

# 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 **cyber-criminals** 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.

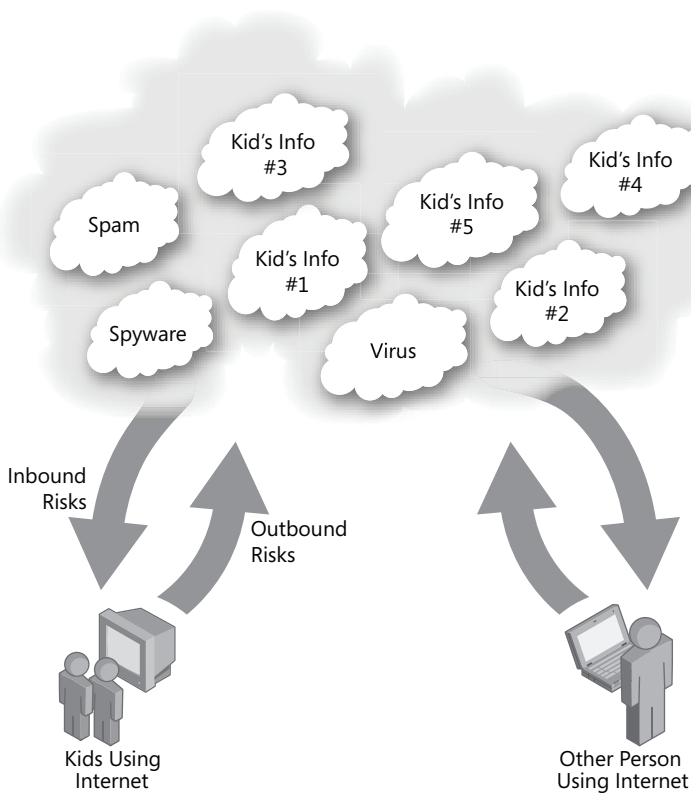
When you include cell phone Internet services, there are over 2 billion people worldwide with Internet access. Within the United States alone, there are over 21 million kids online, according to the Pew Internet & American Life Project. Cybercriminals are keenly aware of the opportunity and are targeting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

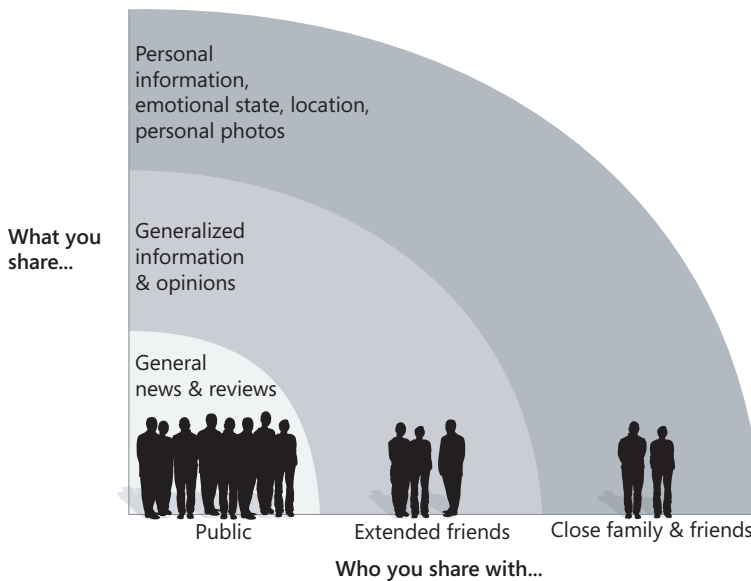
What kind of information are people putting out there? I'm not talking about your bank account or social security number—you wouldn't deliberately give those to strangers any more than you would hand somebody your wallet. I'm talking about seemingly useless information about you, from your favorite book 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 cyber-criminal. 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.