ALWAYS USE PROTECTION

A TEEN'S GUIDE TO SAFE COMPUTING

ALWAYS USE PROTECTION

A TEEN'S GUIDE TO SAFE COMPUTING

Dan Appleman

Apress®

Always Use Protection: A Teen's Guide to Safe Computing

ISBN (pbk): 1-59059-326-X

Printed and bound in the United States of America 12345678910

Technical Reviewers: See Acknowledgments
Editorial Board: Steve Anglin, Dan Appleman, Gary Cornell, James Cox, Tony Davis,
John Franklin, Chris Mills, Steven Rycroft, Dominic Shakeshaft, Julian Skinner, Jim Sumser,
Karen Watterson, Gavin Wray, John Zukowski
Assistant Publisher: Grace Wong
Project Manager: Sofia Marchant
Copy Editor: Ami Knox
Production Manager: Kari Brooks
Production Editor: Ellie Fountain
Proofreader: Elizabeth Berry
Compositor: Gina Rexrode, Point n' Click Publishing, LLC
Illustrator: Kinetic Publishing Services, LLC
Indexer: Valerie Robbins
Interior and Cover Designer: Kurt Krames
Manufacturing Manager: Tom Debolski

Library of Congress Cataloging-in-Publication Data

Appleman, Daniel.
Always use protection : a teen's guide to safe computing / Dan Appleman.
p. cm.
Includes index.
ISBN 1-59059-326-X (soft cover : alk. paper)
1. Computer security. I. Title: Teen's guide to safe computing. II. Title.
QA76.9.A25A63 2004
005.8--dc22
2004003941

Distributed to the book trade in the United States by Springer-Verlag New York, Inc., 175 Fifth Avenue, New York, NY, 10010 and outside the United States by Springer-Verlag GmbH & Co. KG, Tiergartenstr. 17, 69112 Heidelberg, Germany.

In the United States: phone 1-800-SPRINGER, email `orders@springer-ny.com`, or visit `http://www.springer-ny.com`. Outside the United States: fax +49 6221 345229, email `orders@springer.de`, or visit `http://www.springer.de`.

For information on translations, please contact Apress directly at 2560 Ninth Street, Suite 219, Berkeley, CA 94710. Phone 510-549-5930, fax 510-549-5939, email `info@apress.com`, or visit `http://www.apress.com`.

The information in this book is distributed on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this work, neither the author(s) nor Apress shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

CHAPTER 2

When Software Attacks: All About Viruses

Anytime you do something on your computer, whether it's browsing the web, chatting with a friend on an instant messaging service, writing a paper, or drawing a picture, you're running a program. In fact, the Windows environment itself—the desktop that allows you to view and select files or configure the system—is just a collection of programs.

A computer program is just a set of instructions to a computer. But programs take many forms. They can be *executable files* (files with the extension .exe), or *batch files* containing console[1] commands (files with the extension .bat). They can be scripts that control other programs—for example, a program built into a word processing document that automatically counts the number of words or creates an index, or a script that controls game play on a custom game map.

Once a program gets on your computer, it has access to pretty much all of the capabilities of your machine.[2] As long as the software does what you want and expect it to do, there's no problem. But what if the author of that program had other things in mind?

Evil Schemes

There's almost no limit to the kinds of nasty things viruses and other malicious programs can do. Here's a brief list of some of the kinds of threats that your computer faces if one of these programs is allowed to run on your system.

[1] *A* ***console*** *is the window you see when you request the command prompt from the Start menu. It mimics an old-style DOS window where you type commands in without a graphical interface or mouse.*

[2] *There are exceptions to this, depending on the type of program or script, the language it was written in, and the configuration of the system. But it's best to work under the assumption that any program on your system can do anything the program's author wanted to do.*

The Destroyers

These are programs that have one goal—to trash your system. Some of them do it quickly, by simply deleting your disk partition, boot sector, or reformatting your drive.[3] Some do it slowly, deleting or scrambling random files until your system won't run. Some only target your data—scrambling or destroying data files while leaving key system files in place.[4]

The Annoyances

These programs don't want to destroy your system, only your sanity and patience. They just like to get on your nerves. Maybe they'll periodically terminate your Internet connection or reboot your machine. Or throw garbage up on your screen or suddenly close programs. They might redirect your browser to different web sites, or sign you up to spam e-mail lists.

