.

2. Scams

Hacker Busted For Identity Theft:

Van T Dinh, told a bunch of online traders in a chat room that he had created winning stock picking software. He offered it free to anyone to try for themselves.

What he neglected to mention was that within his trading software he installed a keylogger.

This gave Dinh access to the passwords of his victims’ trading accounts, email accounts, banking info, and allowed him to buy and sell stocks with their money.

He sold off all the bad stock he had purchased, by going into his victims accounts and purchasing these bad stocks with his victims money, to the tune of $70,000.

Man Arrested For Stealing With Password From PC:

TOKYO — Police said Thursday they have arrested a 43-year-old man in suburban Tokyo for allegedly stealing money from another person's bank account with a password he obtained from a personal computer at an Internet cafe using software to monitor keystrokes.

Tatsuyuki Akiyama of Mitaka in western Tokyo is suspected of using the software known as a keylogger to transfer around 360,000 yen from an Internet banking account of a 30-year-old company employee in Kawaguchi, Saitama Prefecture, to an account with another bank in Aichi Prefecture registered under a third person's name sometime between June and July.

Fake Lycos Screensaver Hides a Keylogger

December 9, 2004 By Enterprise Planet Staff

Lycos made headlines during the past several days by distributing a screensaver designed to swamp the sites of those deemed responsible for spam with extra traffic, in effect giving spammers, at least the companies that bankroll them, a taste of their own medicine.

After passing the 100,000-download mark, the 'Make Love Not Spam' program was scrapped.

This week, F-Secure warns of emails that seemingly contain the screensaver but instead deliver a dangerous payload that piggybacks on the buzz surrounding Lycos' controversial program.

According to the company, the fake emails can be quickly identified via the following attributes:

Subject: Be the first to fight spam with Lycos screen saver

Attachment: Lycos screensaver to fight spam.zip

The malicious code, known as TrojanDropper. FakeSpamFighter, drops Perfect Keylogger components onto a victim's PC. This makes it possible for a third party to monitor the keystrokes of an infected system revealing user/pass combos to online accounts and exposing private information. **USERS ARE WARNED TO BE ON THE LOOKOUT AND TAKE THE SENSIBLE PRECAUTION OF NOT OPENING UNSOLICITED ATTACHMENTS.**

So what are the courts doing about this?

Judge Dismisses Keylogger Case

By ***Kevin Poulson*** SecurityFocus Nov 19 2004

A FEDERAL judge in Los Angeles has dismissed charges against a California man who used a keystroke logger to spy on his employer, ruling that use of such a device does not violate federal wiretap law.

What does this mean to you?

There are many methods by which a thief can obtain sensitive information about you from your computer with a keylogger program.

- Have you ever gone online to check your bank balance?
- Do you type in a password when you check your email…
- Do you go to sensitive secure areas on your company website?

Every time you type anything on your keyboard or visit a website, you could be leaving all that activity on a recording device, planted in or on your computer and you wouldn't even know it.

Tip:
Never use a public terminal in a Hotel, Public Library or Cyber Café to access any of your password protected information. Many times unscrupulous people will put a keylogger on those public terminals to harvest your sensitive information.

3.Types of Computer Recording Devices:

There are two main products that are used to capture and record computer activity: **Hardware Keyloggers and Surveillance Software**. Of these 95% are specifically designed to be undetectable by you, the computer user.

Many Surveillance Software programs are available via a simple download over the Internet, without charge, and completely anonymously!

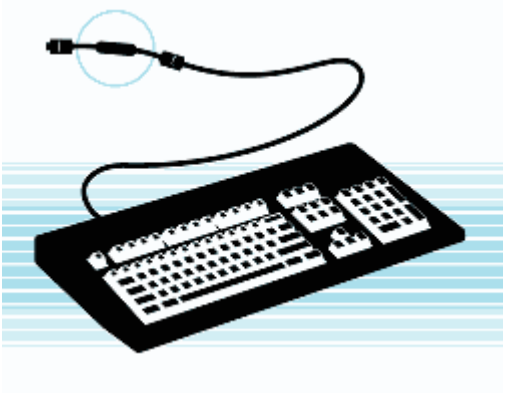
4.Hardware Keyloggers

These types of keyloggers require that the perpetrator have physical access to your computer. They can easily be installed in less than 5 seconds.

Once installed, a hardware keylogger will capture every keystroke entered into your keyboard and then store it for future retrieval on the device itself.

Some hardware keylogger companies boast a two-million keystroke capacity! That's about 5 years worth of typing for the average computer user. Whether at home or in the office, you can easily fall victim to this type of spying. A Hardware Keylogger is installed between your keyboard and computer much like this:

Hardware Keylogger



One of the most popular hardware keyloggers is KeyGhost WWW.KEYGHOST.COM . You can visit their website for more information on hardware keyloggers and why they are such an intrusion into your privacy.

Here is a representation of what a hardware keylogger may actually look like installed:

Tip:
Never Open E-Greeting Cards From Strangers: Software keyloggers can be transmitted over the Internet as an invisible email attachment.

