

KEEPING YOUR COMPUTER HEALTHY

**Get the Cyber-criminals Out
Protect your Money and Identity**



LINDA LINDQUIST
Certified Malware Removal Specialist

Keeping Your Computer Healthy

GET THE CYBER CRIMINALS OUT
PROTECT YOUR MONEY AND IDENTITY

Linda Lindquist
Certified Malware Removal Specialist

Copyright © 2017 by Linda Lindquist.

All rights reserved. No part of this publication may be reproduced, distributed or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, send to pccoach33@gmail.com.

Computer Security Training

Learn WHAT TO DO and WHAT NOT TO DO

In appreciation of your interest in *keeping your computer healthy*, you qualify for a home study course designed to make you aware of how the cyber-criminals trick you into giving up your identity and money.

Learn about phishing, scams, ransomware and how to protect yourself and your computer from hackers and cyber-criminals. Think you are immune? 98% of computers have malware and most people do not realize it.

Sign up to get a link and password to access the free security training course.

[CLICK HERE to get the Free Training](#)

PC Security Course

KnowBe4
Human error. Conquered.

I am indebted to *Self-Publishing School* for providing training and support on how to write and launch a book. If you think you have a book in you, check out the [Self-Publishing School](#).

NOW IT'S YOUR TURN

**Discover the EXACT 3-step blueprint
you need to become
a bestselling author in 3 months.**

Self-Publishing School helped me, and now I
want them to help you
with this [**FREE VIDEO SERIES!**](#)

Even if you're busy, bad at writing, or don't
know where to start, you CAN write a bestseller
and build your best life.

With tools and experience across a variety of
niches and professions,
Self-Publishing School is the only resource you
need to take your book to the finish line!

DON'T WAIT

Watch this [**FREE VIDEO SERIES**](#) now, and
Say "YES" to becoming a bestseller:

INTRODUCTION

Keeping Your Computer Healthy

With a lifetime of computer experience, and nine years of working on over 7,000 Windows computers, I have developed a process to make computers healthy and fast again.

Unhealthy computers are slow, infected with malware, adware and viruses, out-of-date, unpredictable, and often scare their owners into taking unwise actions, such as paying for unknown people to remotely come into their computers.

I use a set of tools that are effective at removing malware, adware and viruses. I recommend an anti-malware program that stops infections from entering, a program that blocks those annoying advertisements, software to keep third party software updated automatically, and a cloud-based backup service.

Because my procedure and recommended software are effective in returning computers to health, I wanted to pass on my knowledge to IT technicians and computer users alike. If, as a computer user, you feel uncomfortable following the steps in this guide, by all means call your IT technician.

Let's get started. What follows are sample chapters on ways to find and remove infections, understand how they get into your computer in the first place, and proactive steps to keep your computer healthy. Taken all together, they will help you restore your computer to a healthy, pleasant experience again.

[Keeping Your Computer Healthy](#) is available for purchase on Amazon.com. (click the link above).

Chapter 1

SYMPTOMS OF AN UNHEALTHY COMPUTER

"**H**ELP! My Computer is SO SLO-O-OW!"
"HELP! I cannot get my e-mail. My homepage disappeared??"

"HELP! Those new toolbars take up too much space."

"HELP! I keep getting pop-ups!"

"HELP! I can't connect to the Internet."

"HELP! What are these new icons on my desktop?"

"HELP! Microsoft pop-ups are saying that my computer has serious problems."

You may notice that your computer is running slow, the fan is running a lot (noisy), your browser homepage disappeared, or new browser toolbars or desktop icons have appeared. If any of these things occur, then suspect malware. If you have any of the above symptoms, you have an unhealthy computer.

These are the cries for help that bring me and my expertise into people's homes and small businesses every day.

The causes and solutions are various, and these symptoms often reveal that Cyber-criminals have invaded your computer.

This chapter shows details on how to recognize that your computer is infected by malware.

Chapter 2

FINDING AND REMOVING INFECTIONS

"HELP! My computer is slow and has pop-ups." I often hear that "My computer is getting old. It is running slow, just like me." (From my senior citizen clients) My response is, "It is probably infected. 98% of the computers I service are. I can help you detect and remove the Malware and return your computer to health."

Removing malicious software (a.k.a. Malware), viruses, and adware is usually the first step toward speeding up a slow computer.

I use a set of software tools that have proven effective in detecting and removing these infections:

- 1) **AdwCleaner** - I first check for adware infections because the tool runs quickly and it finds threats. To clean up the adware, it closes all open windows and requires a restart to remove what it has detected. I get the tool from <https://www.malwarebytes.com/adwcleaner/>
- 2) **Malwarebytes** – download this program from <https://www.malwarebytes.com/>. This diagnostic tool has a robust database of the 'bad guys'. I configure the setting to detect root kits and treat anything it finds as malware. My procedure is to UPDATE its database, SCAN, REMOVE SELECTED (first see that all items are checked), and

RESTART. Although the scan takes a while, the Malware and Viruses are gone.

3) **Emsisoft Emergency Kit** - download this tool from <https://www.emsisoft.com/en/software/eeek/>. They have a very robust database of 'bad guys'. Install, join the network, enable PUPs, do a MALWARE SCAN and Quarantine anything it finds. Their scans are fast and this tool finds and removes Malware and Viruses.

4) **CCleaner** - download this tool from <https://www.piriform.com/ccleaner/download>, and use the Tools tab to check for installed Programs, Startups, and Browser Add-ons that look suspicious. The tool has functions to uninstall programs, disable Windows start-ups, disable scheduled tasks, and disable browser add-ons and extensions.

