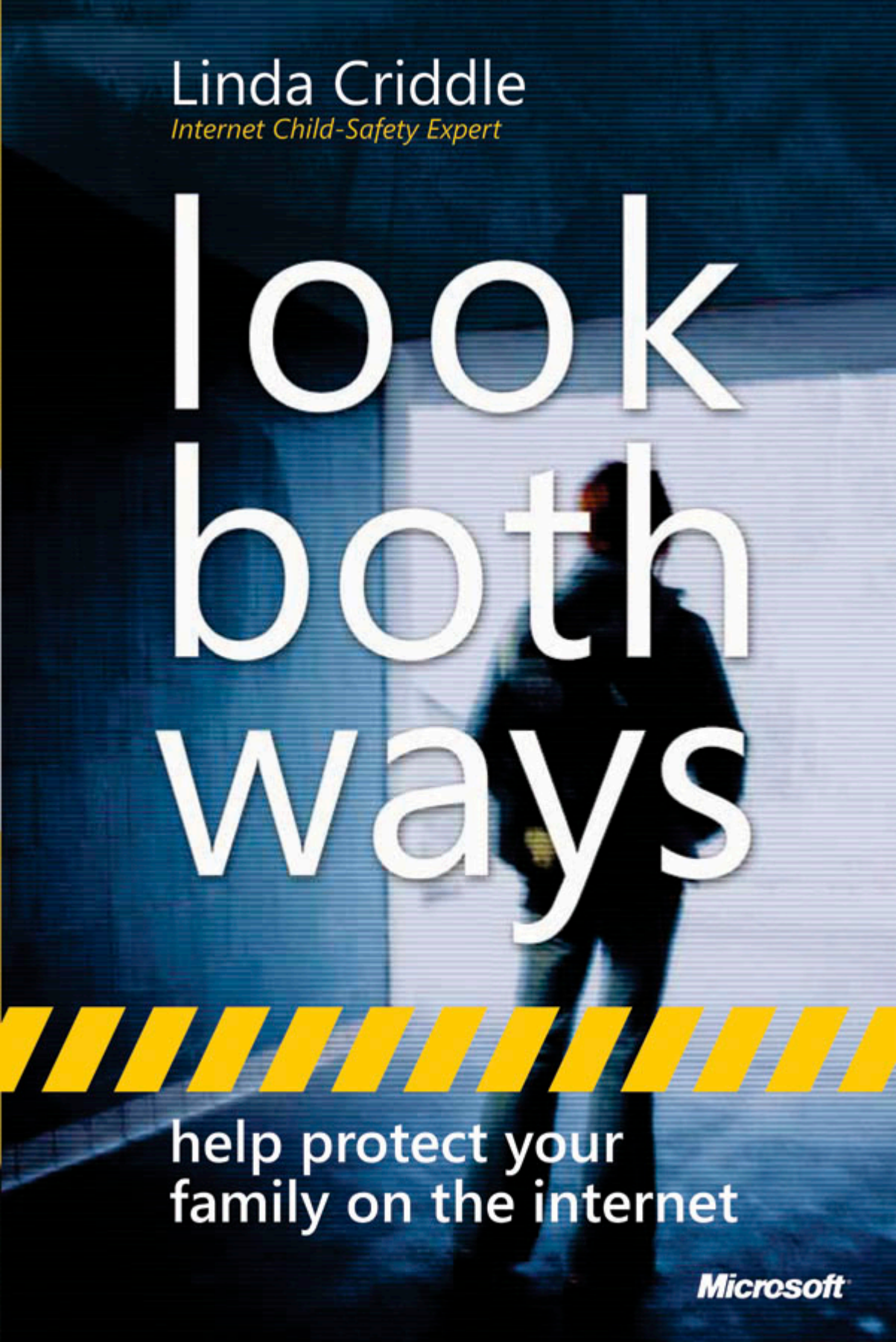
Linda Criddle
Internet Child-Safety Expert

look both ways



help protect your family on the internet

Microsoft

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Control Number: 2006927199
978-0-7356-2347-7
0-7356-2347-3

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9 QWE 1 0 9 8 7 6

Distributed in Canada by H.B. Fenn and Company Ltd.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at www.microsoft.com/mspress. Send comments to mspinput@microsoft.com.

Acquisitions Editor: Juliana Aldous Atkinson
Developmental Editor: Sandra Haynes
Project Editor: Melissa von Tschudi-Sutton
Artist: Jessie Good
Project Management: Publishing.com
Compositor: Curtis Philips
Copy Editor and Proofreader: Andrea Fox
Indexer: Wright Information Indexing Services
Design: Happenstance, Maureen Forys

Body Part No. X12-64008

Table of Contents

CHAPTER ONE

The Landscape of Risk

Marty's feeling good tonight; his law firm just won a big case, and it's a sure bet he'll make partner before his 45th birthday next month. He checks on his wife, and she's watching TV in the living room, starting to doze. He grabs a drink and settles down in front of his computer in the den. Marty logs on to the Internet, turns off the computer speakers so his wife won't hear anything, and types in a **URL**.

Marty discovered Stella a couple of months ago. She's 14 and lives in a nearby city. Like most people, her online journal, called a **blog**, *tells more about her than she realizes, and, like most blogs, it was set up by default to be wide open to the public. In her blog profile she lists her birthday, city and state, her favorite movies, and favorite color. Her blog name is 2SexyStella, and the picture she's posted on her blog space is that of a slim young girl with big eyes, tight jeans and halter top, and the slouching posture of a teen who is unsure of herself and self-conscious, but trying hard to look cool.*

When he first came across Stella's blog, Marty was attracted to her photo, so he started checking her Web site regularly. When Stella posted a complaint about having an argument with her mother, Marty saw the opening he'd been waiting for. He posted a sympathetic and supportive response. He sided with Stella against her mom, introducing a wedge between them, and slowly taking on a role as a confidante. After a few more exchanges through her blog, Stella gave him her e-mail address. They've been e-mailing and **instant messaging** *each other for weeks now. It never ceases to amaze Marty how*

much information people provide about themselves, their family, and their friends without even realizing it.