The Thieves

They say that information is one of the most valuable commodities, and these programs want to steal it from you. They want your passwords, your game CD-keys, and all the personal information they can get. Credit card numbers and tax information (with Social Security numbers) are favorites. They want to know what web sites you've browsed to and get copies of any e-mail you've sent or received. You'll read more about this kind of software in Part II of this book where I discuss privacy.

The Hijackers

These programs don't want to harm your computer at all. They want to take it over and put it to some other use. They might want to use your computer (along with thousands of others) to send corrupt network requests to a particular web site in order to overwhelm it and prevent others from accessing it (this is called a *Denial of Service*, or DoS, attack). They might want to turn your computer into an e-mail server that will allow them to use it to send out spam. They might hijack your hard drive to store pornography, pirate software, or other illegal content.[5]

[3] All things that will cause your computer to fail to start and probably lose all of your files

[4] Hint: The old excuse "The dog ate my homework" won't get you anywhere nowadays, but if you try "A virus ate my homework" you might just get an extension. Most of your teachers don't know much about computer security, and I promise by the time you're done with this book, you WILL know more about it than most of your teachers (actually, most adults, period).

[5] This alone is a good reason to take computer security seriously—do you really want to explain to your parents why the FBI is knocking on your door?

Viruses, Worms, and Trojans

Viruses, worms, and Trojans are different kinds of malicious programs. I'll tell you how they differ in a moment, but in truth, most people use the term *computer virus* to refer to all three types of program. So after this section, just assume that when I talk about viruses I'm referring to worms or Trojans as well.

Viruses

In biology, a virus is a submicroscopic piece of genetic material (RNA or DNA) surrounded by a coat of protein. It reproduces by attacking a cell and hijacking its internal structure to create more viruses. Once the cell has done its job, it self-destructs, leaving behind even more of the virus to go and invade other cells.

A computer virus does much the same thing to a computer program.

A computer program consists of a sequence of computer commands along with some data. Once loaded into memory, the program "runs," meaning that the computer executes the command sequences.

Figure 2-1 illustrates a normal program. Imagine that each square represents an instruction that the computer will execute. Each program has a starting point—the first instruction that runs when the program is loaded. So as the program runs, it will execute each instruction in turn, starting from the "starting point" and continuing to the end.

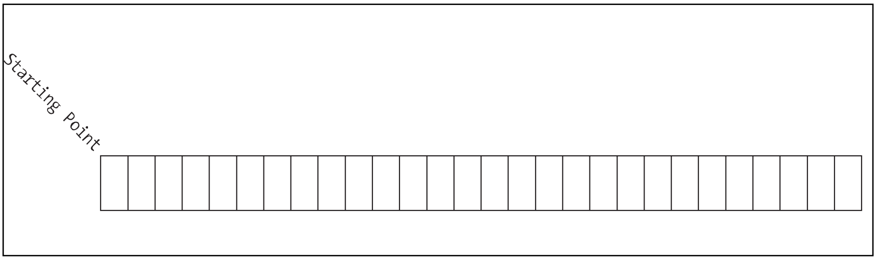

Figure 2-1 A "healthy" program

Figure 2-2 illustrates what happens when a virus infects a program. The virus literally modifies the program file on your disk. The gray squares represent instructions that the virus has added to the program. First, it adds additional code to the program, usually at the end of the program. The viral code is indicated by light gray squares. Next it changes the code at the starting location of the program to force the computer to run the viral code. The new code at the starting point includes an instruction to jump to the rest of the virus code (as indicated by the arrow).

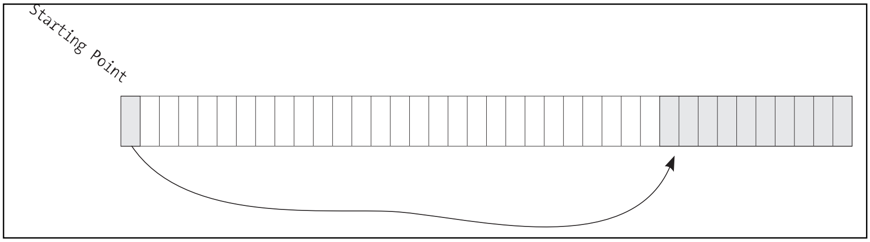

Figure 2-2 An "infected" program

If the virus is really smart, it might also execute the healthy code, in which case you may never know that the virus was running.

