Net Crimes & Misdemeanors

Outmaneuvering the Spammers, Swindlers, and Stalkers Who Are Targeting You Online

By J. A. Hitchcock
Edited by Loraine Page

Information Today, Inc.
Medford, New Jersey

First printing, 2002

Net Crimes & Misdemeanors: Outmaneuvering the Spammers, Swindlers, and Stalkers Who Are Targeting You Online

Copyright © 2002 by J. A. Hitchcock.

All rights reserved. No part of this book may be reproduced in any form or by any electronic or mechanical means including information storage and retrieval systems without permission in writing from the publisher, except by a reviewer, who may quote brief passages in a review. Published by CyberAge Books, an imprint of Information Today, Inc., 143 Old Marlton Pike, Medford, New Jersey 08055.

Publisher's Note: The author and publisher have taken care in preparation of this book but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book and Information Today, Inc. was aware of a trademark claim, the designations have been printed with initial capital letters.

Library of Congress Cataloging-in-Publication Data

Hitchcock, Jayne A.
Net crimes & misdemeanors : outmaneuvering the spammers, swindlers, and stalkers who are targeting you online / by J. A. Hitchcock ; edited by Loraine Page.
p. cm.
Includes bibliographical references and index.
ISBN 0-910965-57-9 (pbk.)
1. Computer crimes. 2. Computer crimes--Prevention. I. Title: Net crimes and misdemeanors. II. Page, Loraine, 1952- III. Title.

HV6773 .H575 2002
364.16'8--dc21

2002004686

Printed and bound in the United States of America.

Publisher: Thomas H. Hogan, Sr.
Editor-in-Chief: John B. Bryans
Managing Editor: Deborah R. Poulson
Copy Editor: Pat Hadley-Miller
Cover Design: Victoria Stover
Book Design: Kara Mia Jalkowski
Proofreader: Dorothy Pike
Indexer: Robert Saigh

Dedication

To my husband, Chris, who has never wavered in his support for me during the ups and downs of my cyberstalking case, who has been my biggest cheerleader when the going got tough, who has put up with my getting laws passed, traveling the country training law enforcement, being interviewed by the media many, many times, and who has endured my writing of this book past dinnertime more often than not. You're the best, hon!

Table of Contents

Figures xi

Sidebars xiii

Acknowledgments xv

Foreword, by Ray Everett-Church xvii

About the Web Page xxi

Introduction 1

You Can Be Safe Online 1

Chapter 1

Cyberstalking Happened to Me 5

Chapter 2

Words Can Hurt 19

Nina's Story 20

Andy's Houseguest 21

"I'm Your Worst Nightmare" 22

What You Should Do 24

Will It Stop? 27

Chapter 3

Spam Not in a Can 29

The Green Card Spam 31

Samsung's Sad Song 32

Usenet Spammers 36

Fighting Spam 40

Chapter 4

Urban Legends and Hoaxes: Can They Possibly Be True? 43

The David Allen Legend 44

The E-Mail Tax 46

Free Stuff 49

The Top 10 Urban Legends/Hoaxes/Chain Letters . . . 50

Educate Yourself 54

Chapter 5

Scams, Safe Shopping, and Online Banking 57

Credit Card Fraud 59

Online Shopping 61

How the Government Helps 70

Online Banking 72

Chapter 6

Auction Caution 75

"Reverse" Auction Fraud 85

Safe Bidding Online 87

Chapter 7
Where the Heartache Is: Adoption Fraud 91
Trusting Sonya 93
The Internet Twins 97

Chapter 8
Cases of Stolen Identity 99
Identity Theft Resources 105

Chapter 9
Your Personal Life Exposed 107
Askance Romance 107
Sorry, Wrong Number 109
Lawmakers Understand 110
The Amy Boyer Story 110
Unwanted Fantasy 117
The Psychology of Cyberstalking 118

Chapter 10
Ugly Beasts Lurking Online 119
Don't Feed the Troll 120
Flaming Beatles 121
Spoofing 122

Chapter 11
A Little Harmful Chat 133
Marci's Story 133
The Urge to Chat 135
A Matter of Free Speech? 136
When Chatting Becomes Harassment 137
Angela 140

