Chapter 1

Understand What's Going On Out There

Throughout this book, we point out again and again what a great tool the Internet is. Why? Because you hear a lot of hype about what a dangerous place the Internet is, and that hype sometimes causes people to miss out on a wealth of information, entertainment, communication, and opportunity.

Do Internet risks exist? Yes, just as risk exists every time you step out your front door, climb behind the wheel, or cross a street. But you haven't stayed in your house your entire life; you've learned how to stay relatively safe while exploring the world all these years.

You can stay just as safe online. First, you need a basic understanding of how Internet risks occur so that you can place any Internet safety advice in context. Once you know the nature of online risks, you can then begin to acquire skills to stay safer.

This chapter explores the landscape of risk online; in the process, we show you which risks are real and which are largely myth, look at the financial model that drives the Internet and the factors that allow abuses to occur, and show you how your own behavior can sometimes put you in harm's way.

In this chapter . . .

Congratulations: You're the Most Sought-After Generation Online

With millions of seniors going online and expanding their Internet activities, service providers see folks over 50 as a critical new target audience (see **Figure 1-1** from AARP) . . . and so do online criminals.

Every age group has unique vulnerabilities in addition to general Internet risks, and seniors are no exception. Few entirely new types of crime are created to target seniors; instead, existing crimes are tailored specifically to exploit older Internet users.

For example, while an online scam targeting minors promises trips to Disneyland or cool toys, scams aimed at seniors are more likely to offer discount medications and low-cost insurance. ***Phishing scams*** are e-mails that frequently target seniors with fake bank notices or official-looking fake government documents.

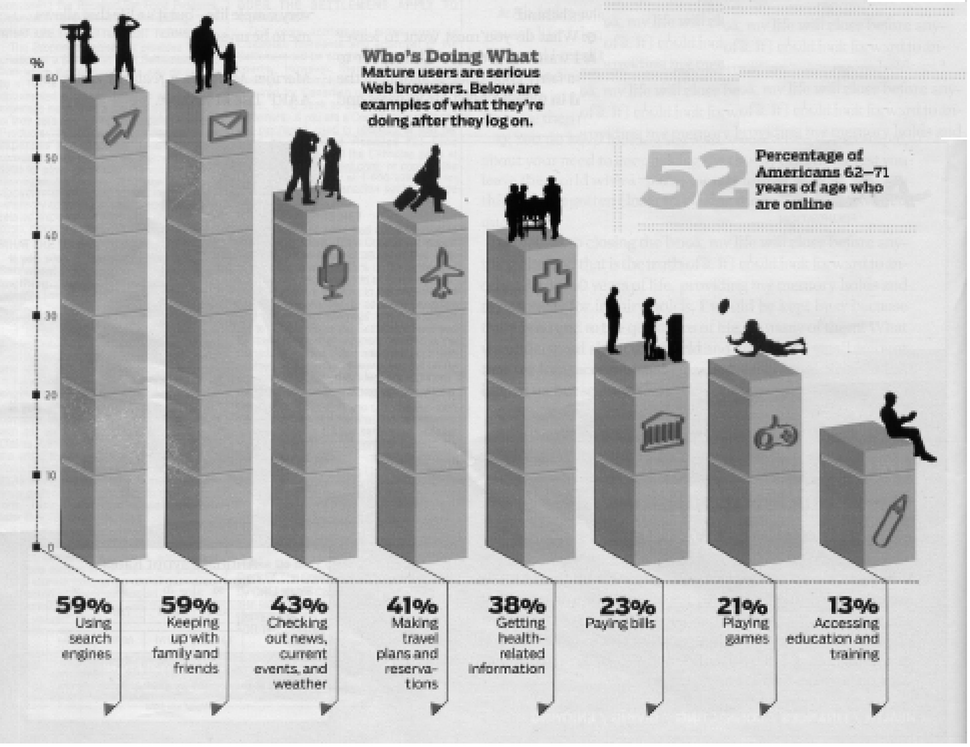


Figure 1-1

In addition to being targeted for different types of crime, seniors may share characteristics that make them especially vulnerable online. Here are some of the major factors that make seniors vulnerable:

- **Lack of computer skills.** Although many seniors are very computer savvy, many more aren't. They may not understand technologies such as firewalls and anti-spyware that they can use to protect their data.

- **Lack of Internet skills.** Though many seniors are cutting-edge users of Internet services, most are beginners when it comes to interacting with others and doing business online. You have a wealth of experience in judging the character of people you meet in person, but you have probably developed fewer skills for assessing the character of the people and companies you meet online.

