

Contents

Online Theft

Think of your computer's hard drive as an online "wallet" that can contain the following:

- Computer login accounts
- Screen names
- Electronic commerce account numbers
- E-mail addresses
- Computer and domain names
- Computer IP addresses
- Passwords, passwords, and more passwords

Foreword

xix

Chapter 1 Identity Theft: Are You At Risk?

1

Introduction

2

Defining Identity Theft

3

Take a Risk Factor Test

4

Why Do They Do It?

5

How Do They Get Away with It?

6

Dumpster Diving

7

Shoulder Surfing

8

Social Engineering

8

Physical Theft

10

Online Theft

12

Privacy Erosion

14

Limited Enforcement Resources

15

Recognizing Identity Theft When It Happens

15

Unauthorized Credit Cards

16

Unauthorized Phone or Other

Utility Services

16

Bank Fraud

17

Fraudulent Loans

18

Government Documents

18

Other Forms of Identity Theft

18

Understanding What Electronic Information

Is Private

19

Striving for Theft Prevention

22

Keeping Private Information Private

26

Protecting Your Social Security Number

26

Taking Advantage of Marketing Opt-Out Programs	29
Using Search Engine Opt-Out Services	30
Using the Direct Marketing Association's Opt-Out Service	32
Protecting Your Computer	34
Applications	34
E-mail	34
Web Browsing	34
Network	35
Your Family's Online Activities	36
Summary	37
Solutions Fast Track	38
Frequently Asked Questions	41

Viewing Hidden Programs

Hidden programs are programs that run on your system without your being aware of them. Some of these programs are called *spyware*, which is software that secretly gathers personal and organizational information from your computer, monitors your Internet activity, and/or obtains other information about you. You can see if hidden programs are running on your system using Task Manager on systems running Windows XP/NT/2000.

Chapter 2 Protecting Your Hard Drive	43
Introduction	44
Know Your Computer	44
Temporary Files	46
Temporary Internet Files	48
Deleting Files Permanently for Privacy	49
Other Information that Might be on Your Computer	52
What Are You Protecting?	54
Password Protecting Your Computer	55
Programs and Files	57
Antivirus Software: Your First Line of Defense	59
What You Might Not Know about Antivirus Software	60
Why Update?	61
What Kinds of Software Are Available?	61
Manually Updated Signatures	62
Automatically Updated Signatures	62
Web-based Software	63
Performing Signature Updates	63
McAfee	63
Norton	64

F-Prot	65
Is Your Antivirus Software Working?	66
Updating Your Software	68
The Number One Mistake People Make	69
Functionality Vs. Secure Updates	70
Installing Security Patches	70
Internet Explorer	71
Outlook	72
IIS	72
Netscape	73
Opera	73
Beware of the Free Stuff	73
Avoiding Account Sharing	74
Common Reasons, Risks, and Deterrents for Sharing Accounts	75
Creating Multiple Accounts in Windows	76
Setting Up an Account in Windows XP	77
Setting Up an Account in Windows 2000	78
Creating Multiple Internet Connection Accounts	78
Setting up Multiple Internet Connection Accounts in Windows 98	79
Setting up Multiple Internet Connection Accounts in Windows XP	79
Setting up Multiple Internet Connection Accounts in Windows 2000	81
Creating Multiple E-mail Accounts with Outlook Express	82
Using Disk and File Encryption	83
Choosing Strong Passwords	86
Avoiding Weak Passwords	87
Protecting PINs	89
Tradeoffs: Using Password Storage	90
Creating Strong Passwords You Can Remember	93

Summary	98
Solutions Fast Track	99
Frequently Asked Questions	101

Chapter 3 Keeping Your E-mail Private 103

E-mail Privacy Is Not Just About SPAM

Check privacy policies of Web sites to determine what they do with any information they acquire from you.

If you receive SPAM, check the message to see if they provide a method to be removed from their mailing list. Look into software or services provided by your Internet Service Provider to have e-mail flagged and/or deleted before reaching your inbox.

Disable cookies to prevent information from being sent to Web sites.

