

\$12.95 USD

Phil Covington's

Reduce
Inbox Spam
To Almost
Zero!

How To

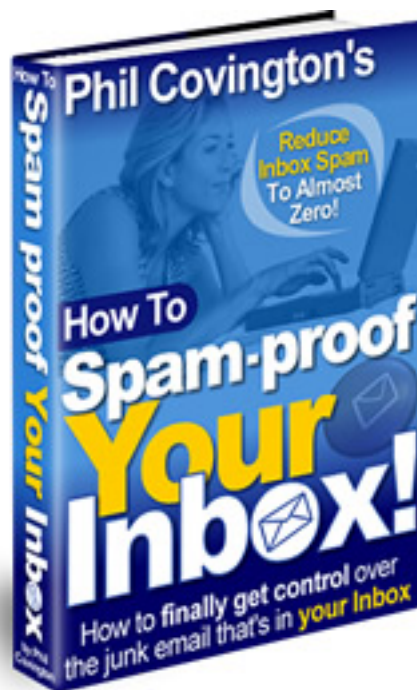
Spam-proof Your Inbox!

How to finally get control over
the junk email that's in **your Inbox**

Phil Covington's How To Spam-proof Your Inbox!

From the bestselling author of
Computers — The Plain English Guide
Almost everything you need to know about computers, even if you don't
know ANYTHING about computers

Reduce Inbox Spam To Almost Zero!



This is NOT a Free eBook

Copyright © 2003 Phillip A. Covington & GRPMAX, LLC
All Rights Reserved

Reproduction or translation of any part of this work by any means, electronic or mechanical, including photocopying, beyond that permitted by the Copyright Law, without the permission of the publisher, is unlawful.

[GRPMAX, LLC](http://www.grpmax.com) 1737 Spring Arbor Road #105 Jackson, MI 49203-2701
Phone: 517-841-0841 Fax: 517-841-0842 Email: Info@grpmax.com

INTRODUCTION.....	6
WHAT MAKES THE INFORMATION IN THIS eBook DIFFERENT?.....	6
IF YOU ARE IN A HURRY!.....	7
IF YOU ARE IN AN EVEN BIGGER HURRY!.....	7
IT'S NOT YOUR FAULT!	14
THE GOOD, THE BAD, AND THE UGLY!.....	15
THE CURRENT STATE OF SPAM	15
YOU HAVE THREE OPTIONS TO STOP SPAM	16
WHY MOST ANTI-SPAM SOFTWARE DOESN'T WORK.....	16
ARE THERE ANY ANTI-SPAM TECHNOLOGIES THAT DO WORK?	17
CAPTCHA	17
SAFELIST OR WHITELIST	20
WHY ANTI-SPAM LAWS ARE LARGELY INEFFECTIVE.....	21
DEVELOPING YOUR OWN PERSONAL GAME-PLAN	21
HOW PEOPLE WHO SEND SPAM GET YOUR EMAIL ADDRESS.....	22
NEVER POST YOUR "REAL" EMAIL ADDRESS TO A PUBLIC NEWSGROUP OR FORUM ..	23
AVOID POSTING YOUR EMAIL ADDRESS ON YOUR WEBSITE OR OTHERS (IF POSSIBLE)	
.....	23
3 BOMBSHELLS THAT YOU PROBABLY DIDN'T KNOW	24
CHECKING EMAIL OFTEN IS YOUR #1 DEFENSE AGAINST SPAM!	24
SOFTWARE FIREWALLS CAN BE MORE USEFUL THAN ANTI-SPAM SOFTWARE!	25
"FREE" SOFTWARE (FREWARE/SHAREWARE, ETC.) OFTEN BRINGS SPAM!	26
AVOID SOFTWARE FROM COMPANIES THAT AREN'T "REPUTABLE"	26
HOW TO SPOT SPAM A MILE AWAY.....	27
WHY SPAM IS LIKE FORTUNE COOKIES	28
BACK TO FORTUNE COOKIES.....	29
TIMING, COINCIDENCE, AND JUST PLAIN LUCK!.....	30
RED ALERT IF YOU ARE ASKED TO VERIFY CREDIT CARD OR SOCIAL SECURITY	
NUMBERS!!!	31
HAVE YOU RECEIVED AN EMAIL THAT LOOKS LIKE ONE OF THESE?	32
MOVING FROM PREVENTION TO DEFENSE	33
WHY WEB-BASED EMAIL (LIKE YAHOO!) ALONE MAY NOT SOLVE YOUR PROBLEM...	33
TEMPORARY EMAIL ADDRESS & PICKUP SERVICES	34
USING SUBJECT LINE KEYWORDS TO SEPARATE CUSTOMER INQUIRIES FROM SPAM ...	36
USING THE 'NO SPAM' KEYWORD ON YOUR WEBSITE.....	36
USING THE "NO SPAM" KEYWORD WITH YOUR EMAIL PROGRAM	37
USING MORE THAN ONE EMAIL ADDRESS	79
EVERYONE SHOULD HAVE AT LEAST TWO EMAIL ADDRESSES!	79
USE WEB-BASED EMAIL TO PROTECT YOUR PRIVACY	79