Viruses can do any of the things listed earlier in this chapter (and others I probably haven't even imagined), but there's one thing almost all of them do. They try to infect other files on your system or on your network.

Worms

Most of the time when people talk about viruses, they're actually talking about worms as well. A *worm* differs from a virus in that it doesn't infect other files. The worm is a standalone program—it works independently.

A virus runs whenever you execute an infected program. For example, if your paint program is infected, anytime you try to run it the virus will run. Worms can't use this particular trickery, but they have their own ways to get started.

- Most worms add themselves to the list of programs that should run automatically when your computer starts. In Appendix B of this book you'll learn more about self-starting programs.
- Worms also like to trick you into running them, claiming to be something they aren't. For example, a worm might claim to be a game, or a cool program sent by a friend. In Chapter 3, you'll learn all about how viruses and worms spread.
- Worms can also attack vulnerabilities in your system across a network or the Internet, even if you do absolutely nothing—quietly sneaking in without your knowledge.

Other than being standalone programs, worms are just like viruses, and do the same kinds of things once running on your system.

Trojans

Trojans are a kind of virus (actually, a worm most of the time). They're named after the Trojan horse.[6] That's the one where the ancient Greeks defeated Troy by pretending to give up, leaving behind a giant wooden horse in which they had hidden some soldiers. The celebrating Trojans brought the horse into their city, only to be defeated when the soldiers snuck out at night and let the Greek army into the city.

When a Trojan gets on your system, its goal is to allow outsiders into your system.

Recently, my nephew visited a friend, and found him struggling with his computer. Every time he connected to the Internet, he'd start getting pop-up window messages from someone. The messages demanded he give over his Warcraft and Frozen Throne CD-keys, or the blackmailer would delete files on his system. In fact, by the time I heard about it, the system had already suffered quite a bit of damage—not only did his Internet browser no longer work, but even basic programs like Notepad had been deleted.

You might be wondering, How did the attacker find the infected system when it connected to the Internet?

The answer is that he didn't. The Trojan knew its creator and would contact him every time the computer connected to the Internet. The attacker only needed to sit back and wait for the Trojans he sent out to call home and let him on to the infected systems. Some Trojans work this way, others simply instruct the computer to wait for instructions, configuring the computer to listen for future contact from the attacker—perhaps sending out an e-mail or other notification to the attacker so he can build a list of infected computers to contact at will.

That is perhaps the scariest thing about Trojans. An ordinary virus or worm is preprogrammed—it can only do what was designed into it originally. As terrible as those things may be, at least they can be identified and dealt with. A Trojan opens your computer to access by outsiders—real people—and there's no telling what they might do on your computer. They might do nothing more than keep watch on what you're doing; waiting for some interesting information they can steal or use to threaten you. You may not know anything is wrong.

Spyware and Adware

Spyware and *adware* are both terms for software that monitors what you do on your system (effectively spies on you) and does something with that information. They can range from extremely dangerous, to helpful—and in fact, in many cases they get installed on your system with your full permission. In fact,

[6] *Not some other type of Trojan*

one can argue that some of them don't qualify as viruses at all. Consider some of these variations:

- A keyboard monitor spyware program might watch every keystroke you type, waiting for cases where it can detect you typing in an account name and password. Once it has them, it might send the information out to someone who can then use them to impersonate you—hijacking your bank account, e-mail service, or other online service.
- A web page tracker might watch while you browse, and anytime you shop for something it might bring up a pop-up redirecting you to a different store, or swapping in an affiliate code[7] so someone else can make money off your purchases. Such a tracker might also check pricing for you and offer you a better deal than you were about to get.
- Some software, especially free software, includes advertising—thus the term *adware*. You accept the advertising in much the same way as you accept commercial television: the commercials pay for the content.

Is an adware program that you allow on your system a virus? Probably not. However, I'll be honest—I'm not a big fan of such software. First, you usually don't know everything they do. Sometimes that information is buried in the fine print—you know, the endless license agreements that you accept without reading.[8] Second, even beneficial adware might have side effects. It might interfere with other programs and will often slow down your system.