In Summary:

- Malware, Viruses and Adware are often the root cause of a slow computer.
- There are tools that find and remove these infections: **AdwCleaner**, **Malwarebytes**, **Emsisoft Emergency Kit**, and **CCleaner**.

Chapter 3

HOW CYBER-CRIMINALS ENTER YOUR PC

Cyper-criminals have discovered many devious ways to infect your computer:

Out-of-date software - vulnerabilities that may have already been fixed by the vendor

Attachments in e-mails - e-mail that entices you to open malware infected attachments or links

Bogus search engines - search engines designed to send you to infected links

Browser add-ons - add-ons to your browser that display infected toolbars

Phishing - bogus e-mail or websites designed to look like they are from a reputable company

Scams - phone calls, pop-ups, etc. designed to appeal to your emotions of fear or greed

Malvertising - malicious advertisements that download malicious code from reputable sites

Hacked address books - this is how the Cyber-criminals get valid addresses to spread their malware

Your behaviors - advice about what not to do

Read more about these in this chapter.

Chapter 4

PROACTIVELY PROTECTING YOUR COMPUTER

After the infections are removed from your computer, protect the continued health of your computer by paying attention to the following:

- Anti-Virus / Anti-Malware Program
- Keep Windows up-to-date
- Keep Software up-to-date
- Declutter temporary files
- Manage your Passwords
- Back up your Data Files
- Have Storm Protection
- Advertising Blocking
- Firewall
- Optimize
- Internet Speed

Read this chapter to find out what to do to keep your computer healthy.

References

SOFTWARE TOOLKIT

What follows is the toolkit that I have found to be useful to remove Malware and keep your computer healthy. I so believe in the effectiveness of many of these products that I have become an authorized reseller (*).

ADGUARD (*)

<https://adguard.com/en/welcome.html>

This software blocks advertisements to speed up the experience of the internet and blocks Malvertising on websites to protect your computer.

AdwCleaner

<https://www.malwarebytes.com/adwcleaner/>

This scanner finds and removes adware infections.

CarrollNet Backup Services (*)

This service provides daily backup of your files to the cloud for individual consumer computers. They also have a service for businesses that provides redundant Backup to a server located at your business.

CCleaner

<https://www.piriform.com/ccleaner/download>

This tool declutters your disk by removing temporary files that will never be used again. It also allows you to see and disable startup program and browser add-ons, as well as uninstall programs.

Emsisoft Emergency Kit

<https://www.emsisoft.com/en/software/EEK/>

I use this one-time scanner to find and quarantine malicious software (malware) and viruses. The scan is fast and it uses a very robust database of known infections.

Emsisoft Anti-Malware (*)

<https://www.emsisoft.com/en/software/antimalware/>

This anti-virus / anti-malware software provides real-time and scheduled scanning to find and quarantine infections. Due to its very robust database of know infections, it stops malware cold! It is effective for both consumers and businesses.

Heimdal Free

<https://heimdalsecurity.com/en/products/heimdal-free>

This patch management software automatically keeps your third-party (non-Microsoft) software up-to-date. Out of date software is vulnerable to Cyber-criminal attacks.

Heimdal Pro (*)

<https://heimdalsecurity.com/en/products/heimdal-pro>

This is a security addition to your anti-virus / anti-malware software. It blocks ransomware, phishing attacks, traffic filtering, zero-day attacks and includes their patch management software.

Hitman Pro

<http://www.surfright.nl/en/hitmanpro>

This software is a second look anti-virus, anti-malware detection and removal tool.

Malwarebytes (*)

<https://www.malwarebytes.com/>

This tool finds and quarantines malicious software (malware). It has been a go-to tool in my toolbox.

Sticky Password (*)

<https://www.stickypassword.com/>

This password management software remembers and fills in your passwords; you only have to remember one password.

TDSS Killer

<http://usa.kaspersky.com/downloads/TDSSKiller>

This special purpose tool detects and removes root kit infections that compromise system functions.

PROCEDURE

I. Observe Malware?

Yes? => Run quick tools to remove malware: 30-60 minutes

AdwCleaner - Download, Run, Scan, Clean, Restart
(10-15 minutes)

Emsisoft Emergency Kit - Download, Install, Update,
Scan, Quarantine, Restart (15-30 minutes)

Manually Disable Browser Add-ons - (15 minutes)

II. Still see problems? (Optional)

Yes? => Run additional specialized tools: 45 – 75 minutes

Malwarebytes - Download, Install, Update, Scan,
Quarantine, Restart (30 - 60 minutes)

TDSS Killer - If suspect root kits, Download, Run,
Clean (15 minutes)

III. Install software for computer health:

60 - 90 minutes (after malware removed)

Emsisoft Anti-Malware - Download, Install, Update, Quick Scan, License, Set up scheduled Malware Scan (15 - 30 minutes)

AdGuard - Download, Install, License (15 minutes)

CCleaner - Download, Install, Configure, Analyze, Run Cleaner (15 minutes)

Heimdal Free - Download, Install, Configure Patch Management, it does the rest (15 minutes)

Backup files: manual backup to flash drive or **CarrollNet Backup Services** if many and/or critical files are not being backed up (depends on how many files)

Sticky Password - Install, Configure - if person forgets their passwords (15 minutes)

See the Software Toolkit Chapter for links to download the software tools.

ABOUT LINDA LINDQUIST



Keeping Your Computer Healthy is based on the practical experience of removing malicious software from more than 7000 computers over the past ten years. If your computer is running very slow, has unexpected advertisements, browser toolbars that you did not install, changed browser home pages, or annoying pop-ups that scare you or ask you to call a Windows tech, then you need to read this book! The author is a Certified Malware Removal Specialist who is sharing her secrets to removing the malware and putting safeguards in place to keep your computer healthy. She has been in the computer industry since 1969.