USING MORE THAN ONE EMAIL ADDRESS AT WORK.....	80
USE VIRTUAL EMAIL ADDRESSES	81
USING YOUR EMAIL PROGRAM TO CREATE DISPOSABLE EMAIL ADDRESSES	81
EMAIL ALIASES ALLOW BETTER INDIVIDUAL CONTROL	82
WHAT IS A "VIRTUAL" EMAIL ACCOUNT?	82
HIDE YOUR EMAIL ADDRESS ON THE WEB	84
MANAGE YOUR INBOX AND EMAIL FOLDERS EFFECTIVELY	88
EMAIL SECURITY TIPS	89
THE #1 WAYS TO LET A SPY INTO YOUR COMPUTER.....	90
SAVVY USERS SHOULD OWN THEIR OWN DOMAIN NAMES	91
ANTI-SPAM SOFTWARE RECOMMENDATIONS	94
THE BEST ANTI-SPAM SOFTWARE FOR END USERS.....	95
A BRIEF WORD ABOUT ONLINE WEB-BASED ANTI-SPAM EMAIL SERVICES.....	97
THE BEST OF THE BIG WEB-BASED EMAIL SERVICES.....	98
THE ULTIMATE SOLUTION RESTS WITH THE INTERNET ITSELF.....	99
YOUR COMMENTS AND FEEDBACK ARE WELCOME!	100
APPENDIX A	101
HAVE YOU RECEIVED AN EMAIL THAT LOOKS LIKE ONE OF THESE?	101

Preface

This book that you've just purchased is worth far more than its cover price. It can literally be worth hundreds and even thousands of dollars because of the time, hassle, and lost email it will save you. I will quickly show you in simple, easy to understand, "Plain English" steps, how to finally get control over the junk email that's in your Inbox.

If you're frustrated by all of the unsolicited email that you keep receiving, you have come to the right place!

Are you ready to begin?

If so... Then let's get started on our way to Spam-proofing Your Inbox!

Introduction

Welcome,

Thank you for having the faith and confidence that we can introduce new ideas, methods and strategies that will be of use to you in finally being able to eliminate unsolicited email (Spam) from your Inbox.

The objective of this eBook is very specific, which is to show you...

How to be assured to the maximum degree possible that you WILL receive important emails that you are expecting and do wish to get, while at the same time reducing the number of unsolicited and unwanted emails or Spam that ends up in your Inbox to Almost Zero.

Before we begin, please allow me to share with you a little background about how we arrived at this place in time... If you are in a hurry, you may skip ahead by clicking [here](#).

What makes the information in this eBook different?

Most of the information provided here, and the tips and techniques that you'll be learning, will be of great benefit to you without you having to purchase any new software or services. That's one of the benefits that I am conveying to you, trying whenever possible to help you avoid unnecessary purchases so that you can avoid spending your money on software or services that either don't work very well, or simply aren't needed if you are armed with the right information.

Only where necessary I'll make various recommendations along the way about software or services that can help you achieve a better computing experience. If you would like to learn more about how I arrive at making product recommendations, and why you can count on them to be the best, you can learn more by reading the overview that you'll find on the Website of my new, just launched computer magazine. Click on the link below.

