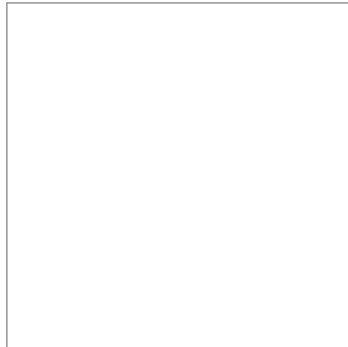**Special Paid**

Report by

[Barbara Ling](#)

Easily Protect Your Computer Online

Some quick easy ways to ensure your computer is protected from baddies

less desirable than shower scum

By Barbara Ling

Introduction

It's everyone's worst nightmare. You download what looks to be a respectable software from the Internet… perhaps a screensaver, a toolbar, a game, etc. But what you're unaware of is while your intended download gets installed, **other extremely undesirable products get installed on your computer as well**.

And these products are dedicated towards popping up porn advertisements, resetting your default browser destination to some place you'd rather not go, and otherwise causing bunches of problems to your online work and weight loss research.

It's frustrating in the extreme. I should know – awhile back I was traveling on the road and needed to use the hotel's computer. Imagine my dismay when I discovered no less than 17 spyware and mal-ware applications clinging to its innards!

By Barbara Ling

After speaking with the staff, I agreed to fix their computer in the wee hours of the morning. It took several hours, but eventually success was obtained!

The good news is that virtually every adware/malware problem you encounter online can be fixed. Not only that, but you can probably uncover step-by-step instructions on how to do so as well! And that's what you'll learn in this special report.

Remember, it's truly the wild wild west out there on the Internet…and while searching for marketing or make money or "what have you" resources, you might fall foul of spyware and malware and other icky things. But not to fear – read onwards!

Quick Easy Ways To Decrease Being Attacked

Follow these instructions to make your life much much easier.

By Barbara Ling

➤ Research potential downloads.

If you want to install a new program, go to Google first and search on

Program name spyware

For example, consider Hotbar, a way to customize your toolbars.   Look what the following search reveals:

http://www.google.com/search?q=hotbar+spyware

➤ Always read the Terms and Conditions.

Prior to installing new software, you might quite surprised to find what else it does. Refer to

http://news.com.com/2009-1023-885144.html

It includes:

…***Virginia Watson unwittingly authorized a company she'd never heard of to install software that would help turn her computer into part of a brand-new network.***

The software, from Brilliant Digital Entertainment, came with

By Barbara Ling

the popular Kazaa file-swapping program. But the 65-year-old Massachusetts resident--who has a law degree--didn't read Kazaa's 2,644-word "terms of service" contract, which stated that Brilliant might tap the "unused computing power and storage space" of Watson's computer.

And don't forget about MagicJack's EULA says it will spy on you and force you into arbitration – *"You also understand and agree that use of the magicJack device and Software will include advertisements and that these advertisements are necessary for the magicJack device to work ... Our computers may analyze the phone numbers you call in order to improve the relevance of the ads".*

Delightful.

Make certain you have updated all spyware/malware/adware definitions.

You can download the free spyware removal program Ad-aware . However,

By Barbara Ling

you might also want to consider eWido at http://www.ewido.net/en/ (now part of AVG). The demo is free and my gosh, it's effective – it was the only commercial tool I tried that actually was able to remove Nail.exe . The download is found here.

 Do NOT open any attachments in your email.

Many malwares and viruses get transmitted via email in the guise of greeting cards, resumes and the like. Not only that, but these viruses can spoof your friends' names via your addressbook (and send out email in YOUR name to your friends that contain the same virus). http://antivirus.about.com/cs/emailviruses/ will give you plenty of resources to help guard against that:

http://www.gfi.com/emailsecurity test/

will allow you to test out your email security.

This is a good thing indeed.

By Barbara Ling

➤ *NEVER click on "Your Computer Has Spyware!" ads.*

Have you ever been surfing along, happy as a clam, and all of a sudden been hit by ads that claim your computer has spyware?

NEVER EVER EVER EVER EVER EVER EVER download whatever is being offered!

Why, I hear you ask?

Because chances are...those are FAKE scanners/spyware-remover programs!

http://www.facebook.com/topic.php?uid=121834767645&topic=10228

http://helpdesk.coloradocollege.edu/index.php/tips-and-how-to/protect-your-computer/protect-your-computer-from-spyware-adware-malware/fake-anti-spyware-programs/

has more information on them.

Want up-to-date information on fake antivirus/scanning tools? Check out this search:

site:tech-linkblog.com fake (antivirus | scanning)

By Barbara Ling

Great information is found there, including explanations as to HOW scammers can penetrate your defenses.