5.Removal of Hardware Keyloggers

By taking a peek behind your system and following your keyboard cable, you can find out if there is something "odd" inserted between your keyboard and computer. **To remove a hardware keylogger, you must shut down your system!** You could damage your system if you attempt to remove the keylogger while your computer is running!

Once your system is powered off, carefully remove the device from in between your keyboard and computer, and then plug your keyboard directly back into the computer. Make sure that it is plugged in completely and be gentle as the connectors are somewhat fragile.

6. Adware… Surveillance Software… Spyware… Keyloggers… I'm Confused?

Don't worry, you're not alone...

Surveillance Spy Software, Keyloggers, Password Grabbers, etc. are generally lumped together with Adware (Advertising Spyware) into one general category called SPYWARE.

In fact, **these are two separate and distinct product types and require very different security measures.**

Adware (Advertising Spyware) which is the most prevalent form of spyware, monitors Internet activity to send targeted advertising to you as a consumer. Adware is generally not a security threat, but can really mess up your computer when you try to remove it. Adware can cost you hundreds of dollars in repair bills.

Surveillance Software is designed to silently record computer activity and then archive it for later retrieval, or stealthily send it back to the intruder, **even bypassing firewalls**.

Surveillance software can be slipped onto your system via greeting card, email attachment, trojan or physical access to your PC.

Tip:
Music or File Sharing Can Be Dangerous: Never download ANYTHING from a website you don't know or can't verify they are a legitimate download site. Many times spyware can be attached to the music or file sharing programs.

7. Adware: The Rest of The Story...

The public has become outraged at the advertisers who use hidden marketing programs to take over computers for the purpose of marketing their products.

Symptoms:

The symptoms of Adware are uncontrollable popups, unwanted extra toolbars, and drastically slowed down computer performance that can result in freezes or lock up.

Most spyware detectors are concentrated on detecting adware because that is what is getting all the press…hence there are large profits to be made by anyone who writes an adware detection program, whether it works well or not. Who's to know?

There are no hard fast rules regarding how effective any software programs have to be. ***This means anyone can become a spyware detection company and charge you money for their "services".***

Unfortunately, because of this, there are many poorly written products out there that won't do you much good.

I attended an FTC Spyware Workshop in Washington last year and I fully expected to meet companies and groups who were 100% dedicated to stamping out this spyware. Wrong… while there were many against adware spyware, I found that a lot of the larger search engines, and some big Internet providers, were there with high priced lawyers defending adware, or at least attempting to inhibit new legislation from taking effect.

8. How To Detect And Remove Adware

I'm going to let you in on a little secret that many in this industry don't want you to know...

You DO NOT have to spend ANY money to detect and deal with Adware, because the best product out there is FREE…

Yes, I said FREE, and it amazes me how many people are spending their hard earned cash to detect Adware…but as I explained earlier, there is a lot of confusion regarding the subject of spyware.

Look what Andrew Brandt from PC World says about the subject:

Poor Defenders

Some anti-Spy Software companies use confusing ads, and our tests show their $20-$60 products are less effective than free competitors.
Andrew Brandt
From the December 2004 issue of PC World magazine

You've almost certainly encountered the ads: A dialog box pops up on your system bearing the message...Warning! Your computer may be infected with Spy Software, and suggesting that you scan your computer immediately.

Click it, and you often reach a Web site providing a "free Spy Software scanner" that finds all sorts of malware on your PC--and then offers to sell you software that will clean it all up

Should you buy these products?

Based on our tests, our opinion is no.

Following complaints from several PC World readers, we tested seven heavily advertised Spy Software-removal tools-- MyNetProtector, No Adware, Pal Spy Software Remover, SpyAssault, SpyBlocks, Spy Software Stormer, and XoftSpy…

and found that none were as effective as reputable free products such as SpyBot Search & Destroy.
Andrew Brandt PC World Magazine

Tip:
Wireless Can Be Dangerous: If you use a public system in airports, restaurants, etc., be sure you read up on the vulnerabilities before you open up your system. You can get more information here:
http://www.microsoft.com/athome/security/privacy/wirelessnetwork.mspx

Here's what some of the leading experts are saying about SpyBot

Spybot Search and Destroy is adaptable for both beginning and power users,

BRUCE STEWART CNET EDITOR.

Spybot: A powerful, easy to use tool for detecting, removing, and preventing adware…

WINPLANET.COM

So folks, don't waste your money on Adware Spyware detectors, listen to Andrew Brandt and get your FREE copy of SpyBot S&D from the website link below:

To download your FREE copy of SpyBot www.safer-networking.org

There are a lot of companies imitating SpyBot and tricking customers into thinking they are going to the SpyBot website when they are really going to a competitor who wants to cash in on SpyBot's popularity.

I got this directly from the SpyBot website:

SpyBot Customers Please BEWARE ! 17. January 2005

If you search for the keyword *Spybot* on Altavista or some other search engines, you'll got a bunch of *sponsored results*. One of them is *Spyware Doctor*, who seem to be agressively using our name *Spybot* to advertise their software. We receive a bunch of emails every week from people complaining to us and asking for a refund. After some mails we usually find out that those people believed they had bought *Spybot-S&D*, but actually got *Spyware Doctor*.

9. Careful What Browser You Surf With

Many people are unaware that they can get adware deposited on their computer simply by visiting a website with an insecure browser.

To help prevent new adware from making its way onto your machine when you surf the net, I recommend FireFox. FireFox is the latest FREE cutting-edge browser designed for simplicity and security:

To download your copy www.mozilla.org

10. Surveillance Spy Software: The Rest of The Story…

Uses And Misuses

Surveillance Spy Software, in my opinion, is by far the most dangerous…and hard to detect of all computer monitoring type spy products.

There are what some consider legitimate uses for Surveillance Spy Software. These include watching a child's Internet activity, monitoring employees while in a work environment, or just to see if anyone is illegally using your computer when you're not there.

Unfortunately, this type of spyware is often used unethically and even illegally by those who want to steal sensitive or private information from you or your business, without ever being caught, or are just curious as to what the heck you do on your computer for all those hours.

Tip:
Never Give Away Your Old Computer: I'm not being stingy here, but whether you know it or not, your old computer hard drive has a record of everything you've ever done on it, even if you put all that data into the trash bin. It's so easy for someone to retrieve information from your old hard drive, even if it has crashed and been considered unfixable.

Surveillance Spyware can be broken down into four main sub categories:

- **Keyloggers**, which record keystrokes like a hardware keylogger, but without a physical device.
- **Email Redirectors**, which silently duplicate all incoming and outgoing messages to a third party.
- **Chat Loggers** and **URL Recorders**, which will monitor popular instant messaging programs such as AIM and Yahoo Messenger, regular IRC chat clients and web browsers. All communications and web site visits are recorded and sent back to the intruder.
- **Screen Recorders,** which silently take snapshots of your entire desktop screen and everything you are doing, and then package it up as a slide show for the intruder to view. Screen recorders can also email or upload these recordings for remote access.

Surveillance Spy Software can be misused for

- **Spousal Spying**
- **Financial Spying**
- **Blackmail**
- **Identity Theft**
- **Corporate Espionage**
- **Stalking**

Anything anyone wants to find out about you or your business can now be easily obtained by capturing and recording your computer usage with Surveillance Spy Software…

One of the leading Surveillance Spy Software companies is Spector Soft - www.nospyzone.com/ss Spector has openly acknowledged that a large part of their sales are from spouses who spy on their mates.

Tip:
Password Protect Your Computer: Anyone who can access your computer can easily install a software keylogger and retrieve sensitive information.

11. How To Detect & Remove Surveillance Spy Software

Most software companies who manufacture and sell Surveillance Spy Software are making very good money. They can afford to have top-notch techs whose main job is to make their spy products undetectable to computer users. This makes it very difficult to spot if someone has decided to use it against you.

So what can you do to find out if you're being snooped on?

The only product I've found **made specifically to detect and remove Surveillance Spy Software** is from a company called SpyCop:

Download your copy of SpyCop from www.spycop.com/index1

Here's what some of the leading experts in the industry are saying about SpyCop:

"SpyCop... found a trace of SpectorSoft's Eblaster keylogger on my system that Spy Sweeper and Norton AntiVirus failed to notice"

EDWARD C. BAIG PERSONAL TECH WRITER USA TODAY

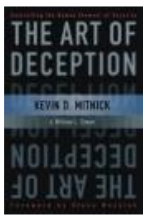
"The best I've seen so far is SpyCop. It scours your system, looking for secret keystroke-logging software."

JOHN DVORAK CONTRIBUTING EDITOR, PC MAGAZINE

If you're on the receiving end of a snooping program, wouldn't you want to know? SpyCop can ferret out hidden spy programs…

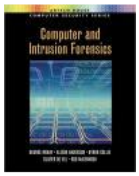
KIM KOMANDO THE KIM KOMANDO SHOW

BOOKS THAT RECOMMEND SPYCOP:



The Art of Deception:
Controlling the Human Element of Security
by Kevin D. Mitnick

Microsoft Encyclopedia of Security
by Mitch Tulloch (Paperback)



Computer and Intrusion Forensics
by George Mohay

Additional Resources: **Secrets of Computer Espionage: Tactics and Countermeasures** by Joel McNamara, **Steal This Computer Book 3: What They Won't Tell You About the Internet** by Wallace Wang, **Privacy Tactics** by Scott Germaise, **Home Networking Bible** by Sue Plumley, **Absolute PC Security and Privacy** by Michael Miller

12. Four Easy Steps To Spy Proofing Your Computer

1. Check for hardware keyloggers attached to the keyboard input.
2. Download your copy of SpyBot from www.safer-networking.org
3. Download your copy of SpyCop www.spycop.com/index1
4. Download your copy of FireFox browser www.mozilla.org

Synopsis:

I want to thank you for taking time to read this report. I hope it has been beneficial to you. Please feel free to pass this report around or use it on your website, or your ezines. All I ask is that you print this report in it's entirety.

Safe Surfing,

Elizabeth

Elizabeth Ward, Author
Web - www.nospyzone.com
Email - ward@nospyzone.com