The overview is titled, "[What Makes Phil Covington's Best Different?](#)"

If You Are In A Hurry!

If you are in a hurry and short on time, then you might try first going through this eBook by focusing on the sections of text that are **highlighted**. You won't get all of the information that way, but you will pick up the most important points and tips.

Then, when you have more time, you can go back and read through the remaining text at your leisure.

If You Are In An Even Bigger Hurry!

If you are in an even bigger hurry and even shorter on time, but you still want to know what is the single most effective step you can take that would be most effective right now, then start with the section on Anti-Spam Software Recommendations.

Be sure to read the entire software recommendations sections all the way through:

[Anti-Spam Software Recommendations](#)

[The Best Anti-Spam Software For End Users](#)

When you have more time then come back for more, perhaps focusing first on the sections of text that are **highlighted**, and then finally you can read through the remaining text at your leisure.

It's Not Your Fault!

The first thing that we need to clear up is this very important point: **The fact that you currently have a problem with a lot of unsolicited junk email and Spam in your Inbox is not your fault!**

In fact, many if not most of the computer problems that you might encounter are likely not to be your fault.

In most cases the blame rest squarely with poorly designed and implemented software, hardware, the nature of the Internet and network infrastructure itself, and, of course, those unscrupulous businesses and individuals who send you their Spam to begin with.

Unfortunately, many who work in the computer industry have a habit of blaming the users of their products when in many cases there is indeed a legitimate bug, design flaw, or other problem.

It is true that there *are* things that you *can* do, such as being careful about whom you give your email address and other information out to. And it is possible to learn such things as how to recognize when an email might contain a virus or other potentially harmful content. And, of course, you can and may have already installed software on your computer designed to do such things as stopping Spam or viruses, etc.

The problem is that even many of these programs either don't work well, can't be relied upon, require expertise the user doesn't have, or require frequent updates, etc.

Programs such as anti-virus software work reasonably well at stopping known threats, and even at stopping some email and other activity that is viewed as potentially suspected of containing a new unknown virus or threat. Anti-virus software is probably a good idea for the average computer user or network, and is worth the expense and maintenance of getting the required updates.

The same cannot be said of currently available anti-Spam technologies.

Let's take a brief look at the current state of the Spam problem, anti-Spam technologies, and why they have so far proven to be problematic.

The Good, The Bad, And The Ugly!

The “Good” is that by utilizing the information in this eBook you will be able to get your Spam problem under control.

The “Bad” is that as the old saying goes, “all good things take time,” so you will have to expend some effort. That effort, however, is certainly better than the prospect of continuing to simply have Spam flood into your Inbox.

The “Ugly” is that Spam truly is a nasty problem. Spam is forced upon you by the unscrupulous senders of unsolicited junk email. It’s a problem that you didn’t ask for. The senders of Spam don’t care about the value of your time, or the negative and costly effects of their actions. Many of the biggest offenders are in fact lawbreakers, in that they are violating existing laws against sending Spam, or emails containing certain types of offers.

It is also “Ugly” that law-abiding citizens like you and I have to pay to address a problem that people like the above create for us. No one should have to install a security system on their home or car, for instance, but not only are security systems now commonplace in homes, cars, and offices, but even churches, of all places, now need security systems. So, yes, it’s ugly. But in the same way that millions of people pay a price for physical security and peace of mind, we also have to pay a price for electronic security, peace of mind, and privacy.

At least this eBook can show you how to pay the least in time and dollars to get the maximum possible benefit in reducing the Spam hitting your Inbox.

The Current State Of Spam

Spam (unsolicited and unwanted email and email advertising) has grown to become a multi-billion dollar problem and a major headache for businesses and home computer users alike.

According to almost all estimates and surveys **Spam now accounts for as much as 80% of the email arriving in many people’s Inboxes.** The estimates vary from as low as 50% for home computer users to the 80% figure for ISPs (Internet Service Providers) and other major business relying or based upon the Internet.