Chapter 12

Other Ways They Can Get You 145

Personal Ads 145

E-Newsletters 148

Greeting Cards 149

Guestbooks 151

The Other Side of Online Auctions 154

PC Webcams 156

What's Next 157

Chapter 13

Protecting the Children 159

Agencies and Organizations Are Here to Help 162

How Bad Is It? 166

It's Not All Bad 168

How to Protect Your Child Online 173

Filtering Programs 175

Chapter 14

Office Know-How: Stay Safe in the Workplace 181

Melanie's Surprise 181

I Spy 184

Office Netiquette—More Than Just Manners 187

To Monitor or Not to Monitor 188

Chapter 15

Police Duty: Our Nation's Finest Boot Up 193

Kennebunk, Maine 193

Another Maine Unit 195

Nashua, New Hampshire 196
Massachusetts 196
Alexandria, Virginia 197
Somerset, Kentucky 197
San Diego, California 198
National Center for Victims of Crime 200
From Cop to Cybersnitch 202
SamSpade.org 203

Chapter 16
Universities Catch Up with the Net 205
GMU Has a Clue 208
UB Good 210
CMU Cares 213
A Distinct Challenge 214

Chapter 17
Encryption Made Easy 217
Encryption Is Built into Your Web Browser 217
What's PGP? 221
Electronic or Digital Signatures 226

Chapter 18
Protect Your Computer! 229
Viruses 230
Firewall, Internet Security, and Hackers 234
Firewall Protection Programs Mentioned in This Chapter 239
Putting a Spin on It 243
Passwords 248
Cookies 249

Chapter 19

Is It Spam—or Harassment? 255

First Step: Full Headers 256

Where to Go for Help Online 262

How to Find Full Headers in E-Mail and Newsgroup Programs 265

Chapter 20

A Recap: The Basics of Staying Safe Online 273

Afterword 289

Resources 291

Glossary 317

About the Author 329

Index 331

Figures

Figure 2.1 Whois.com. 27

Figure 3.1 CAUCE. 32
Figure 3.2 SpamCop.net. 40
Figure 3.3 SpamCon. 41

Figure 5.1 IFCC. 58
Figure 5.2 IFW. 58
Figure 5.3 Unlocked. 65
Figure 5.4 Locked. 65
Figure 5.5 Netscape secure. 66
Figure 5.6 MSIE secure. 67

Figure 6.1 Indiana Jones. 76
Figure 6.2 Pretty Woman. 81

Figure 9.1 Amy's smile. 111
Figure 9.2 Infidels. 112
Figure 9.3 Guns. 113
Figure 9.4 Plan. 114

Figure 10.1 Google. 124
Figure 10.2 Google results. 125
Figure 10.3 Yahoo! search. 128
Figure 10.4 Yahoo! results. 129
Figure 10.5 Yahoo! other search. 129

Figure 13.1 NCMEC. 160
Figure 13.2 SafetyEd. 162
Figure 13.3 Operation Blue Ridge Thunder. 163
Figure 13.4 Guardian Angel. 164
Figure 13.5 McAfee Kids. 167
Figure 13.6 Netscape history. 170
Figure 13.7 Netscape cache. 171

Figure 13.8 MSIE cache. 172
Figure 13.9 MSIE history. 173
Figure 13.10 Lighthouse history. 177
Figure 13.11 Lighthouse summary. 178
Figure 13.12 CyberPatrol. 179

Figure 14.1 WinWhatWhere. 185
Figure 14.2 WinWhatWhere—stealth mode. 186
Figure 14.3 SurfControl. 189

Figure 15.1 San Diego DA. 198
Figure 15.2 The National Center for Victims of Crime. 200
Figure 15.3 U.S. Department of Justice. 202
Figure 15.4 Cybersnitch. 203
Figure 15.5 SamSpade.org. 204

Figure 17.1 MSIE e-mail. 219
Figure 17.2 Netscape e-mail. 220
Figure 17.3 PGP Eudora. 225

Figure 18.1 BlackICE. 240
Figure 18.2 Norton Internet Security. 241
Figure 18.3 Jammer. 242
Figure 18.4 McAfee Firewall. 243
Figure 18.5 ZoneAlarm. 244
Figure 18.6 GRC NetFilter. 245
Figure 18.7 MSIE cookie. 252
Figure 18.8 Netcape cookie. 253