Introduction	104
E-mail Privacy Is Not Just about Spam	104
How E-mail Services Work	105
Big Brother and Your E-mail	108
How E-mails Can Get Lost	110
Understanding Spam	113
E-mail Attacks Are Not Just about Viruses	114
E-mail Attachments	115
How Your E-mail Can Be Hijacked	116
E-mail Interceptions	116
Recognizing Mail Scams	119
Solicitations and Chain Letters	120
Nigeria 419 Scam	122
Spam as Social Engineering	124
Using Antivirus Protection for E-mail	126
Hiding Your E-mail Identity	128
Knowing What's in Your E-mail Headers	128
Knowing What Your Chat Says about You	132
Setting Up Anonymous E-mail	133
Free Anonymous E-mail	134
E-mail Encryption Made Simple	135
Using Pretty Good Privacy (PGP) with Microsoft Outlook	138
Using Personal Certificates with Netscape	140
Verifying E-mail Senders in Outlook	141
Importing a Personal Certificate File into Opera	143
Choosing a Secure E-mail Provider	144
Using Encrypted Web-based E-mail	144
Summary	146
Solutions Fast Track	146
Frequently Asked Questions	149

Chapter 4 Self Defense on the Web	151
Introduction	152
Understanding Risk on the Web	152
Learning to Be Street Smart on the Web	154
Understanding the Privacy Policy	155
Managing Risk on the Web	159
Protecting Yourself With SSL Certificates	159
Avoiding Malicious Applets	162
Managing Passwords	164
Using Microsoft's Passport	165
Protecting Your Purchasing Power	166
PayPal and CyberCash	166
American Express Private Payments	167
Microsoft Wallet	167
Anonymous Web Surfing	168
Improving Browser Safety	169
Updating Your Browser Software	169
Internet Explorer	170
Netscape	170
Opera	170
Putting Browser Security Features to Work	171
Internet Explorer	171
Netscape	171
Opera	171
Covering Your Internet Footprints	171
Deleting Hidden Information About You	172
Opting Out of Ad-ware Cookies	176
Abacus: A Division of DoubleClick	177
ValueClick	178
Advertising.com	179
Summary	181
Solutions Fast Track	182
Frequently Asked Questions	185

**Employer-Provided
Internet Access**

According to the FBI, the vast majority of corporate information theft occurs by employees taking advantage of access to information they probably shouldn't have. Companies have every right to protect their own informational assets by monitoring how those assets are being used.

Chapter 5 Connecting to the Internet Safely	187
Introduction	188
Different Connections, Different Risks	189
Understanding Network Terminology	189
Dial-up Connections	190
America Online	192
Employer-Provided Internet Access	194
Always-on Broadband	196
DSL, ISDN, and Cable Modem	197
Cable Modem	198
ISDN Modem	199
Wireless	199
Understanding Data Interception	200
Snooping on a Network with a Sniffer	201
Snooping on Your Network with Network Neighborhood/My Network Places	203
Snooping on Your Network with nbtstat	204
Taking Precautions	207
Setting Permissions for Shared Drives and Files	208
Registering Your Domain.com	211
Turning Off Unneeded Services	212
Securing Your Personal Web Server	215
Firewalls for the Home	216
Personal Firewalls for Home Office Use	219
Network Firewalls for Home Office Use	221
Using Common Firewall Configuration Features	223
Network Configuration	223
Setting Inbound Filtering	226
Setting Outbound Filtering	227
Virtual Private Networks	228
Connection Alerts	229

SafeKids Kid's Pledge

1. I will not give out personal information, such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' permission.
2. I will tell my parents right away if I come across any information that makes me feel uncomfortable.
3. I will never agree to get together with someone I "meet" online without first checking with my parents.
4. I will never send a person my picture or anything else without first checking with my parents.
5. I will not respond to any messages that are mean or in any way make me feel uncomfortable.
6. I will talk with my parents so that we can set up rules for going online.
7. I will not give out my Internet password to anyone (even my best friends) other than my parents.
8. I will be a good online citizen and not do anything that hurts other people or is against the law.