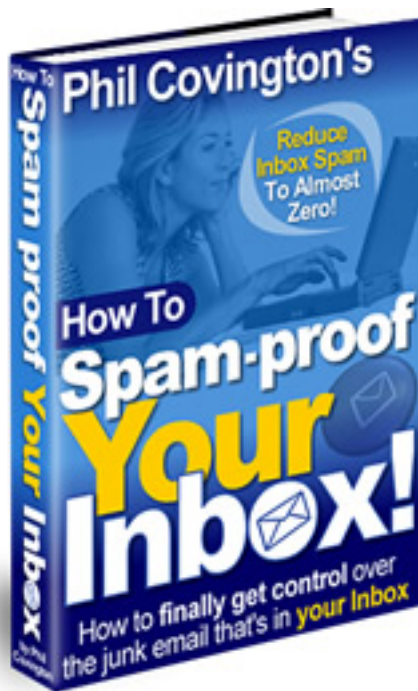
Besides being annoying, this makes it more difficult to sort through your Inbox to get to email that you really want. It also clogs up corporate networks and hard

Is Your Computer Spying On You?

From the bestselling author of
Computers — The Plain English Guide
Almost everything you need to know about computers, even if you don't
know ANYTHING about computers

and...

How To Spam-proof Your Inbox!



Free Offer Does Not Mean Free To Copy!

Copyright © 2003 Phillip A. Covington & GRPMAX, LLC
All Rights Reserved

Reproduction or translation of any part of this work by any means, electronic or mechanical, including photocopying, beyond that permitted by the Copyright Law, without the permission of the publisher, is unlawful.

GRPMAX, LLC 1737 Spring Arbor Road #105 Jackson, MI 49203-2701
Phone: 517-841-0841 Fax: 517-841-0842 Email: Info@grpmax.com

INTRODUCTION.....	6
WHAT MAKES THE INFORMATION IN THIS eBook DIFFERENT?.....	6
IF YOU ARE IN A HURRY!.....	7
IF YOU ARE IN AN EVEN BIGGER HURRY!.....	7
YOUR COMPUTER IS ALMOST SURELY SPYING ON YOU!.....	8
THE THREE MAJOR TYPES OF COMPUTER SPIES	8
INTERNAL SPYING.....	8
NEFARIOUS OR ILLEGAL SPYING	9
LEGITIMATE USES.....	10
HAS YOUR COMPUTER BEEN HIJACKED?	11
DENIAL OF SERVICE ATTACK.....	11
DRIVE-BY DOWNLOADS (NOT LEGITIMATE!).....	12
MARKETING RELATED SPYING	12
COOKIES: THEY ARE WATCHING YOU!	12
BUT WHAT ABOUT YOUR BROWSER'S COOKIE MANAGEMENT FEATURES?	13
ERASE OR TURN OFF COOKIES WHENEVER POSSIBLE.....	13
“FREE” SOFTWARE (FREWARE/SHAREWARE, ETC.) OFTEN BRINGS TROUBLE!.....	27
AVOID SOFTWARE FROM COMPANIES THAT AREN'T "REPUTABLE"	28
ALWAYS READ THE FINE PRINT!.....	28
CHECK YOUR SOFTWARE'S CONFIGURATION SETTINGS	29
THE DIFFERENCE BETWEEN ADWARE OR SPYWARE AND A COMPUTER VIRUS	29
WHAT TO DO IF YOU SUSPECT ADWARE OR SPYWARE	30
PERSONAL FIREWALL SOFTWARE SHOULD BE #1 ON YOUR LIST!.....	30
WHICH IS THE BEST PERSONAL FIREWALL SOFTWARE FOR YOU?.....	32
WHAT IF YOU ALREADY HAVE A FIREWALL?	32
FIREWALLS BUILT INTO DSL/CABLE MODEMS, ROUTERS, SWITCHES, & WIRELESS ACCESS POINTS.....	33
THE #1 PERSONAL FIREWALL SOFTWARE.....	33
YOU HAVE EVERYTHING TO LOSE AND EVERYTHING TO GAIN!!!.....	34
FIREWALL INSTALLATION AND CONFIGURATION TIPS	35
USING YOUR FIREWALL CORRECTLY.....	35
USING YOUR PROGRAMS WITH YOUR FIREWALL....	37
BLOCKING PROGRAM ACCESS	40
USING YOUR FIREWALL TO STOP SPYING ATTEMPTS	41
BE ESPECIALLY CAUTIOUS ABOUT ALERTS FROM UNKNOWN PROGRAMS.....	46
WHEN MULTIPLE ALERTS ARE OK	46

