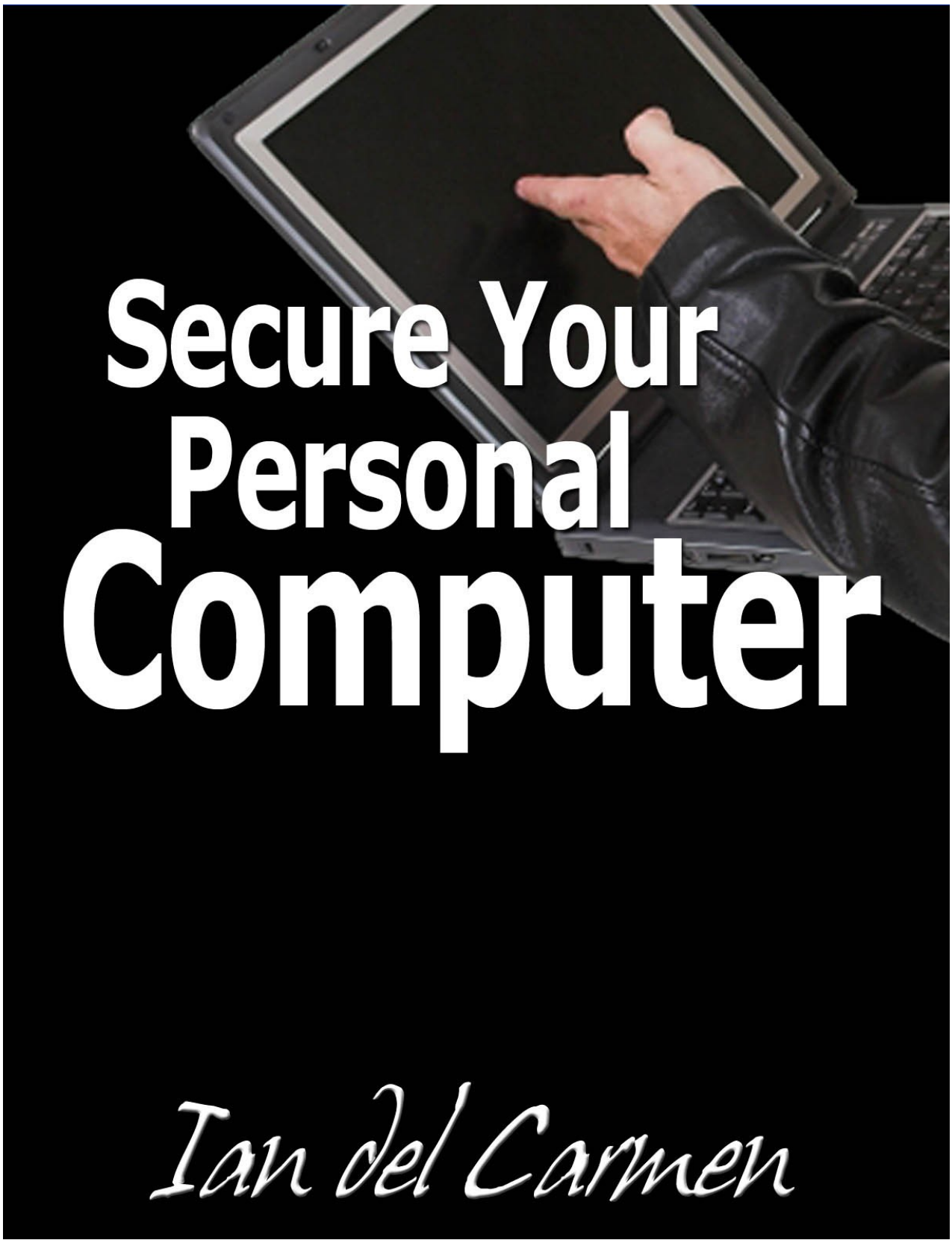

Secure Your
Personal
Computer
Ian del Carmen

Secure Your Personal Computer

"Your Info Guide to Beefing Up Your Personal Computer's Safety From Malicious Threats!"

LEGAL NOTICE

The Publisher has strived to be as accurate and complete as possible in the creation of this report, notwithstanding the fact that he does not warrant or represent at any time that the contents within are accurate due to the rapidly changing nature of the Internet.

While all attempts have been made to verify information provided in this publication, the Publisher assumes no responsibility for errors, omissions, or contrary interpretation of the subject matter herein. Any perceived slights of specific persons, peoples, or organizations are unintentional.

In practical advice books, like anything else in life, there are no guarantees of income made. Readers are cautioned to reply on their own judgment about their individual circumstances to act accordingly.

This book is not intended for use as a source of legal, business, accounting or financial advice. All readers are advised to seek services of competent professionals in legal, business, accounting, and finance field.

You are encouraged to print this book for easy reading.