So I won't tell you that you should delete all adware from your system. But you should be aware of what adware is present on your system, and know how to remove it if you don't like it. As for malicious spyware, it's a virus, period.

RULE OF THUMB If you install software, and can't easily figure out what it does or how to remove it, you should consider it a potential virus.

Adware and Lag

Spyware, adware, and P2P services such as Kazaa make use of the Internet. The thing to remember is that their use isn't limited to when you're actually doing something relating to the software. For example, you know that when you're downloading a file on Kazaa, or someone is uploading one from your system, Kazaa is making use of the Internet. But it turns out that Kazaa uses the

[7] *This is a code added to a web address to help web sites know who referred them to the site. Some web sites will pay money to sites that generate referrals that result in sales.*

[8] *Almost nobody reads those agreements before clicking "I Accept". You might try reading one sometime—the things you are agreeing to might astonish you.*

Internet even when no files are being transferred. When Kazaa is running, your computer is part of the P2P network, and your computer will periodically send out and receive information relating to searches and other maintenance operations. It will also periodically download and display advertisements if you're using the adware version. The same applies to other adware and spyware—you have no control over when they connect to the Internet to perform their operations, and how much data they are transferring.

When you're connected to the Internet, you have a certain amount of bandwidth available—this is the number of bytes per second that your Internet connection can handle. On a modem, you have up to 56 kilobits per second download and 28 kilobits per second upload. That translates into under 7 kilobytes per second download and half that on upload—not very fast.[9] Any data transferred by spyware and adware subtracts off the available bandwidth for other tasks. It can slow your Internet performance even on a fast DSL or cable line, and can make a dial-up modem connection virtually useless.

Each spyware or adware program on your system can take up some bandwidth—and it can definitely add up. Worse, it's not evenly distributed—a program may do nothing for an hour, and then try to tie up all your bandwidth for several minutes.

This "hidden" use of your Internet bandwidth can be fatal for online gaming, and is actually one of the common reasons for lag and for people being dropped from games. You can be in the middle of a Warcraft game when an adware program wakes up and starts several large transfers. Next thing you know, your screen freezes and you find yourself dropped from the game.

Viruses can have the same impact on bandwidth, but there are plenty of good reasons to get rid of viruses that have nothing to do with gaming. But adware is something you may allow on your system intentionally, and it's important you realize the side effects this may cause.

Why Do People Write Viruses?

Viruses cause a huge amount of harm. They cause individuals and corporations to lose critical data. They waste enormous amounts of time. They are expensive to deal with, both in prevention and in cleanup.

So it's worth taking a moment to consider why people write these things.

There is the stereotype of the nerdy teenager or college student who writes viruses just because they can. It's part of the "hacker" mythology—a way to prove one's technical prowess or just get some attention. And there is some truth to this stereotype. I should, however, note that the use of the word

[9] *There are 8 bits in a byte, so a modem speed of 56 kilobits per second is about 7 kilobytes per second. In fact, you'll get less, because a 56k modem only gets at best 53k in practice.*

hacker is really incorrect here. A classic hacker is someone who delights in solving tough technical problems. The kind of "hacker" who writes viruses is more correctly called a *cracker*. You may also hear the terms *white hat* and *black hat* to replace hacker, where a white hat is someone who uses their knowledge of computer security for good to protect people's systems and privacy, and a black hat is someone who is using their skills to cause harm.

Definitions notwithstanding, the term *hacker* is commonly used today to represent both white hats and black hats. So if, later in this book, I refer to a hacker attacking your system, you'll know I'm really referring to a black hat. Why? Because only a black hat would use their hacker skills to attack your system.

For those of you who are interested in going further into computer security or computer internals, it's a fascinating field. I would strongly encourage you to become a hacker in the classic sense—a white hat. Aside from the ethics of the matter, it's just as challenging, just as fun, and a whole lot less likely to land you in jail.

The Real Threat: Cyberwar

The media may play up the occasional teenage hacker who edits or spreads a virus, but that isn't where the real danger in the future lies. You may have already heard that more and more viruses are coming out of countries that aren't entirely friendly to Western ideals. As more and more of the free world's infrastructure and economy becomes dependent on the Internet, we become increasingly vulnerable to attack by terrorist organizations or unfriendly governments. The terms for this are *cyberwar* and *cyberterrorism*. (Perform an Internet search on these terms for further information—there are many sites that discuss the issue.)