Figure 19.1 SpamCop. 257
Figure 19.2 SpamCop results. 258
Figure 19.3 SamSpade. 259
Figure 19.4 SamSpade results. 259

Figure 20.1 Yahoo! chat. 280
Figure 20.2 Compuserve chat. 282
Figure 20.3 ICQ security. 283
Figure 20.4 ICQ chat. 284
Figure 20.5 AIM. 285

Sidebars

Chapter 3	What's in a Name?	30
	On the Other Hand …	35
	How to Avoid Spam	37
Chapter 4	Good Luck, Mr. Gorsky!	48
	Is It Real?	56
Chapter 5	Sites That Offer Tips/Advice/ Comparison Shopping	61
	Make Your Online Shopping Experience a Safe One	63
	Online Scam and Fraud Statistics	68
	Top 10 Countries Reporting Internet Fraud	69
	Top 10 Countries of Alleged Perpetrators	70
	FDIC Tips for Banking Safely Online	72
Chapter 7	Adoption Resources	92
	Top 10 Online Adoption Tips	95
Chapter 8	How to Protect Yourself from Identity Theft	101
	Steps to Follow if Your Credit Card Is Stolen	103
Chapter 9	Sites about Online Stalking That Should Scare You	108
	Cyberstalking Facts	110
	Cyberstalking Estimates	114
	Cyberstalking Statistics from WHOA	116

Chapter 11 Chat Room Tips from Paul Hook of TheGuardianAngel.com 137
Common Chat Terms (Also Used in E-Mail, Newsgroups) 139

Chapter 12 Dealing with Fraudulent Personal Ads 147
Dealing with Junk You Never Requested 150
Good Guestbooks 153
Webcams Can Be Fun—if You Follow These Simple Tips 157

Chapter 13 Just for Kids 160
Monitor Your Child 165
What's a Cache and How Do You Check It? 169
How the Filtering Software Rates 175

Chapter 14 E-Mail Usage Study 182

Chapter 15 The U.S. Department of Justice 201

Chapter 16 Cyberstalking on Campus: How Prevalent Is It? 207
What Can Universities Do to Prevent Online-Related Incidents? 212

Chapter 17 Checking Your Web Browser 218
Examples of Encryption 223

Chapter 18 Common Home Computer Intrusions . . 246
Tips to Help Keep Your Passwords Confidential 248

Chapter 19 Some Tips for Contacting the Police, DA, or AG 262

Acknowledgments

Thank yous go to many people, and I know I'll probably forget someone:

My "Internet Posse"—especially the ones who stuck it out to the end, namely Cyber-Sheriff Chris Lewis, Jack Mingo, Stan Kid, Curt Akin, James Charles Rau, Mary Kay Klim, Bob Pastorio, Dick Harper, Erin Barrett, Colin Hatcher, Wayne Lutz, Crusader Rabbit, and Mary Jo Place aka "Kiki"; also Marty, Sal, Bjorn, Ellie, Marjike, Kye, and Katy Munger; and the newsgroup misc.writing. Without all of you, I never would have learned so much about the Net and how to educate others about it.

My lawyer, John Young, who took my cyberstalking case on contingency—you truly are a blessing.

My "big brother" Raymond E. Feist. He kept me sane when I was depressed about my cyberstalking case and encouraged me to keep at it when my book proposal was rejected numerous times.

My editor Loraine Page. When I groused to her that my book proposal was rejected by just about every publisher and I'd gone through three literary agents, she suggested sending the proposal to the book division of the publishing company that produces *Link-Up,* a print Internet magazine I contribute to and she edits. I slapped myself on the forehead for not thinking of it myself. If it hadn't been for Loraine, this book might never have come to fruition—and she's one of the best editors I've ever worked with.

All the people interviewed for this book—victims and experts. There are too many to mention by name, but you know who you are, and you were all wonderful to share your experiences and expertise.

My fellow volunteers at WHOA (Working to Halt Online Abuse). I couldn't ask for a better group of people to work with, and a special

thank you to Lynda Hinkle, who founded WHOA in 1997 and handed over the reins to me in 1999.

The University of Maryland University College and my boss (and friend) Art Huseonica. UMUC became one of the first universities to deal with a cyberstalking case—mine—and they handled it well (especially Rocky). I'm glad I didn't "quit teachering" after all!