For her part, Stella was thrilled to find that Marty was so cute, and only a few years older than her. He thinks she's the most wonderful person alive. They have so much in common! They love the same movies and even share the same birthday. They've swapped pictures of their families and houses. (Stella never realized the photo of her sitting on her front porch contained the house number and a street sign in the background, so now he knows where she lives.) She's just excited by how this 17-year-old guy flirts with her.

In his last e-mail, Marty asked if Stella had a digital camera, and they began sharing personal photos using instant messaging. The first picture he asked for was innocent, but now that he's established the connection, who knows where this friendship could go?

What's Going On Out There?

There was a time when you had to leave your house to shop, hang out with friends, visit the library, or meet a date. That's changed: Now you can do all this and much more online. The Internet has enabled fantastic opportunities for education, social contact, and entertainment, and it enriches hundreds of millions of lives every day. For most people, most of the time, that convenience is a tremendous asset and the Web is a powerful tool. But just as there are potential dangers any time you get into your car and drive across town, there are potential dangers on the Web.

What the Internet does for "good" people, it also does for "bad" people: It gives broad access to people and information and allows users to remain largely anonymous. Criminals leverage any tool they can to commit their crimes; their latest tool of choice is the Internet. Often referred to as **cybercriminals** or predators, these individuals are committing a wide variety of offenses from **identity theft** and harassment to stalking and assault. Is what's going on all that different from what criminals have done for years and what you've learned to protect yourself from offline? No. Only the tools at their disposal have changed.

That there are bad people out there is a fact of life, but the existence of cybercriminals should not force you to avoid the Internet any more than you avoid walking or driving because a bad driver might do you harm. You walk down the street without fear because you learned as a child to *look both ways* and cross streets safely. The same is true for the Internet. You can use this powerful tool safely if you understand not only the opportunities

the Web provides, but also the risks and what you can do to mitigate those risks. Then you can make choices that provide the level of protection you want for yourself and your family.

Who Are These Cybercriminals?

If you have a particular image of the type of person who commits these types of crimes, it's probably wrong. **Predators** come in every age, shape, and gender and live in any part of the world:

- Many are well-respected business or professional people who appear to be upstanding citizens.
- Sexual predators who target minors are predominantly, though not exclusively, male (95 percent; Wolak et al., 2004).
- Predators might act alone, in loose groups, or in formal gangs. Even organized crime syndicates are cashing in on people's online vulnerabilities.
- There is also a "middleman" predator class out there, assembling publicly available information into virtual catalogs and selling that information to anybody willing to pay. Some of these catalogs contain mundane information such as your preference in soft drinks and TV programs, but other catalogs list your identity, home address, age, photos, and other identifying information.

Find Out More
For more detail about who predators are and their behavior, see Chapter 3, "Thinking Like the Enemy: Predatory Behavior."

Who's Vulnerable?

Who could become an online victim? Quite simply, anybody. Whether you go online yourself or another person or company puts information about you online, there are risks. Depending on the type of information out there, your risk might be fairly low or significant. Children are at special risk because of their high volume of online activity and naïveté about human nature. However, people of all ages, even those who make their livings in law enforcement and computer security, are astounded when I point out what information is being shared online and with what consequences.

Think About It

The most critical years for children are around ages 13 to 15, when they begin to reach out and form relationships with others. These kids are often not streetwise, and they are looking for validation and approval, rebelling against their parents' values, and drawn to the latest technologies. They are discovering who they are and enjoy trying on other identities. Online predators know this and take full advantage of it (Wolak et al., 2004).

But, you say, you use **antivirus software**. You regularly scan to rid your computer of **spyware**, and you turned on your computer **firewall**. You even have **content filtering** installed to try to prevent your kids from viewing pornography. But consider this: *It's not just about technology; it's about your online behavior.*

A firewall is useless against financial fraud. If your elderly mother willingly responds to an e-mail purporting to be from her insurance company, asking her to provide her bank account information for a direct deposit of a refund, all the software in the world won't help. There's no antivirus program on the planet that will protect your daughter if she posts messages on her blog that give away her location, her age, and her vulnerable emotions.

Think About It

Once you have technical protections in place, you might well be the biggest remaining risk factor. But because your behavior is in your control, you can feel empowered to reduce your risk online.

How Big Is the Problem?

The Internet provides unparalleled opportunities for instant access to information and helpful services. Unfortunately, cybercriminals are among the most adept at leveraging these new technologies, and have embraced the Internet to facilitate their criminal behavior.

When you include cell phone Internet services, there are over 2 billion people worldwide with Internet access. Within the United States alone, there are over 21 million kids online, according to the Pew Internet & American Life Project. Cybercriminals are keenly aware of the opportunity and are targeting these groups accordingly.