Table of Contents

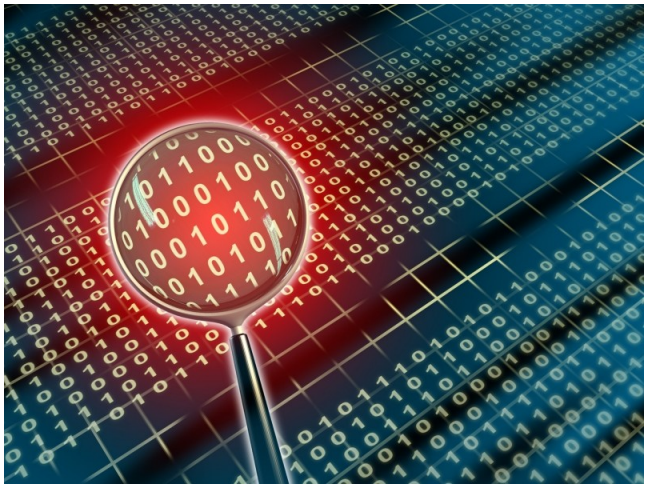
CONGRATULATIONS!

You now have Resell Rights to this eBook.

Just be sure to register your license by sending us your full name, your primary email address, and your website URL to this email address.

Ian Del Carmen

Protecting Your Computer's System



Today, more and more people are using their computers for everything from communication to online banking and investing to shopping.

As we do these things on a more regular basis, we open ourselves up to potential hackers, attackers and crackers. While some may be looking to *phish* your personal information and identity for resale, others simply just want to use your computer as a platform from which to attack other unknowing targets.

Below are a few easy, cost-effective steps you can take to make your computer more secure to begin with:

1. **Always make backups** of important information and store in a safe place separate from your computer.

2. **Update and patch your operating system, web browser and software frequently**. If you have a Windows operating system, start by going to www.windowsupdate.microsoft.com and running the update wizard. This program will help you find the latest patches for your Windows computer. Also go to www.officeupdate.microsoft.com and locate possible patches for your Office programs.

3. **Install a firewall.** Without a good firewall, viruses, worms, Trojans, malware and adware can all easily access your computer from the Internet.

Consideration should be given to the benefits and differences between hardware and software based firewall programs.

4. **Review your browser and email settings for optimum security**. Why should you do this? Active-X and JavaScript are often used by hackers to plant malicious programs into your computers. While cookies are relatively harmless in terms of security concerns, they do still track your movements on the Internet to build a profile of you. At a minimum set your security setting for the "Internet zone" to High, and your "trusted sites zone" to Medium Low.

5. **Install anti-virus software and set for automatic updates** so that you receive the most current versions.

6. **Do not open unknown email attachments**. It is simply not enough that you may recognize the address from which it originates because many viruses can spread from a familiar address.

7. **Do not run programs from unknown origins**. Also, do not send these types of programs to friends and coworkers because they contain funny or amusing stories or jokes. They may contain a Trojans horse waiting to infect a computer.

8. **Disable hidden filename extensions**. By default, the Windows operating system is set to "hide file extensions for known file types". Disable this option so that file extensions display in Windows. Some file extensions will, by default, continue to remain hidden, but you are more likely to see any unusual file extensions that do not belong.

9. **Turn off your computer and disconnect from the network when not using the computer**. A hacker cannot attack your computer when you are disconnected from the network or the computer is off.

10. **Consider making a boot disk on a floppy disk in case your computer is damaged or compromised by a malicious program**. Obviously, you need to take this step before you experience a hostile breach of your system.

Fighting Spam

How prevalent is Spam? According to Scott McAdams, OMA Public Affairs and Communications Department (www.oma.org):

> *"Studies show unsolicited or "junk" e-mail, known as spam, accounts for roughly half of all e-mail messages received. Although once regarded as little more than a nuisance, the prevalence of spam has increased to the point where many users have begun to express a general lack of confidence in the effectiveness of e-mail transmissions, and increased concern over the spread of computer viruses via unsolicited messages."*

In 2003, President Bush signed the "Can Spam" bill, in December of 2003 which is the first national standards around bulk unsolicited commercial e-mail. The bill, approved by the Senate by a vote of 97 to 0, prohibits senders of unsolicited commercial e-mail from using false return addresses to disguise their identity (spoofing) and the use of dictionaries to generate such mailers.

In addition, it prohibits the use of misleading subject lines and requires that emails include and opt-out mechanism. The legislation also prohibits senders from harvesting addresses off Web sites.

Violations constitute a misdemeanor crime subject to up to one year in jail.

One major point that needs to be discussed about this: *spam is now coming from other countries in ever-greater numbers*. These emails are harder to fight, because they come from outside our country's laws and regulations. Because the Internet opens borders and thinks globally, these laws are fine and good, but do not stop the problem.

So what do you do about this?

Here are the top 5 rules to do to protect from spam:

Number 1: Do what you can to avoid having your email address out on the net.

> There are products called "*spam spiders*" that search the Internet for email addresses to send email to. If you are interested, do a search on "*spam spider*" and you will be amazed at what you get back. Interestingly, there is a site, WebPoison.org, which is an open source project geared to fight Internet "*spambots*" and "*spam spiders*", by giving them bogus HTML web pages, which contain bogus email addresses.
>
> A couple suggestions for you:

A) Use form emails, which can hide addresses or also
B) Use addresses like sales@company.com instead of your full address to help battle the problem.
C) There are also programs that encode your email, like **jsGuard**, which encodes your email address on web pages so that while spam spiders find it difficult or impossible to read your email address.

Number 2: Get a spam blocking software.

There are many programs out there for this. (Go to www.cloudmark.com or www.mailwasher.net for example). You may also buy a professional version. Whatever you do, get the software. It will save you time. The software is not foolproof, but they really do help. You usually have to do some manual set up to block certain types of email.

Number 3: Use the multiple email address approach.

There are a lot of free email addresses to be had. If you must subscribe to newsletters, then have a "back-up" email address. It would be like giving your sell phone number to your best friends and the business number to everyone else.

Number 4: Attachments from people you don't know are BAD, BAD, BAD.

A common problem with spam is that they have attachments and attachments can have viruses. Corporations often have filters that don't let such things pass to you. Personal email is far more "open country" for spamers. General rule of thumb: if you do not know who is sending you something, DO NOT OPEN THE ATTACHMENT. Secondly, look for services that offer filtering. Firewall vendors offer this type of service as well.

Number 5: Email services now have "bulk-mail" baskets.

If what you use currently does not support this, think about moving to a new vender. The concept is simple. If you know someone, they can send you emails. If you don't know them, put them in the bulk email pile and then "choose" to allow them into your circle. Spam Blocking software has this concept as well, but having extra layers seems critical these days, so it is worth looking into.

Spyware & Adware

Spyware and Adware are not only an **ever-increasing** nuisance for computer users everywhere, but also a booming industry.

According to Webroot Software, Inc., the distribution of online advertisements through spyware and adware has become a whopping $2 billion industry.

The aggressive advertising and spying tactics demonstrated by some of these programs, require an equally aggressive response from a seasoned eradicator. Sunbelt Software is such a company. A leader in Anti-Spyware, Anti-Spam, Network Security and System Management tools, they gave consistently remained on the cutting-edge of anti-spyware programming since 1994.

So you might be asking:

"Why do I feel as if somebody's watching me?"

According to the National Cyber Security Alliance, spyware infects more than 90% of all PCs today. These unobtrusive, malicious programs are designed to silently bypass firewalls and anti-virus software without the user's knowledge.

Once embedded in a computer, it can wreak havoc on the system's performance while gathering your personal information. Fortunately, unlike viruses and worms, spyware programs do not usually self-replicate.

Where Does It Come From?

Typically, spyware originates in three ways. The first and most common way is when the user installs it. In this scenario, spyware is embedded, attached, or bundled with a freeware or shareware program without the user's knowledge. The user downloads the program to their computer.

Once downloaded, the spyware program goes to work collecting data for the spyware author's personal use or to sell to a third-party. Beware of many P2P file-sharing programs. They are notorious for downloads that posses spyware programs.

The user of a downloadable program should pay extra attention to the accompanying licensing agreement. Often the software publisher will warn the user that a spyware program will be installed along with the requested program.

Unfortunately, we do not always take the time to read the fine print.

Some agreements may provide special "opt-out" boxes that the user can click to stop the spyware from being included in the download. Be sure to review the document before signing off on the download.

Another way that spyware can access your computer is by tricking you into manipulating the security features designed to prevent any unwanted installations. The Internet Explorer Web browser was designed not to allow websites to start any unwanted downloads. That is why the user has to initiate a download by clicking on a link. These links can prove deceptive.

For example: a pop-up modeled after a standard Windows dialog box, may appear on your screen. The message may ask you if you would like to optimize your Internet access. It provides yes or no answer buttons, but, no matter which button you push, a download containing the spyware program will commence. Newer versions of Internet Explorer are now making this spyware pathway a little more difficult.

Finally, some spyware applications infect a system by attacking security holes in the Web browser or other software. When the user navigates a webpage controlled by a spyware author, the page contains code designed to attack the browser, and force the installation of the spyware program.

What Can Spyware Programs Do?

Spyware programs can accomplish a multitude of malicious tasks. Some of their deeds are simply annoying for the user; others can become downright aggressive in nature.

Spyware can:

- ⇒ Monitor your keystrokes for reporting purposes.
- ⇒ Scan files located on your hard drive.
- ⇒ Snoop through applications on our desktop.
- ⇒ Install other spyware programs into your computer.
- ⇒ Read your cookies.
- ⇒ Steal credit card numbers, passwords, and other personal information.
- ⇒ Change the default settings on your home page web browser.