Foreword

It is my happy privilege to write a foreword for a book about protecting your privacy and personal security in the Internet age. More than that, I am especially happy to write it for my longtime friend Jayne Hitchcock. Still, it disturbs me that such a book is necessary, and as I think readers will come to agree, the environment that has led to the need for such a timely book is something that should concern us all deeply.

The problems of stalking, harassment, identity theft, and the other topics covered herein are not at all unique to the Internet. For a thousand years, paupers have paraded around passing themselves off as princes, and even a few princes have skulked around in paupers' guise. But with modern technology, what was once the province of a few flim-flam artists is now available to millions.

The ease with which people—be they criminals, the news media, or just nosey neighbors—have been able to access the personal information of others, both off-line and online, has been a source of increasing concern for privacy advocates for some years now. In fact, an entire industry has grown up around the construction of massive databases filled with every shred of data about your life, your health, your finances, your buying habits, and your desires.

These databases are carefully guarded, except of course if you are willing to pay the right price; then the doors are flung open so the data can be massaged and manipulated for purposes of sending you junk mail and calling you at dinnertime. If you ask these new merchants of data why they gather and sell the personal information of consumers, they cheerfully answer that it is so that businesses can better serve consumers. This is the "just think what terrible offers we'd call you with at dinnertime if we didn't know you so well" argument.

The depressing news is that calls at dinnertime are surprisingly the happy side of this story.

There is a much darker and more sinister side to this new marketplace of personal information, a side that we are reminded about all too frequently. In recent years we have seen an explosion of news reports about stalkers and identity thieves who have bought or stolen personal information and used that data to destroy their victims' lives, both figuratively and literally.

As a law student studying under the great trial lawyer Jonathan Turley, I learned that problems are often best solved by those for whom the cost and complexity of the solution is the least. Carrying that lesson into a career in the privacy arena, I have long argued that when the practices of data collectors become a problem, those best suited to solving the problem are the ones whose activities have helped create the problem.

I do not dispute that some uses of personal information are helpful, such as credit services that help consumers get loans more promptly than in years past. Yet where more menacing uses of personal data are occurring, the data brokers have largely thrown up their hands and declared that there is nothing to be done about the many personal disasters their services have made possible. For businesses whose stock in trade is keeping tabs on people whose car payments are a few weeks past due, their apathy toward promptly fixing the destroyed credit of an identity theft victim borders on criminal negligence. As a result it can take years to fix what identity thieves can do in days.

What gives me such mixed feelings about the reasons for this book is that, as critical as it is for everyday people to understand how desperately important it is to protect themselves and their private information from misuse and abuse, the need for such a book reminds me that things are getting worse. The negligence of the data brokers in today's information age, coupled with ways new technologies are being employed to gather even more information, evokes the image of a new Wild West kind of frontier, where all men, women, and children are forced to fend for themselves.

For these reasons, books like *Net Crimes & Misdemeanors* have become urgently necessary. If our privacy is up to us to protect, we need resources like this book to teach us how to assert our right to be left alone. We should all be thankful that Jayne has assembled a balanced and thoughtful resource for teaching us all how to sail through our lives in the information age, leaving fewer broken bits of our privacy floating in our wake.

When I think about why Jayne Hitchcock is such a perfect person to help average folks learn to protect themselves, I am reminded of an illustration from a political event many years ago. In 1987, I had the privilege of working for then-Senator Al Gore on his first campaign for president. At a fundraising breakfast he thanked everyone for coming to the event and expressed his appreciation for their involvement in his fledgling campaign. But, he exhorted the crowd, it was now time for each of them go a step farther, to move from just being involved to being fully committed to the campaign.

To illustrate the difference between involvement and commitment, he pointed to a plate sitting on the head table, still piled high with scrambled eggs and country ham. "Just looking at this fine breakfast, the difference between involvement and commitment is clear," he continued. "The chicken was involved. But the hog is committed!"

There are a growing number of very excellent books on the market discussing the perils of privacy invasion and threats to personal safety coming both online and off-line. But for the vast majority of those authors, their relation to the issue is much more akin to the relationship between the chicken and that breakfast plate: they have an expertise and interest sufficient to inspire them to take on the task of writing a book. For Jayne, it is something much deeper than that. This book is evidence of her passionate commitment to make sure that others are not forced to live through the nightmares.

Unfortunately, it is a commitment that was forced upon her in an especially awful way.

It was while doing some consulting work for America Online (AOL) that I first met Jayne. AOL had asked me to help them develop and enforce policies regarding Internet abuse, including "spam" and other inappropriate uses of network resources. In the course of that work, I spent a lot of time working on problems related to the Internet discussion boards called Usenet newsgroups.

In culling through piles of complaints and abuse reports, I noticed a sizeable number of complaints relating to a few newsgroups devoted to creative writing. The more I delved into those reports, the more complicated and sordid the tale became. Before I realized it, I was smack in the middle of Jayne's protracted battle with cyberstalkers. I will not steal her thunder except to say that it was, at the time, both gripping and deeply disturbing to see the harassment, abuse, threats, and intimidation heaped upon Jayne by a band of thugs.

Reflecting upon the circumstances that give Jayne such intimate knowledge of these issues, the old adage "that which does not kill us

makes us stronger" comes to mind. I must admit however that I use that phrase with some trepidation. For me, that phrase has always seemed particularly infuriating, offered up as consolation from bystanders to the struggle, as if it actually helped to soothe a wound. As maddening as that saying can be, it is nevertheless apt. The horrific circumstances through which Jayne passed not only made her stronger, but made her something more: a passionate and articulate advocate for those who, like her, have landed in the sights of the deranged and disturbed.

It is so very understandable that many who have experienced a loss of privacy and security would seek to return to an anonymous life as quickly as possible. That is why I am amazed at how often people choose to turn the trauma of such events into action. But I am happy to report that Jayne Hitchcock is no shrinking violet—not by any means! She chose to see her struggles as a challenge laid, a gauntlet thrown. That which did not kill her did indeed make her stronger, turning her into a fierce advocate for victims of abuse.

The encouraging irony is that such ghastly incidents often turn victims into some of the world's most effective advocates for change. One would never wish hardship on anyone, yet if there was an easier and more pleasant way to inspire good people to draw such strength from deep within themselves, I wish we could reproduce it and put it in the drinking water. Until that day, we have books like this and people like Jayne to show us not just how to survive, but to reassert control over our lives so we can thrive and prosper in this new frontier.

I urge you to read carefully and let these lessons help you to assert your right to privacy and take charge of your own life again. And who knows? Some day, you might even get to finish your dinner without being called to the phone.

Ray Everett-Church, Esq.
San Jose, CA

Ray Everett-Church, a senior privacy strategist at ePrivacy Group, is an internationally recognized expert on privacy law and Internet-related public policy. He is an advisor to the Privacy Officers Association and a member of the National Advisory Council of The George Washington University School of Engineering and Applied Science. A graduate of George Mason University, he received a law degree from the National Law Center at The George Washington University.

About the Web Page: netcrimes.net

The world of online information changes with each blink of the eye, and the limitations of any print volume covering Internet resources are obvious: New sites and resources appear every day, other sites are expanded to include new or enhanced features, and still other sites disappear without a trace.

At netcrimes.net, the author is maintaining a regularly updated directory of key Internet resources—including, wherever possible, active links to sites (you must have an Internet connection and WWW browser to utilize these links). This directory is designed to help you pinpoint sites offering specific types of help and information, and to keep you up-to-date on the trends and issues. It is being made available as a bonus to readers of *Net Crimes & Misdemeanors*. Please take advantage of the feedback feature at the site to let us know what you think, and to recommend additional sites that readers may find useful.

Safe surfing!

Disclaimer

Neither publisher nor author make any claim as to the results that may be obtained through the use of the above mentioned links to Internet sites and resources, which are maintained by third parties. Neither publisher nor author will be held liable for any results, or lack thereof, obtained by the use of any links, for any third party charges, or for any hardware, software, or other problems that may occur as a result of using netcrimes.net. This program of Internet resources and links is subject to change or discontinuation without notice at the discretion of the publisher.

Introduction

You Can Be Safe Online

You wouldn't walk down a dark street in an unfamiliar neighborhood alone, would you? You wouldn't divulge where you live or work to a stranger in an elevator, would you? Surprisingly, many otherwise sensible people throw caution to the wind when they're online, assuming, apparently, that they're completely safe. They're not, no matter how computer savvy they think they are.

Danger lurks on the Internet.

Consider these scenarios:

- You purchase bath products from an online shopping site. When you receive your credit card bill, you find there are several more charges on it…and you didn't buy anything else.
- You go to an online auction, bid on a photograph "signed" by a celebrity, and win. You send in your payment and wait. And wait some more. You do some investigating and find that not only are you not going to get the photograph you paid for, but there are serious doubts about the authenticity of the autograph.
- You receive phone calls and knocks on your door from strangers—all in response to a message "you" placed online. Only you don't own a computer.
- You're on a newsgroup called alt.business.home and someone gets angry at an innocent question you've asked. Messages begin to appear from "you" insulting other people in the group. This results in a barrage of e-mails to you from the

people "you" offended. Your e-mail account is canceled, and your employer receives phone calls from people complaining that "you" are harassing them online.

You may think you know better than to get caught up in a scam or a harassment situation. But I will show that it can happen to even the most experienced online user. It happened to me. In 1996, I thought I knew everything about the Internet. I'd already been online a number of years, was a teaching assistant for basic and advanced Internet courses at a university, wrote hardware and software reviews for magazines, participated in newsgroups and forums, and surfed like a pro. Then I unwittingly became the victim of Internet harassment so threatening that it changed my life. Read my story in Chapter 1.

Net crimes and misdemeanors are committed against more than 60,000 people a year, and the number is growing every day, according to statistics from the FBI and victim advocate organizations. NUA Internet Surveys (www.nua.com) estimates there are more than 500 million people online worldwide. If only 1 percent become online victims, that is still over five million people—a drop in the bucket as more people go online for the first time every day.

When my harassment occurred, I didn't know where to go for help. There certainly was no book available to explain things to me, and there were no laws to protect me. Because what happened to me was so extreme, and because I saw such a lack of understanding of cybercrime, I have since become one of the nation's leading cybercrimes experts, giving lectures nationwide and appearing on TV programs to get the word out about Internet crimes. I serve as president of Working to Halt Online Abuse (WHOA), a group that works with more than 100 online victims a week.

The media has given some coverage to this growing problem, but not enough. It tends to emphasize sensational cases without imparting safety information to the public. I give lectures and training workshops to law enforcement personnel around the country, and am always surprised at how few of those in attendance are up-to-date on online harassment and cyberstalking issues. I've been told time and again that a book explaining what can occur and offering preventative measures would be welcome.

That's why I decided to write this book.

Net Crimes & Misdemeanors is written in language that is easy to understand if you are not familiar with the online world, but it is not written so simply that experienced Internet users will find it too basic. Each chapter begins with an explanation of the chapter's focus—and

sometimes a definition or two of online harassment terms—and includes one sample case or more to show that even smart folks can have bad experiences. This is followed by tips and advice from experts. If, as you're reading, you come across a computer term you're unfamiliar with, check the Glossary in the back of the book. If you see an organization or a product you want to know more about, check the Resources section for the Web site address. In addition, there is an official Web site for the book at www.netcrimes.net, where you will find an updated list of links from the book and other links that may be of interest.

This book is only a first step in learning how to be safe online. To be truly Net-savvy, you'll have to keep vigilant long after you've read these chapters. Though I am known as a cyberstalking expert, I always keep an eye open for the latest developments in the world of online safety. If you and I don't remain alert, danger could strike. I don't know about you, but I don't intend to let it happen to me—not again.

A note on the case histories: Some of the victims I describe are actually composites of people from cases I've worked on through WHOA; I have done this to keep those victims anonymous. Some victims allowed me to use their real names, and others allowed me to use their stories verbatim but asked me to use pseudonyms. When recounting case histories, sample e-mail messages, posts, or chat room transcripts, they are exactly as they appeared online—with grammatical and spelling errors intact. Profanities are not spelled out, however, because I wanted parents to be able to share the information in this book with their children.

Don't let trolls, spoofers, spammers, e-mailbombers, cyberstalkers, and other online miscreants make you live in fear or give up the many advantages of Internet use. In reading this book, you've already taken the first step to arm yourself.

You're on your way toward becoming safe online.