Cyberwar typically refers to government-sponsored attacks. These can be attempts to hack into sensitive government installations to obtain secrets or interfere with government or military operations. Or attacks on banks to try to cripple the financial system.

Cyberterrorism typically refers to attacks made by nongovernmental groups. Occasionally you'll hear about acts of cyberterrorism—government or media web sites that are hacked into and modified for political purposes. One can make the argument that many viruses are, in fact, acts of cyberterrorism.

We don't actually know what a real cyberwar would look like. You can bet that most governments invest heavily on both offensive and defensive techniques. But considering how poorly we are handling viruses and privacy attacks in a time of relative peace, the thought of full-scale cyberwar is disturbing indeed.

An attacker doesn't have to actually break into a web site to bring it down. Even the largest web site can handle only a limited number of requests at a time. Let's say a bank's web site can handle 50,000 requests per second—a very significant number. Rather than attack the bank directly, a cyberattacker might distribute a worm that would quietly infect millions of computers. That worm might have a trigger date—as soon as that date arrives, every single infected computer tries to contact that bank's web site. Suddenly, the bank is receiving a million fake requests per second—far more than it can handle. Legitimate requests get crowded out by the fake requests—so people trying to contact the site see an error. This is called a Denial of Service attack.

Because Denial of Service attacks rely on hijacking as many computers as possible to perform an attack on a few sites, one can argue that protecting your own computer and making sure it can't be hijacked isn't just a matter of personal defense, but of national defense as well.

When Software Sneezes

Biological viruses infect people in several ways. Some travel through the air when you sneeze or cough. Others sit on a surface until you touch it, or touch someone who is sick. Yet others are transferred through close contact or cuts, wounds, or unsterile needles.

A virus can't hurt you until it gets inside of you, and so it is for computer viruses as well. They can't harm you until they find their way onto your computer. Unfortunately, computer viruses have just as many ways of spreading as biological viruses, maybe more.

Scientists couldn't learn how to prevent the spread of disease until they understood how viruses and bacteria spread.[10] So you too will need to learn something about how computer viruses spread, the subject of the next chapter, before you'll be able to deal with them effectively.

[10] *For example, the reduction in worldwide cases of malaria didn't begin with vaccines or medication—it began with the discovery that malaria was spread by mosquitoes.*

CHAPTER 9

What to Do When You've Been Hit

Reading about security can be rather depressing. You may feel, based on what you've read in this book so far, that your poor computer is under constant attack by evil forces that are out to get you.

This is probably because your poor computer is under constant attack by evil forces that are out to get you.

But there is some good news.

If you follow all of the precautions, or even most of the precautions, you've read about so far—keeping an up-to-date antivirus program running at all times, using a firewall, and keeping your system up to date—chances are actually good that you'll never be infected by a virus or have your system penetrated by an attack from the Internet. I've been a professional software developer for a long time, and the only virus that (to my knowledge) has ever been on one of my personal systems is one that I captured intentionally for a talk I was doing on security.[1]

I've also been exceptionally lucky and paranoid about what goes on my system. Yet I also know that tomorrow can be the day that I make a mistake, or the day an attack succeeds due to some system vulnerability I have no control over.

Many of you reading this book will make a mistake, or get unlucky. And many of your computers will get infected before you have a chance to put the precautions you've read about into place. Many of your computers are infected right now.

And the best precautions don't do much good when you already have an active infection.

This chapter is all about what to do to clean up your computer as safely as possible.

[1] *It was the Melissa virus, one of the first really nasty viruses that lived in Microsoft Word documents. I defanged it (removed its ability to spread and replaced the harmful code with messages saying "If I were real I'd be doing something bad to your system"), then used what was left in a presentation illustrating the amount of damage such a virus can actually do.*

Introduction to Readers Who Are Starting Here

For those of you who've already read the previous chapters, what you've learned will help you understand the instructions that follow on how to clean your system. So you can skip the next couple of paragraphs.

I'd like to welcome those of you who have flipped directly to this chapter. I know you're out there. Maybe your computer is already infected with a virus and you're desperately looking for an easy solution to your problem. If so, I'll help you as best I can—but you won't necessarily understand everything you find here. I'll try to point out which chapters covered key concepts so you can backtrack if you get confused.