ADWARE AND SPYWARE REMOVAL SOFTWARE.....	48
THE #1 WAYS (NOT) TO LET A SPY INTO YOUR COMPUTER.....	49
EMAIL SECURITY TIPS	50
TRY TO NEVER OPEN YOUR EMAIL WHILE ONLINE!.....	51
DON'T USE THE "PREVIEW" FEATURE IF YOU CARE ABOUT SECURITY!	55
SPY GRAPHICS (WEB BUG; WEB BEACON; CLEAR GIF; SPAM BEACON).....	68
WEB BUGS CAN TRACK AN EMAIL THROUGH MANY PEOPLE.....	69
A WEB BUG DEMONSTRATION	69
TIPS FOR PROTECTING YOURSELF FROM WEB BUGS.....	70
HOTBARS AND TOOLBARS – OPEN DOOR TO YOUR PC?	70
HOW TO TEST YOUR COMPUTER'S SECURITY	71
MORE COMPREHENSIVE INTERNET SECURITY TESTS.....	72
USE THIS — FOR WHEN BAD THINGS HAPPEN TO GOOD COMPUTERS!	73
ANONYMOUS SERVICES AND PRODUCTS	76
KNOWLEDGE IS POWER (BUT WHAT IF SOMEONE ELSE HAS YOURS?).	76
ERASE YOUR HARD DRIVE, REALLY!.....	78
YOUR COMPUTER'S RESTORE DISK DOESN'T ERASE YOUR HARD DRIVE.....	78
WHAT REALLY HAPPENS WHEN YOU "ERASE" YOUR DATA	79
OLD COMPUTERS AND HARD DRIVES ROUTINELY CONTAIN SENSITIVE DATA	79
HOW TO PROPERLY ERASE AND SANITIZE YOUR HARD DRIVE.....	80
ERASING AN ENTIRE HARD DRIVE	80
SECURELY ERASING DATA WHILE STILL USING YOUR COMPUTER.....	81
YOUR COMMENTS AND FEEDBACK ARE WELCOME!	83

Preface

This book that you've just purchased is worth far more than its cover price. It can literally be worth hundreds and even thousands of dollars because of the time and hassle it can save you. It will help safeguard you from the potential loss or compromise of the personal information on your computer.

I will quickly show you in simple, easy to understand, "Plain English" steps, how to determine if your computer has been spying on you, what to do to stop it, and how to prevent it from happening in the future.

If you bought this eBook just out of curiosity, but didn't really think you had a need for it, prepare to be surprised when you find out just how many ways that your computer probably has been spying on you!

Are you ready to begin?

If so... Then let's get started on our way to actually learning the answer to our question, "Is Your Computer Spying On You?"

Introduction

Welcome,

Thank you for having the faith and confidence that we can introduce new ideas, methods and strategies that will be of use to you in your efforts to make your computing experience secure, private, and free of intrusion by unauthorized means.

The objective of this eBook is very specific, which is to show you...

How to be assured to the maximum degree possible that software does not exist on your computer that is spying on you without your knowledge, how to disable or remove any spy software that we do find, and how to secure your computer from intrusions and tracking via your Web browser, email, Internet, or other means in the future.

What makes the information in this eBook different?

Most of the information provided here, and the tips and techniques that you'll be learning, will be of great benefit to you without you having to purchase any new software or services. That's one of the benefits that I am conveying to you, trying whenever possible to help you avoid unnecessary purchases so that you can avoid spending your money on software or services that either don't work very well, or simply aren't needed if you are armed with the right information.

Only where necessary I'll make various recommendations along the way about software or services that can help you achieve a better computing experience. If you would like to learn more about how I arrive at making product recommendations, and why you can count on them to be the best, you can learn more by reading the overview that you'll find on the Website of my new, just launched computer magazine. Click on the link below.

The overview is titled, "[What Makes Phil Covington's Best Different?](#)"

If You Are In A Hurry!