Summary	231
Solutions Fast Track	234
Frequently Asked Questions	236

Chapter 6 Are Your Kids Putting You at Risk? 239

Introduction	240
Raising Children in the Digital Age	241
Keeping Clear Online Identities within Families	244
Supervising Online Activities	246
Channeling a Child's Interest in Hacking	247
Identifying Risky Software and Risky Behavior	250
Chat Programs	250
Web Forums and Newsgroups	252
Massive Multiplayer Online Games	253
File-Sharing Software	254
Hacking Tools	256
Monitoring Online Activities	257
Parental Contracts	258
Application Logging	260
Browser Activity Logging	261
Keystroke Logging	264
Screen Imaging	264
Avoiding Monitoring Pitfalls	265
Summary	267
Solutions Fast Track	268
Frequently Asked Questions	270

Chapter 7 If You Become a Victim 271

Introduction	272
Taking Immediate Action	272
Step 1: Filing Police Reports	273
Step 2: Reporting Fraud and Stolen Accounts	276
Closing Credit Card Accounts	276
Closing Bank and Loan Accounts	277
Reporting and Closing Other Commercial Accounts	279

Answers to Your Frequently Asked Questions

Q: I keep getting these embarrassing pop-up ads on my computer for things like viagra and pornographic sites, but I've never visited anything like that on the Web! Does this mean someone else is using my computer?

A: No. What it means is that you've visited some fairly innocuous Web site that has set a cookie or installed some spyware on your computer that is displaying those ads. If that's the case, you should follow the instructions in Chapter 4 for deleting cookies and temporary files from your computer, and blocking ad-ware. You might have installed some software that contains spyware within it. It's easy to do if you download software from the Internet frequently. If this is the case, the pop-up ads won't go away until you remove the spyware from your computer.

Dealing with Compromised Online Accounts	280
Step 3: Notifying the Federal Trade Commission (FTC)	281
Managing Other Fraud Situations	282
Reporting Stolen IDs	282
Dealing with Telephone Fraud	283
Dealing with Stolen Wireless Service	284
Managing the Fallout	284
Contacting Credit Bureau Services	285
Obtaining a Report	286
Understanding Your Credit Report: A Case Study	288
Preparing Your Victim's Statement	290
Knowing When to Seek Legal Help	292
Keeping Records	292
Locating Government Resources	292
Statutes in Your State	293
Federal Trade Commission	293
Understanding the Fair Credit Reporting Act	294
Other Suggested Resources	294
Privacy Rights Advocates	295
The Electronic Frontier Foundation	296
The Privacy Rights Clearinghouse	296
The Identity Theft Resource Center	296
Privacy International	296
The Electronic Privacy Information Center	296
The Privacy Coalition	297
The Global Internet Liberty Campaign	297
Summary	298
Solutions Fast Track	299
Frequently Asked Questions	301

NOTE

Most browsers have an option that allows you to enter your personal information profile. A form typically asks for the kind of information you'd put on a business card. The browser can then insert the information into Web forms, e-mails, or news postings without having to retype it. This feature makes life easier, certainly, but it also stores private information you might not want to be viewable by everyone. There is a small risk that the information might be shared with the wrong service, your computer could be stolen, or the information could otherwise be obtained without your knowledge.

Chapter 8 Configuring Your Browser and Firewall	305
Introduction	306
Managing Your Web Browser's Security Features	306
Internet Explorer Version 6	307
Netscape 6.2	313
Opera 6	316
Configuring Your Home Firewall	319
BlackICE Defender for Windows	319
Packet Log Menu	323
Evidence Log Menu	323
Back Trace Menu	323
Intrusion Detection Menu	324
Notifications Menu	326
Prompts Menu	326
Zone Alarm Pro for Windows	328
Firewall Menu	329
Program Control Menu	331
Alerts and Logs Menu	335
Privacy Menu	336
Email Protection Menu	337
Siemens Speedstream SS2602 DSL/Cable Router	337
Pros and Cons of Using the Siemens Router	339
Configuring the Router on the Network	339
Configuring Advanced Settings	342
Applications Port List	346
Index	357