But for those of you who think this is all you need to know—that you don't need to read the first eight chapters, please reconsider. When it comes to dealing with viruses and Internet attacks, prevention is infinitely better than trying to clean up the mess afterwards.

Some Advice Before You Start

Before you begin cleanup, I'd like to offer some observations and suggestions to get you off on the right track.

There Is No Easy Solution

I wish I could offer you a guaranteed way to clean your system—one that will always work and will rescue all your data. But I can't.

IMPORTANT WARNING Anytime you're dealing with viruses or system repairs, you risk loss of data. The information provided here is a set of guidelines that have a good chance of working on most typical home systems. However, because of the huge number of different viruses and possible system configurations, I can't guarantee that the suggestions here will work for your situation. In fact, they may very well make things worse.

So consider yourself warned—whatever happens from here is at your own risk and your own responsibility. If you have information on your system that you can't afford to lose, you should call in expert help from someone who can base their advice and actions on your specific situations.[2]

[2] Finding an expert can be a challenge also. A friend of mine recently brought her computer to a major computer chain to have a virus removed. They said it would be back in two days, but it took three weeks, cost her $160, and she ended up losing all the data and programs on her system anyway.

Check for Book Updates

Believe it or not, I rewrote this chapter four times to get to this point, and I'm still not entirely happy with it. What I'd like is to be able to help every reader clean their system—but I know that's impossible, because every system is so different. I can't even include everything I know about cleaning a system, because the result would be a much longer and exceedingly boring book, containing large sections that would only be needed by a few readers. Plus, today's best recommendations may not match tomorrow's.

For that reason, I run the web site AlwaysUseProtection.com, which is dedicated to providing ongoing information and advice. It also includes updates to the book. I encourage you to visit and check for updates to this chapter before you continue.

Take a Deep Breath

I'm going to let you in on a secret. Even the most experienced computer engineer faces an infected system with at least a mild degree of panic. Many times cleanup and system repair is easy and straightforward, but even the experts know that no matter how experienced you are, you may be facing a situation that you just can't fix, and you may be about to lose valuable data beyond any hope of recovery.

So before you start, take a deep breath, and remember these words of advice.

Don't Panic

The Hitchhiker's Guide to the Galaxy[3] was right on this score. If you have a hardware problem like a disk crash, there's not much you'll be able to do about it—other than pay a lot of money to a disk recovery service that might be able to rescue some of your information. Otherwise, you may have a lot of restoration to do, but if you follow the advice here, you should be able to minimize actual loss of data. Just try to stay calm and . . .

Be Patient

Cleaning and restoring a system is a very slow process. Don't rush into things. I know you'll be tempted to just run your virus scanner and delete every infected file—but that can lead to worse problems, so it's best to prepare for them in advance. Read these instructions twice—read the instructions on your antivirus program—and then, when you've thought things through the best you can, don't be afraid to try things.

[3] *Great book by Douglas Adams about a galactic encyclopedia that had "Don't panic" stamped on its cover*

Be Persistent

Cleaning and restoring a system can be frustrating. But don't give up. Try not to skip any of the recommendations I offer—they are there to help you and are based on harsh experience.[4] Read them carefully—I've kept them short and every sentence counts. And don't be afraid to ask for help—you can probably find a friend who can answer your questions and get you over the rough spots.

Don't Read This Chapter

Unlike most of the other chapters in this book, this chapter isn't meant to be read from start to finish. It's more like one of those "choose your own adventure" books you may have read as a kid. You'll begin by evaluating the current state of your system, and then read and perform only the tasks that are needed for your situation. If you're lucky, you'll never need to read most of this chapter!

Ready to start? Here we go.

The Three Steps to Cleaning Your System

Regardless of the current state of your system—whether you're doing a routine virus scan or trying to rescue a system that won't even boot—the job divides into three parts:

1. Decide what information on your disk you don't want to lose, and try to rescue it.
2. Prepare for the virus scan, and then do it.
3. Clean up the mess that's left afterwards.

Sounds easy, doesn't it?

If only it were so.

The actual job of cleaning your system may involve a variety of tasks. Later in this chapter, you'll see a section named "The Task List," which goes into detail on how to do the following tasks. (Don't do them now! Think of this as a preview.)