If you are in a hurry and short on time, then you might try first going through this eBook by focusing on the sections of text that are **highlighted**. You won't get all of the information that way, but you will pick up the most important points and tips.

Then, when you have more time, you can go back and read through the remaining text at your leisure.

If You Are In An Even Bigger Hurry!

If you are in an even bigger hurry and even shorter on time, but you are concerned about the security of your computer and want to know what is the single most effective step you can take that would be most effective right now, then start with the section on using a personal software firewall.

Be sure to read the entire personal software firewall sections all the way through:

[A Personal Software Firewall Should Be #1 On Your List!](#)

[Which Is The Best Personal Firewall Software For You?](#)

When you have more time then come back for more, perhaps focusing first on the sections of text that are **highlighted**, and then finally you can read through the remaining text at your leisure.

Your Computer Is Almost Surely Spying On You!

The title of this special report is in the form of a question, "Is Your Computer Spying On You?" But for most computer users it's probably not a question at all. **If your computer is configured like those of more than 80% of computer users then the question is not, "is" your computer spying on you, but "how much is it spying on you?"**

If you are among the small percentage of people who have never accessed the Internet then your computer may be more secure than most. However, if you have ever browsed the Internet (the "Web"), participated in a newsgroup, or received email, then it is highly likely that your computer is spying on you.

If you have browsed the Internet and used email frequently then it is almost certain that your computer is spying on you.

If you have ever downloaded and installed software from the Internet (even if from a well known, reputable company) then it is highly likely that your computer is spying on you.

If you have ever downloaded "free" software, or even the trial versions of certain software packages, then there is a more than 90 percent chance that your computer is spying on you!

The Three Major Types Of Computer Spies

The kinds of spying that you are likely to be affected by fall into three main categories: internal, marketing related, and nefarious or illegal.

It's also important to point out that, except for the last category (nefarious or illegal) that most kinds of spying can be for either good or bad purposes, and can be attempted or conducted with or without your knowledge.

Internal Spying

Let's take internal spying as just one example. Many office workers are by now aware of the fact that **employers not only routinely monitor their computer activities, but can and often do monitor certain phone conversations as well.** Numerous court cases have made it clear that employers have this right. As just one example, it is entirely acceptable for an employer to monitor the Internet usage of its employees to ensure that they are not viewing or distributing

pornographic materials while on company premises. The same would apply to office gambling pools, etc.

There are many other legitimate ethical, business, and legal reasons for employers to be concerned about making sure that their computers aren't used for illegal or questionable purposes. So, while some employees may not like this form of "spying," it is legal, and courts have so far ruled that employers have the right to do so.

Another common example of internal spying is parents who wish to monitor the Internet activities of their children, for much the same reasons as just mentioned above. Some parents install such monitoring software on their children's computers with the children's knowledge, while others do so without their children being aware of the fact that their activities are being monitored. Either way, this also is considered an acceptable practice.

Things start to cross into the grey area when spying is conducted under other circumstances. For instance, some spouses suspicious that the other may be involved in pornography or having an affair install secret monitoring software to monitor his or her spouse's computer related activities. Is that ok? Of course, if the level of trust in a marriage has broken down to that level, that's an entirely different topic, and not the purpose of this report. But the point is, when is it ok for someone to use your computer to spy on you without your knowledge?

One important distinction in the above examples is that they all involve someone inside your home or office. Kids might not like it, for instance, if they know their parents are monitoring their Internet activities, but it's still ok. The same applies to employers and employees. A spouse being spied on without his or her knowledge moves things into the grey area, but it's still someone you know, and that probably has legitimate legal access to your computer.

Most would agree, however, that when it comes to someone from the outside (whom you may not even know) using your computer to spy on you without your knowledge, that's an entirely different matter.

Nefarious Or Illegal Spying

The last category, "Marketing Related Spying," is an example of circumstances where spying on you, even without your knowledge, may not always be for questionable or illegal purposes. However, in most cases, if someone is using your computer to spy on you without your knowledge, they are probably up to no good!

Everyday millions of unsuspecting computer users open emails or browse Websites that install a hidden piece of computer code or software that spies on