The magnitude of the abuse problem is proportional to the number of potential victims. Consider that

- In Canada, 94 percent of kids report they have Internet access from home (Media Awareness Network, 2005). In the United Kingdom, 90 percent of children have a personal computer at home, and 75 percent have Internet access (*www.childwise.co.uk*).
- A 2004 study by the National Cyber Security Alliance and America Online found that 80 percent of home computers are infected with spyware or **adware**, and 63 percent of users have encountered a computer **virus.**
- In 2005, the worldwide financial impact of **malware** (virus, spyware, and so on) attacks was $14.2 billion, according to *www.computereconomics.com*.
- Testimony given before a U.S. congressional panel (April 2006) noted that commercial child pornography on the Internet worldwide in 2005 was a $20 billion business. The trade in child pornography in the United States alone is estimated at approximately $3 billion.
- 12 percent of Web sites include pornography, and 25 percent of **search engine** requests are for pornography, according to *www.familysafemedia.com*.
- One in five children ages 12 to 17 are sexually solicited online every year in the United States (according to the National Center for Missing and Exploited Children, NCMEC), and a similar number is estimated in the United Kingdom (according to the Internet Crime Forum).
- In the year 2000 there was an average of 220 arrests a month for Internet sex crimes against minors in the United States (Wolak et al., 2003). But the problem is worldwide: Law enforcement agencies around the world are expanding their online criminal units to combat the growth of online crime.
- One account of a teenage boy who sold sexual images of himself via webcam reported that he had 1,500 customers. The majority of these were professionals such as doctors, lawyers, businesspeople, and teachers.

How Are You Putting Yourself at Risk?

You are in danger on the Internet from two directions: inbound and outbound (see Figure 1-1). Spam, viruses, and spyware flow toward you through e-mail, instant messaging (IM), Web sites, and so on. They can be downloaded onto your computer without your knowledge. There is much you can do to protect yourself from these threats, and most online security books focus on this kind of defense. (See "Technology Toolkit" in Part Four for my basic advice about implementing technical protections.)

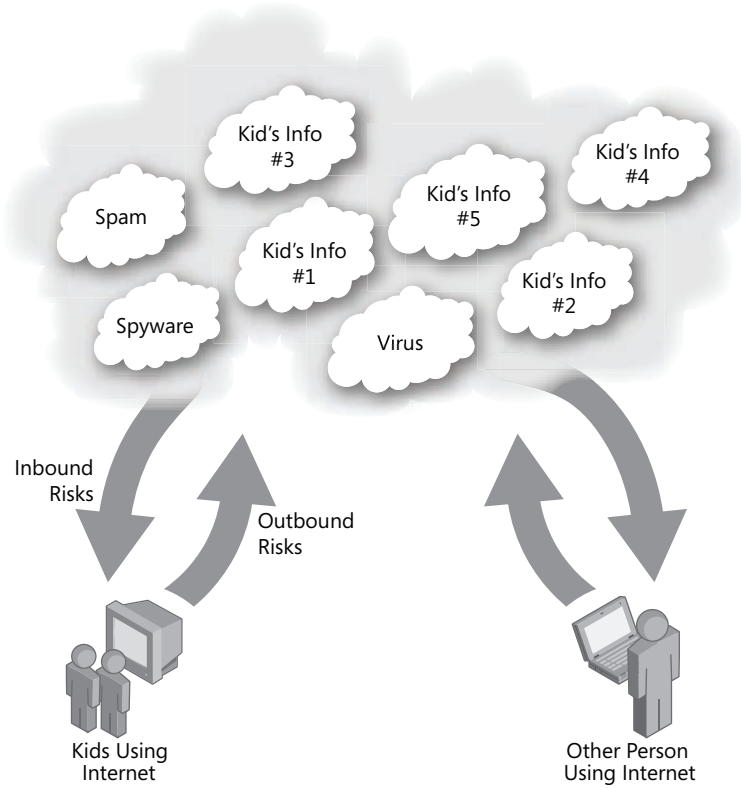


Figure 1-1 Risk flows both ways online.

Perhaps more dangerous are outbound risks; these occur when you willingly (though often unwittingly) reveal information about yourself through the data you put online every day. You might be providing the very information cybercriminals need to take advantage of you. Outbound risk is the focus of this book.

One of the most important things you can do to reduce your own vulnerability is to grasp this one concept: Every piece of information about you is a valuable commodity. Publically available user information has the potential to be tracked, cataloged, analyzed, and sold, both legally and illegally.

The fact is that many people, particularly but certainly not exclusively children, are making available a variety of information via the Web that makes them identifiable and places them at risk every day.

> **Find Out More**
> For more about how to avoid giving away too much information about yourself, see Chapter 5, "Step 2: Don't Tell People More Than You Should."

What kind of information are people putting out there? I'm not talking about your bank account or social security number—you wouldn't deliberately give those to strangers any more than you would hand somebody your wallet. I'm talking about seemingly useless information about you, from your favorite book to your age, the color of your eyes, and even what makes you sad or happy. Using that information and a few facts about you, such as your name and address, a predator can find you and use key information about you to either impersonate you, steal from you, or initiate a relationship.

Think about what you or your friends have shared online about you, and the people out there who might use that personal information to impersonate or approach you, and then consider these statistics:

- 67 percent of teen bloggers provide their age; 54 percent provide specific demographic information; 61 percent provide contact information; and 39 percent include their birth date (Huffaker et al., 2005).
- 76 percent of victims of online sexual exploitation are found via **social networking** applications such as **chat rooms**, **discussion boards**, and blogs (Wolak et al., 2004).
- 63 percent of all bloggers use **emoticons** (little icons that show their emotional state) (Huffaker et al., 2005).
- Approximately 50 percent of people blogging are doing so as a form of self-therapy (The AOL Blog Trends Survey. Digital Marketing

Services, Inc., 2005). (This means that they are emotionally vulnerable and might reveal more than they should about themselves.)

Remember that you control the level of your exposure through the information you place online. Risk is commensurate with the choices you make about the type of content you post, the breadth of contacts you make information available to, and whether you share information about others as well as yourself. The more personal the information you choose to share, the more careful you should be to share only with close friends and family (see Figure 1-2).