- **Prepare for a Scan or Update:** What to do before you scan your system or do a system update.
- **Update Your Restore Tools and Information:** Preparing information that can help you rescue your system in case of disaster.
- **Disconnect from the Net:** When you need to get off the Net, fast.

[4] *My own as well as others*

CHAPTER 10

When They Think It's You, but It Isn't: Identity Theft

You might be wondering—what does identity theft have to do with you? After all, what can you possible have that would make someone want to steal your identity?[1]

And in a sense, you'd be right. Identity theft is a much greater problem for adults than for teenagers.

However, consider the following discussion:

Your friend: Hey, why did you call me an idiot on IM last night?

You: What? I wasn't online.

Your friend: You were calling me all sorts of stuff.

Your friend: And you were telling OtherFriend99 that she was a big fat stinking slob. She was really pissed.

You: No way! I was grounded from the computer yesterday.

Your friend: Yeah, sure . . . she's gonna believe that.

You may already have guessed what happened here. "You" in this case left an instant messenger program installed on a computer configured in a way that it automatically logged on under "your" account. Perhaps it was at a friend's house or public computer. Anyway, someone came along, found an active instant messenger screen, and started chatting with people on "your" buddy list.

Yes, it might just be a practical joke. But it can also be socially devastating. And things are worse if someone can change your IM or e-mail password and continue to pretend to be you. It can take days or weeks to notice the problem, not to mention clean up the mess.

[1] If you're an adult reading this book, the answer is a lot easier . . . bank accounts and credit cards are obvious, but there are other risks, as you'll soon see.

So surprise—teens do suffer from identity theft. And it happens all the time. In this chapter and the ones that follow, you're going to learn the basic precautions to prevent this kind of problem.[2]

And guess what? Many teens do have bank accounts, and though they usually aren't quite big enough to justify a determined assault, if you make it easy enough someone might just slip in and clean out what you do have. And someone trying to commit fraud or a crime and frame someone for it may not care if it's an adult or teen identification they steal for that purpose. Oh, and one more thing: The things you learn and habits you form in this chapter will help you for the rest of your life. They'll help you prevent identity theft later, when an attack can cost you thousands of dollars and take years to clean up.

NOTE How big a problem is identity theft?

In a Federal Trade Commission survey dated September 2003,[3] 1.5 percent of respondents experienced a major fraud incident, with an average loss of $10,200 (of which the victim ended up losing an average of $1,200). Another 2.4 percent of respondents experienced some sort of credit card fraud. When asked, an astonishing 12.7 percent of respondents experienced some kind of identity theft in the past five years, and spent an average of $500 and 30 hours cleaning up the mess. Note, however, that in most of these cases the information used for the identity theft was obtained through old-fashioned methods—stolen mail or credit card receipts—and not through the Internet. Visit `http://www.ftc.gov` for more details.

What Identity Thieves Want

Ultimately, what thieves want is the ability to pretend to be you. They want to be able to buy things on a victim's credit cards, to pull money out of their bank accounts, and even to commit crimes and have the victim take the blame.

One way they can do this is by calling up an institution (bank, credit card company, etc.) and pretend to be you. These companies verify your identity by asking personal questions that supposedly only you would know. If the thief has that information, they can successfully pretend to be you and give instructions to the institution that they will follow, assuming they are talking to the correct person.

It's a bit like the classic case of a student calling the school office while pretending to be a parent, and trying to explain why they aren't in school that day—except it's much more extreme and the stakes are higher.

[2] *You'll find details on disabling automatic logon for instant messenger programs in Chapter 11.*

[3] *Prepared by Synovate Research. See* `http://www.ftc.gov` *for the complete survey.*

Who Are You?

To steal your identity, a thief needs information about you. And some information is more dangerous than others. The following list is roughly in order from least to most dangerous with regards to identity theft.

Name and Address

This information is actually more important to protecting yourself (Part III) than protecting your identity. You should only give this information to a web site when you are asking them to send you something by mail (either information, or when you are buying something). It's generally safe to use your first name on web sites, but you should not give out your last name unless you have good cause. Name and address alone is not generally enough to steal someone's identity,[4] so shopping online and requesting information be mailed to you is reasonably safe.