And oh yes, here are some **useful video tutorials** for removing both those program types and other spyware infections.

http://www.youtube.com/watch?v=5ewvssLTxEg

http://www.youtube.com/watch?v=d30hQFcu8Hk

Make certain you have a firewall.

Firewalls protect you against viruses and hackers online. You can grab a free one from ZoneAlarm.

The above are some quick and easy ways to protect yourself. But what do you do if you already are infected? It's time for:

Step 1.) Find the process name.

If you're already running a firewall, you'll probably be prompted that a certain program is asking for permission to access the Internet. Find the name of that

By Barbara Ling

process, and then search for it on Google coupled with the keyword "remove".

For example, when I was fixing the hotel computer I saw repeatedly that the program "Nail.exe" was trying to do something (anything!). Searching for

http://www.google.com/search?q=nail.exe+remove

provided me with excellent results.

Another way to check the process name is to do the three fingered salute (<control><alt><delete>) and choose

"**Task Manager**". You can then see process names in the left hand column.

Step 2.) Look for word clues

If you don't recognize anything, look for common clues. Does your computer always try to access a certain destination online? Do you see a trademark like "CoolWebSearch"? Look what searching for coolwebsearch reveals online:

http://www.google.com/search?q=coolwebsearch

Now try that with the added keyword "remove":

By Barbara Ling

http://www.google.com/search?q=coolwebsearch+remove

Coolwebsearch, by the way, is extremely difficult to remove. However, there's a great free tool online that you can use that does it admirably called CWShredder and is available at http://free.antivirus.com/cwshredder/ .

Searching on word clues and process names, coupled with the keyword "remove", is a very effective method in learning how to remove just about any kind of spyware.

Step 3.) Ask for help

There are lots of forums online that are dedicated towards helping people rid themselves of spyware. They include:

http://www.spywareinfoforum.com/

http://pcpitstop.invisionzone.com/index.php?showforum=9

http://spywarewarrior.com/index.php

http://forums.majorgeeks.com/forumdisplay.php?f=35

http://www.daniweb.com/techtalkforums/forum64.html

By Barbara Ling

http://forums.cnet.com/5204-6132_102-0.html?forumID=32

http://forums.mcafeehelp.com

http://www.bleepingcomputer.com/forums/forum22.html

When in doubt, the people who frequent these forums really come through! The help they offer is awesome.

Step 4 – When you remove spyware, make sure…

Have you ever encountered the problem of the automatically reappearing spyware?

It's frustrating beyond belief! That's why prior to removing spyware, you should boot into Safe Mode (that inhibits the re-creation of it). You can boot into Safe Mode by pressing F8 during your bootup. Explicit instructions are found at http://www.bleepingcomputer.com/tutorials/tutorial61.html

Step 5 – When browsing on the Internet…

I know that many people use Internet Explorer. Apparently, however, you must continuously keep up with the patches to

ensure you don't get hit with malware when browsing online.

The latest security patches for Microsoft products are found [here on this page](#).

Alternatively, you can use Mozilla Firefox at http://www.getfirefox.com . While not indestructible, it does appear to have far better safety features included.

Resources for learning more about Internet security include:

- http://netsecurity.about.com/

- https://www.grc.com/x/ne.dll?bh0bkyd2

- http://vil.mcafee.com

and free virus scans can be found at

- http://housecall.trendmicro.com/

- http://www.pandasoftware.com/activescan

- http://security.symantec.com

- http://www.kaspersky.com/virusscanner

By Barbara Ling

Want to keep on the cutting edge? http://www.virtual-coach.com

Enjoying this information?

Feel free to follow me on ***Twitter***

and/or join my network at Facebook!

What You Should Do Now

I certainly hope these ideas that I have revealed have whetted your interest in protecting yourself online!

When you're finished reading this report, STOP! Do not pass GO, do not collect $200…**but DO make certain you have the latest updates to your browser, know how to fix spyware and malware on your computer, and protect yourself as much as possible.**
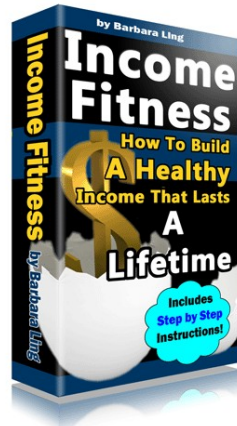
Your income's fitness will thank you for it.

☺

ThankYouVeryMuch!

Sincerely,

Barbara

By Barbara Ling

PS – Speaking about Income Fitness, have you seen the latest at

PPS – Speaking about the Internet, got questions about being profitable online or just want some helpful support and cheering on? Check out our Virtual Coach Income Fitness forums - a friendlier community for finding what works for YOU just doesn't exist. Stop by today!

Income Fitness will constantly evolve as the days go by….be sure to check out the latest updates!

By Barbara Ling