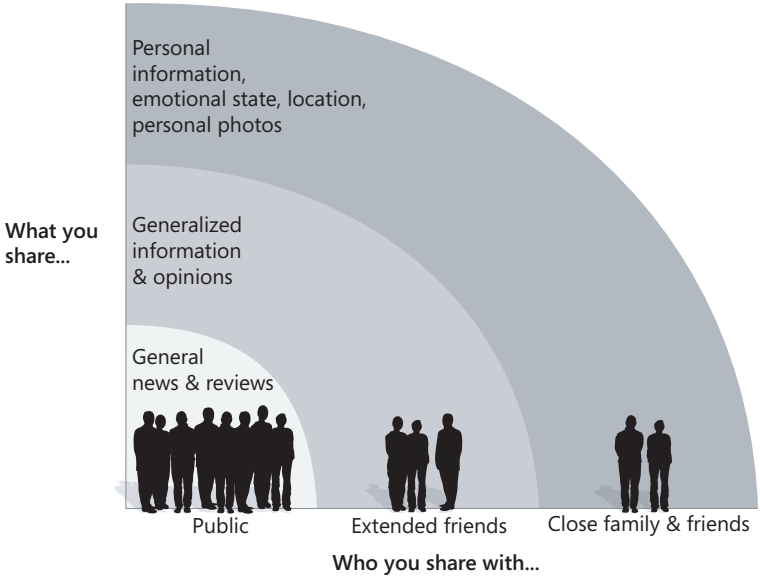


Figure 1-2 The amount you share online should be determined by your intended audience.

Think About It

Sit down and make a list of all the information about you that might interest a cybercriminal. Check off the items you've made available online in any fashion. Search on your name to see what information you can find. When you go online, think about exactly what you want to share with total strangers, and what you want to reserve for more trusted groups of people.

What Can You Do?

So, what's the answer to avoiding risk? Do you disconnect your computer, cancel your Internet service, and hide under your bed, safe from all that online danger? Of course not. Just as your parents taught you to be careful when you walk around town, to obey the school crossing guard and look both ways before crossing a street, you simply need to learn how to look both ways when you move around the Web.

Think of it this way: Cars, buses, and trucks are wonderful tools, but they can be dangerous in certain circumstances. According to the Department of Transportation, in the United States alone, over 40,000 people die every year in traffic accidents. To mitigate the risks, you teach your children about traffic safety. You don't avoid walking across the street for fear of all the danger out there because you know the rules and how to protect yourself.

Making the Internet Safer for Your Family

The Internet is also a wonderful tool, offering a vibrant world of interaction and information. The problem is that nobody taught you or your children how to be online safely because the entire online world didn't even exist in its current state 10 years ago. That lack of training has left you and your family open to a variety of risks online. Fortunately, these risks can be minimized by taking a few easy steps.

I wrote this book to give you some of the tools you need to act safely on the Web and take advantage of all the positive things it has to offer without fear. Some of these tools involve technology. The good news is that, more and more, safety measures are being built into the software you use every day—your operating system and browser, for instance. There are good tools out there and you should use them. But remember: The most important step you can take, starting today, is to educate yourself and your family about the risks and make informed choices about your online behavior.

Taking the First Step

I won't tell you to never post a picture online, to dismantle your blog, or to never have an online date; that type of advice makes about as much sense as telling you to never leave your house or never cross a street to avoid being hit by a car. What I will teach you is how to recognize some common risks and predatory behavior, how to come to an educated decision about

your personal risk tolerance and comfort zone, and how to define a framework for online interactions for you and your family.

If you're a parent, you have to move beyond the idea that Internet security is something you can "do" to your kids by following them around online. Just as you can't follow your kids all around town during the day, you can't be there every minute they spend online. Instead, with a few simple steps you and your family can learn how to protect yourselves with a three-tiered approach of education, infrastructure, and enforcement.

When cars came into peoples' lives, society had to do that same thing. People *educated* themselves about how to drive and cross streets safely, they created an *infrastructure* of roads, sidewalks, street signs, and regulations to keep drivers and pedestrians safe, and they *enforced* those regulations. That same approach is necessary when you drive around online. For the time being, however, that education, infrastructure, and enforcement might rest mainly in your own hands as schools and government scramble to come up with solutions and put them in place.

Find Out More

See Chapters 17, "Talking About Safety," and 18, "It Takes Everyone to Make a Safe Internet," for more about how to implement this three-tiered approach in your family.

You Are Not Alone

Internet companies and regulatory authorities are becoming much more aware of the problem and are taking action. Companies are investing in online safety. Laws have been created to facilitate the prosecution of a wide variety of online crimes.

As this book goes to press, the U.S. House of Representatives is holding hearings on the sexual exploitation of children, and there are several Internet safety proposals up for consideration. Funding for the Justice Department Internet Crimes Against Children (ICAC) program jumped from $2.4 million in 1998 to $14.5 million in 2005.

In France, a law has been passed requiring all Internet service providers to provide content filtering features. Governments around the world are mobilizing to provide educational materials and regulatory infrastructure. The United Kingdom has established a crime unit, CEOP, to target online child sexual predators. The Royal Canadian Mounted Police and Microsoft have jointly developed a tracking system (Child Exploitation

Tracking System, or CETS) to facilitate the discovery and prosecution of child sexual predators. Australia has established a safe ISP program called Ladybird, and similar programs are being created around the world.

The news is hopeful for a better Internet in years to come. But the strongest link in online safety today is you.

What's Next?

The 13 chapters in Part Two of this book provide 13 simple steps you can take to protect yourself and your family. Part Three gives you advice on putting those steps into action.

Just as you learned to look both ways as you were crossing the street when you were young, you can learn to look both ways and use the Internet more safely, without fear.

CHAPTER NINE

Step 6: Reduce Your Vulnerability When Blogging

Caroline's family had just moved to a new town, and she missed her friends in Brisbane. She decided that a great way to keep in touch would be to start a blog. All the kids at her new school were getting into blogging, so it would be a good way to make new friends, too.

Caroline found the sign-up process for her site easy to work through. Eager to get started, she accepted all the default settings and typed in her city and state in Australia. She thought that a racy nickname might make the kids at her new school think she was cool, so she chose "NaughtyCaroline." She entered her contact information and customized her Web address using her last name and the year she was born so she could remember it easily.

Caroline tried to make the background of her site look impressive (like many 14-year-old girls, she loves hearts and hot pink) and added a bunch of photos of herself and her friends with labels identifying them and the scenery in the photos. She also created a list of her favorite songs and posted it to the site.

Her new friend Amy came over to look at the site one Saturday morning and said it still looked kind of empty. Together the girls downloaded and filled out a few quizzes, challenging each other to come up with more and more outrageous answers. One survey asked how many beers she drinks in a week, and Amy taunted Caroline to say a dozen. In fact, Caroline doesn't drink at all, but she wants Amy to think she's sophisticated, so she entered 12 for her answer.

Over the next week, Caroline made lots of journal entries, finding that it was liberating to write about herself. In one entry, she mentioned her most recent fight with her mother, and admitted to being kind of lonely since she and Nigel broke up. She added that she's hoping to meet a "hot guy" when her family goes on vacation in Perth next week. Now that her blog isn't looking so empty, Caroline sends an instant message to her old and new friends telling them to check out her site.

She doesn't know that several online predators have already seen her site and are already getting to know her–really well.

What Just Happened?

Caroline just did something more common than you'd expect: she created her own blog without a clue about the safety risks. She didn't stop to consider that the default setting for her site is "viewable by the public" and that anyone with Internet access can see everything she's shared, including

- Her name
- Her friends' names
- Her family members' names
- Pictures of herself and others
- Where she lives
- Where she goes to school
- That she's lonely and fighting with her mother
- That their house will be empty next week

It never occurred to Caroline that anyone other than her friends can read her blog, that her information is now searchable by Internet search engines, or that she might have placed herself, her family, her home, her friends, and her possessions in harm's way.

Let me be clear about this: There is nothing at all "bad" about public blogs or other publicly posted content as long as you consider and make a clear decision about what you feel is appropriate to share with the public. There are literally millions of wonderful public blogs that are not placing their authors at any risk. But if you share personally identifying information about yourself or others, you should do so with a full understanding that this could easily be used by others.

Find Out More

See Chapter 17, "Talking About Safety," for information about how to create a family discussion guide to set parameters for online behavior in your family.

What Is a Blog?

Blogs, short for W*eb logs*, first appeared when journalists in remote places wanted to post stories and commentary about their war-time experiences that they couldn't get out through other communication channels. Blogs then went mainstream, becoming personal online journals where entries could be posted by the blog owner and comments added by those visiting the blog. This frequent updating and interaction makes blogs much more dynamic than most Web sites. Each blog entry usually contains a title, a profile of the author, a date stamp, photos, and the poster's comments. They might also contain lists of favorite music and books, maps, videos, search tools, quizzes, and so on. Businesses and organizations have also jumped on the blogging bandwagon to offer information-rich sites that encourage interaction among their readers or users.

Blogs are social networking sites (Web sites that connect people and allow them to communicate with each other) *if* the blog owner includes contacts in the blog so that visitors (select friends and family or the public) can communicate with those people and thereby extend their networks.

Assessing the Risks

Blogs offer an environment where people can share their ideas and feelings with friends and family or with others who have similar interests, or even with the public at large. They encourage creativity, expression, and interaction. Blogs enable people to get involved and have a voice in politics and news reporting and other forms of participatory citizenship. They enable people to meet new friends and expand their horizons. So what makes people anxious about blogs?

The Blogging Phenomenon

There are more than 70 million blogs online today (*www.blogherald.com*). I've talked about blogs frequently throughout this book, in part because they are a relatively new tool for the general public and have become a wildly popular trend that is often in the headlines, usually because of abuses.

Unfortunately, a small segment of the population uses blogs in hurtful and illegal ways. Predators and bullies use the information that was intended to allow expression and inspire contact to spam, con, stalk, harass, and groom victims of every age. In a microcosm, blogging reinforces the point that anything new and popular, such as the Internet itself, poses problems in part just because it is new. People simply haven't learned about the potential risks and don't know how to blog safely.

Criminals and Blogs

As I mentioned in Chapter 1, "The Landscape of Risk," about half of all those who blog use their blogs as a form of emotional therapy. Because the blog format often is geared toward enabling people to reveal their attitudes, feelings, and personal information in a public way, they are attracting predators and criminals who hunt for the emotionally vulnerable or unwary. As in the real world, where you're advised against looking distracted or passive when walking alone, projecting an emotionally vulnerable face to the general public in a blog is an invitation to cybercriminals and predators.

Think About It

According to WiredSafety (*www.wiredsafety.org*), in 2005 about one-third of students in the United States had Internet blogs, although only about 5 percent of parents were aware of that fact.

Remember, the creators of the Internet didn't invent criminals or predators. The people who commit crimes online are the same people who commit crimes in the physical world. The Internet and the services enabled by it, such as blogs and social networks, are just new tools for them to use.

The Information Connection

All types of cybercriminals leverage information posted online to help them identify opportunities. Identity thieves look for identifying information, robbers look for items to steal, scam artists target people who seem susceptible to scams, and sexual predators search for victims. Middlemen aid these criminals by building catalogs of people and items that might be of interest: information about children, identities, addresses of homes whose owners are away, and locations of valuable cars. A lot of the leveraged information is gleaned from publicly accessible blogs, where people unthinkingly post all kinds of data about themselves.