> **CAUTION** While your name and address is not high-risk information in regards to identity theft, it is extremely high-risk information to give out in a public chat room or otherwise post in a public forum. Be sure to read more about this in Chapter 14.

Phone Number

Your phone number is also a relatively low-risk piece of information to give out—as long as your number is unlisted. If it is listed in a phone book with an address, it is possible to use a reverse directory to obtain the address given the phone number. One quick way to find out if this applies to you: Go to Google.com and enter your phone number in the search window. If it pops up with your address, you should use extra caution in posting your phone number.

Credit Card Numbers

While most teens don't have credit cards, they routinely use their parents' cards for online shopping. And in fact, that's pretty much the only time you want to enter your credit card onto a web site—when making a purchase on a secure web site.

Curiously enough, credit cards are the safest way to make purchases online because they have the strongest fraud protection. If you buy something by credit card, and it never arrives, the credit card company will refund your money and charge the seller.[5]

[4] *However, many cases of identity theft occur not from the Internet, but from the more primitive approach of mail theft. And if someone knows where you live . . .*

[5] *Protection for debit cards is more limited, as you'll see later in this chapter.*

Driver's License Number

As a form of identification, it's fairly dangerous—the last thing you want is somebody else creating a fake driver's license with their picture, and your personal information.

Never give this information out online.

Birth Date

Your birth date is a key piece of information that can be used to identify you. Never give it out unless you are on a secure connection (which you'll read about shortly), and you absolutely trust the security of the web site.

Some sites will ask for your birth date—they want this information because your age is one of the most useful pieces of marketing information a site can have when trying to sell you things. In cases like this, you should seriously consider not registering with the site at all—any site that requires you to provide personal information should be considered suspect. If you want to register anyway, consider creating a fake birth date for use online.[6] If you want them to know how old you are, keep the year the same, just change the month and day. As long as it doesn't match your birth date on official records, you're reasonably safe.[7]

Social Security Number

This one is worse than the birth date. Never give it out—period. Any site that asks for your Social Security number is almost certainly pulling a scam.[8] Don't use a fake Social Security number either—that's just plain against the law. Plus, you run the risk of choosing a real one, which can cause grief to someone else.

Mother's Maiden Name (or Secret Word)

Historically, most banks and similar institutions would use your mother's maiden name (that's her last name before she got married) to help identify you, under the assumption that it's the kind of information only close family would know.

Nowadays most institutions will accept any password as an alternative.

Treat this information as you would your Social Security number. Never give this information out online.[9]

[6] *I'll talk more about lying online in Chapter 11. There are cases where you can get into trouble for lying—if you are attempting fraud or agreeing to a document where you assert that everything you're saying is truthful. But for surveys and routine registration on web sites (where they are just collecting marketing information), it's generally OK.*

[7] *I say reasonably safe, because banks and financial institutions do make mistakes.*

[8] *There are a few exceptions to this—when dealing with some financial institutions and insurance companies with which you already have an account, or when applying for credit. Some colleges use it for identification purposes as well.*

[9] *The same exceptions apply here as with Social Security numbers.*

Online Account ID and Passwords

If you really want to make it truly easy for people to steal from you or impersonate you, the best thing you can do is give out an online ID or passwords. That saves thieves the trouble of trying to obtain the information by pretending to be you and allows them to go directly to the account in question and do whatever they want.

Never give out your password. If you do give it out, or you receive a password reminder or temporary password via e-mail, change it immediately.

Your password is more critical than your online ID (the login or user name you use on various sites). That's because many sites use your e-mail as the user name, and that is generally considered public information anyway.

I'll talk more about passwords in Chapter 11.

Permanent vs. Temporary Information

These warnings may seem extreme—especially given that many of you don't have dealings with financial institutions at all. But it really is important to get into good habits now. That's because some of the information here—like your Social Security number and birth date—are going to be with you for the rest of your life. The last thing you want is an entry like this somewhere on a web site:

Jan Somebody

123 Someplace Lane

SomeCity, California 95151

SSN 123-45-6789

DOB: 1/1/1990

Once archived by search engines, it may be impossible to ever remove this information from the Internet—meaning you will spend the rest of your life potentially at risk of identity theft from anyone who stumbles on this information—or who even does a search based on your name!

How They Get It

There are three main ways that outsiders can get at your personal information using the Internet: