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.