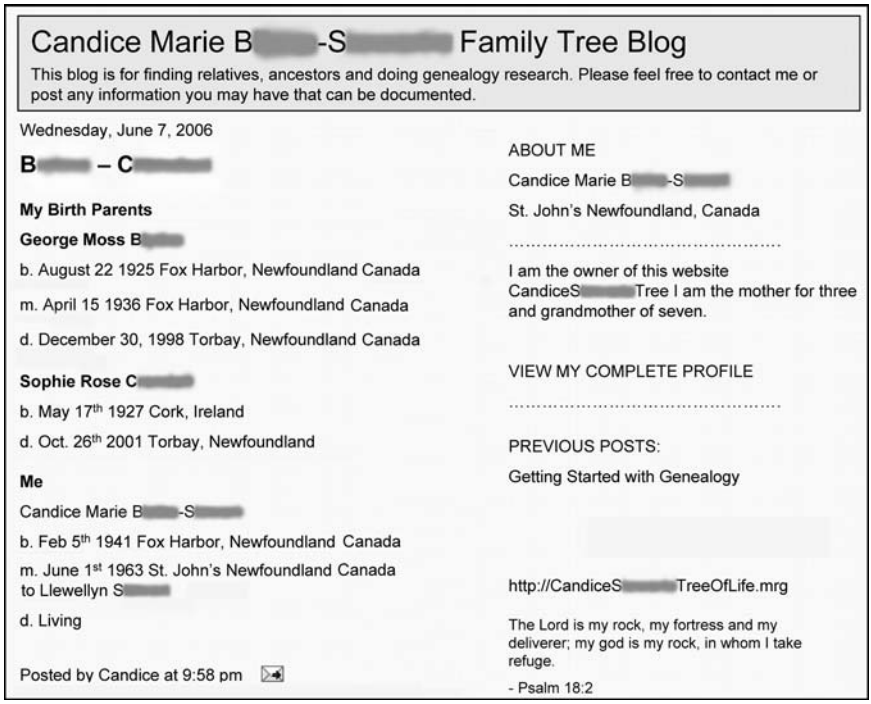
While much of this information is provided by the victims themselves, sometimes it is unintentionally provided by friends or family members. It is the cybercriminal's ability to find *in one place* pieces of information that have been left over time by multiple people that gives him or her an advantage over other criminals, who have no such repository of information to sift through.

What You Expose About Yourself and Others

Bloggers expose their information in a variety of forms—from text descriptions of their feelings to photos and videos, music preferences, voice clips, lists of favorites, and maps.

A blog's topics can also reveal personal information. For example, adult and older bloggers are often interested in their family tree and genealogy research and frequently post all this information online (see Figure 9-1 on the next page), providing full names, mother's maiden name (a frequent password prompt used by online sites and financial institutions), birth dates, locations, marriage information, and so on, going back several generations. This is an identity thief's dream come true.

Information can also be discerned from a blog's background motif, a blogger's nickname, a Web URL (www.blogsite.Cecil24livin'thelifein-Victoria or www.blogsite.RobWalters26, for example), emoticons displayed, quotes, address field information, relationship status, or a biography. Figure 9-2 on page 77 shows a typical blog that provides a lot of information about its owner and is publicly posted.


Candice Marie B[redacted]-S[redacted] Family Tree Blog

This blog is for finding relatives, ancestors and doing genealogy research. Please feel free to contact me or post any information you may have that can be documented.

Wednesday, June 7, 2006

B[redacted] – C[redacted]

My Birth Parents

George Moss B[redacted]

b. August 22 1925 Fox Harbor, Newfoundland Canada

m. April 15 1936 Fox Harbor, Newfoundland Canada

d. December 30, 1998 Torbay, Newfoundland Canada

Sophie Rose C[redacted]

b. May 17th 1927 Cork, Ireland

d. Oct. 26th 2001 Torbay, Newfoundland

Me

Candice Marie B[redacted]-S[redacted]

b. Feb 5th 1941 Fox Harbor, Newfoundland Canada

m. June 1st 1963 St. John's Newfoundland Canada to Llewellyn S[redacted]

d. Living

Posted by Candice at 9:58 pm

ABOUT ME

Candice Marie B[redacted]-S[redacted]

St. John's Newfoundland, Canada

I am the owner of this website CandiceS[redacted]Tree I am the mother for three and grandmother of seven.

VIEW MY COMPLETE PROFILE

PREVIOUS POSTS:

Getting Started with Genealogy

http://CandiceS[redacted]TreeOfLife.mrg

The Lord is my rock, my fortress and my deliverer; my god is my rock, in whom I take refuge.

- Psalm 18:2

Figure 9-1 A genealogy blog

Many people provide contact information, such as IM and e-mail accounts, phone numbers, and full street addresses. Many bloggers fill out one of the myriad surveys people can post about themselves, thinking that a flirty answer about their personal life is just fun, until a predator latches on to their answer and targets his next victim. Surveys and profiles are particularly high-risk collections of information. I found answers such as these to a survey on a 17-year-old girl's site (I've inserted the categories of answers):

- **Drugs**

  I've tried marijuana.

  I have passed out drunk in the past six months.

- **Sex**

  I go for older guys/girls, not younger.

- **Emotional health**

  I have changed a lot mentally over the last year.

I fall for the worst people and have been hurt every time.

I have been intentionally hurt by people that I loved.

- **Self-esteem**

  I don't like it when people are unpleased or seem unpleased with me.

- **Identifiers**

  I have long hair.

  I have lived in either three different states or countries (MA, ID, AK).

  I have at least one sibling.

- **Internet usage**

  I have more friends on the Internet than in real life.

  I'm online 24/7.

  I like surveys.

Figure 9-2 A blog that reveals too much to predators

Find Out More

Find out about the risks of sharing information in Chapter 5, the risks of sharing photos and other visual clues in Chapter 4, and how predators prey on the emotionally vulnerable in Chapter 6. For information about the risks involved in blogging when you're grieving, refer to *www.look-both-ways.com*.

Who's Most at Risk?

According to David Huffaker's analysis and FBI data, at particularly high risk are young people between the ages of 13 and 15, when they make their blogs available to the public instead of to a limited group of friends and family. This is a time when teens are reaching out for new identities, friends, and validation. At the same time, they are often struggling with their existing relationships with their current friends, with their girlfriend or boyfriend, with family members (especially parents), and with teachers, as well as with their own unstable emotions.

Also at higher risk are young people who live in rural areas or suburbs (Wolak et al., 2004). They have a greater need to meet new people (they probably already know everyone in town) and tend to be more trusting of strangers than are kids in urban environments.

When Spam Meets Blog: Spam + Blog = Splog

If you allow the public to leave comments on your blog, you have opened the door to another rapidly increasing phenomenon, spam on blogs. Called "**splog**," this involves placing a comment, link, or graphic on your site that encourages you and anyone viewing your blog to visit the spam author's own blog or some commercial site. Of course, when you get there, you find that you're viewing an advertisement for anything from a gambling site to a pornography site. Or you discover that someone is trying to cheat the system and increase their blog's popularity for some reason—possibly because they are getting a revenue share from advertisers based on how many people they can attract to their site.

But people of any age who are looking for new friends, have low self-esteem, or who are suffering from depression, grieving, or otherwise emotionally vulnerable are also likely victims. In less than nine minutes on average, I can locate adults, as well as teens, through the information they've put in their public blogs. Ironically, some of the worst examples of adults providing too much information in public blogs are individuals whose jobs are computer related. Although they might be confident techsperts (technical + expert = techspert) who can avoid technical issues such as viruses and spyware, they are often no more likely to understand human predators and the risks they pose than the average 13-year-old.

Protecting Yourself

Blogs, when open to the public, are often the intersection of several sets of potential pitfalls I've explored in previous chapters in this book. The specific advice in Chapters 4 through 7 on mitigating those risks should be applied to your own blogging activity. In addition to that advice, this section provides recommendations to help you blog more safely.

Don't Overreact

How do you advise your children if you feel they have placed themselves, your family, or their friends at risk? One of the most common reactions parents have when they read about abuses of people through public blogs is to want to stop their child from blogging altogether. While that is an option—and perhaps an appropriate option if a child is very young—for most kids this is simply not practical, nor particularly helpful.

Kids can access the Internet and blog from their friends' computers and many cell phones today, and the ability to blog from commonly available devices will only increase. Instead of cutting them off from the tremendous opportunities blogging affords, you should focus on teaching them *how to blog safely.*

Find Out More

See Chapter 17 for information about how to start a dialog and create a family discussion guide.

Knowing How Information Adds Up

Most people (but far from all) are cautious about putting *all* their information in their blog profile. But what people don't realize is that the information they provide usually compounds over time. Here's an example of how this works:

David creates a blog and enters his city and state, first name, and age. He posts a few photos of himself with family and friends. That's a big chunk of personal information and introduces *some* risk, but he talked this over with his folks and they decided they were fine with it.

- A friend comments on one of his photos and refers to David by his last name: "Hey M------ (I'm disguising the last name here, but his friend did not), great photo."

  A predator now has a full name, identifying photo, age, and city and state, and might well be able to use a white pages listing to pinpoint David as one of seven M------s living in Williamsburg, Virginia. In addition, because mapping technologies allow you to plot multiple locations on a map, the predator can begin tightening the web of location information to zero in on David's house.

- David posts a blog talking about his science lab at school. He also notes that he is in a bad mood because he got dumped by Jacqueline. Though he deserved it, he still feels crummy.

  David has exposed an emotional vulnerability. Anyone scanning the blog knows David might be looking for a new girlfriend. An easy way to approach him is with a fake picture of a cute girl who thinks he's "wonderful." Rarely do boys resist providing access to their blog to a "cute girl" who is interested in them. Of course, it might not be David the predator is interested in; it could be his 6-year-old sister Sarah who is in his photo album, or his 9-year-old brother Adam, or both.

- A second friend leaves a comment that he'll watch him in next Tuesday's game and meet him at the side gate after–"Go Titans!"

  A quick Web search on high school football teams in Williamsburg provides David's school name so David can be easily located (a predator has the place, date, and time of the game and his photo). This information also corroborates that David's age and city information were accurately entered and not faked. The school location eliminates four of the last-named "M-----s" in town from the potential list because they live within other school districts. The search is now down to three likely houses.

- In a blog entry the next day, David talks about going fishing in the river and tells Ben and Tom to meet him at the dock behind his house and gives driving directions.

  David is now locatable both at school and at home, and he's made his house a good target for theft. It's a safe bet his house will be empty during the ballgame because his folks will probably attend. A robber now has a great opportunity. David's picture and identity information could be used to create a phony passport or a fake ID.

Think About It

People who post on social networks would reduce their risks considerably if they didn't leave all their postings, photos, and other material out there forever. It is very easy to leak a few drops of information here and there into a large online bucket. That wouldn't be such a big deal if the bucket were emptied occasionally.

Taking Steps for Safety

The first step to protecting yourself and your family is to have a solid understanding of what kinds of information risks there are, how information might get exposed, and what you can do to mitigate or avoid the risks.

Think About It

There are several sites that blatantly push users into revealing a great deal of personal information about themselves publicly, telling them that nobody will visit their space unless they put interesting details in their profile or that posting their pictures will get more new friends to visit their blog. This is entirely irresponsible. Know the attitude toward safety and the privacy policy of any site before using it.

Beyond basic awareness, here's a checklist of advice to help make your blogging safer:

- Make a conscious choice when setting up access to your blog. Most blog sites have several options, ranging from a personal journal that only you can see, to a site open to a defined group of friends and family, to a site available to a looser group of friends and their friends, all the way to a completely public site accessible to anyone in the world. Unfortunately, most sites default to a "publicly viewable" option, and you have to make an effort to look for the other options.

- If you want to share your blog with a larger group that includes people who do not know you personally or make your blog public, consider archiving older material so there is no accumulation of information. Review your blog postings periodically with a view toward understanding how much information you have made available as content and comments begin to accumulate.
- Choose a user name that is not suggestive or revealing. Your name should also not reveal your age, location, or gender.
- Be careful what you divulge through text and don't be recognizable through your photos (see Figure 9-3 for an example of a photo that isn't too revealing). Also, be aware what you might give away in a photo label. All too often users place clearly identifying information in photo captions that give themselves and their friends or family away, such as "Nigel and Kate in Kingsbridge on Saturday." If you want to post identifying images, you should strongly consider more restricted access to your site.

Figure 9-3 This blogger's photo doesn't show her appearance too clearly.

- Monitor your friends' comments so you are not exposed through them. The example shown in Figure 9-4 reveals how quickly friends' comments expose others. In this example, these three friends completely exposed the blog owner and themselves.
- Encourage your children to come to you if somebody who comments on their blog makes them feel uncomfortable in any way—whether that person is a friend, a family member, or a stranger.
- Be cautious about what you include in your profile and recognize that some blog and social networking sites make your profile

contents publicly available and searchable, even if your blog itself is private.

Figure 9-4 Taken together, all this information reveals a lot about these kids and the blog's owner.

- Make sure the blogging site you use has clear privacy and security policies, provides tools for protection, and is responsive to reports of abuse.
- According to international ethnography research as well as industry research, for many teens, more buddies equals increased social status. Don't add people you don't know to a buddy list if you are sharing personal information, and don't include people on your buddy list unless you feel comfortable about who they are. Remember: If you don't recognize the buddy name and the person has not requested contact with you in your comments area, the comment is quite likely spam.
- Don't play blog exposé. To get repeat attention teens will often get more and more risqué in their content and pictures. The potential for harm even within extended friend and family groups increases as the site gets racier and more personal.

- Finally, talk to your family and your friends. Everyone you interact with online needs to work together if you are to help each other learn your way around this new online world.

Think About It

Often people feel safer about receiving comments from and responding to somebody who lives far away, assuming they can't get at them. Keep in mind, however, that people can say they are located anywhere they want. They might live exactly where they claim to live, or they might live much, much closer.

Be Aware of What Your Friends Are Saying About You

One final point to keep in mind is that you are not the only one putting your information online through blogs. *Your risk level is based on what your collective group is saying about you, not just what you say.* It's vital that you share the cautions contained in this book with your friends and family and be aware of what they are putting online.

Here are the key steps for working with your family and friends to keep all of you safe:

- **Posting photos of others, or text that provides information about others in any way, without their knowledge and permission is disrespectful and might well be illegal.** It isn't okay to provide a friend's last name, their birthday, or where you're going to meet them, unless both parties agree that they want that information posted. This shows disrespect for their right to choose the level of exposure they are comfortable with. You should not only ask permission, but you should also make it clear who can see your site. In the case of minors, you might need to get their parents' permission.
- **Discuss your comfort level with sharing information that locates you.** If your social networking site is conservative and doesn't provide personal information that would help locate you but your friend's site does, then your information is still public. Take the time to browse through a couple of your friends' blogs to see what they say about you. If a friend tells what school they attend and there is a comment that you two have a class together, a suggestion

to meet out front after school, or a remark about a favorite teacher, it doesn't matter that you didn't provide your school information. Your friend just did it for you.

- **Keep in mind that "friends" can be a very fluid concept.** Both you and your friends will meet new people and shift friendships throughout your lives. At some point you might just drift away (jobs change, schools change, interests change), or you might experience a rift that suddenly breaks the friendship. How will your information be treated then? Occasionally you should review who has access to your site and make changes if necessary.
- You might have two friends who don't like each other. You don't want your blog to become the middle ground in a battle between your friends. Perhaps they've had a falling out or perhaps they never liked each other. What agreements are you making with each of them that will provide the level of safety the other needs?
- **Permissions can change.** Either you or a friend might, at a later date (even tomorrow), decide to change the permissions on your sites. How will your/their information be treated if the permissions on their site become public? Will your information be removed or archived? Will it be maintained in a section that is only for limited viewers (where some information is viewable by the public and some is set to private)? Or will your information get the same level of exposure as the rest of the site and suddenly become much more public than you had intended?
- **If you want your blog to be a social networking site, keep in mind that your level of safety from exposure is only as strong as the weakest link in your social network chain.** Even if you and your friends have agreed about avoiding exposure, you probably don't have such an agreement with all of *their friends*. Although you might ask your friend not to tell people what school *you* go to, if your friend posts a comment about *his* school and mentions your name, a predator can assume it's pretty likely that you all go to the same school. There is a potential for information to leak several tiers out in the network and eventually identify you.

As you apply the age-old social network infrastructure to your new virtual world, you have to be careful to look both ways and consider all the potential hazards to be able to get around safely.