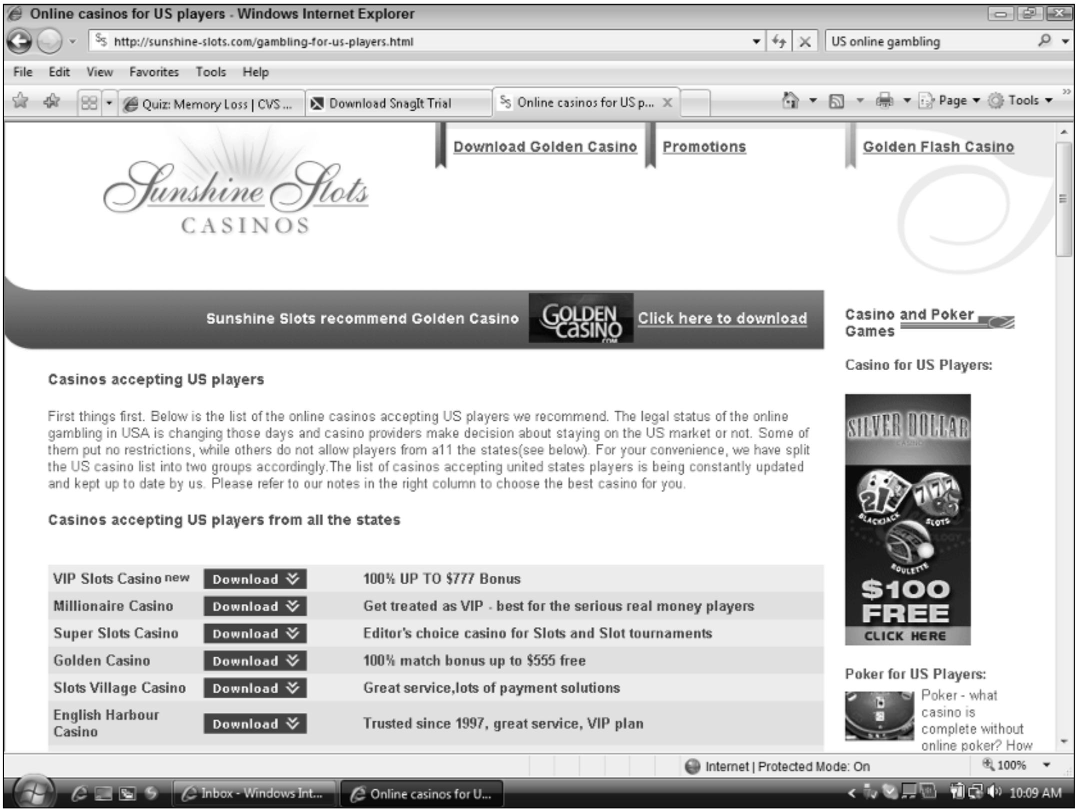
Lack of exposure to technology can make you more vulnerable. Understanding how content you place online (an activity called posting) might be misused, how criminals try to deceive you, or how to determine the trustworthiness of a site, for example, actually has little to do with how well you can use a computer. See the section "It's Not Always about Technology, It's Often about Behavior," later in this chapter, for more about this key concept.

- **More trusting.** Seniors are typically more trusting and respectful of official-looking material than younger generations, so seniors are more apt to fall for scams. And you're more worried about notices that claim that there's a problem with your information that might somehow sully your good name or threaten your life savings.

Roads Have Rules, The Internet Doesn't

The Internet began as a tool for university researchers to share information. When it took off with the general public, nobody was in charge, nobody owned the Internet, and no rules governed what you could and couldn't do online. Today, this is largely unchanged.

In addition, because of its global nature, the Internet lets us all cross borders — for good, and for bad. Some governments have regulations about Internet use. But with an international population using the Internet, it's hard to enforce the laws of a single country — and it's easy for people to fly under government radar. For example, in the United States, gambling online can be illegal, yet the casino in **Figure 1-2** actively solicits U.S. customers.



Casinos accepting US players

First things first. Below is the list of the online casinos accepting US players we recommend. The legal status of the online gambling in USA is changing those days and casino providers make decision about staying on the US market or not. Some of them put no restrictions, while others do not allow players from a11 the states(see below). For your convenience, we have split the US casino list into two groups accordingly.The list of casinos accepting united states players is being constantly updated and kept up to date by us. Please refer to our notes in the right column to choose the best casino for you.

Casinos accepting US players from all the states

VIP Slots Casino new	Download	100% UP TO $777 Bonus
Millionaire Casino	Download	Get treated as VIP - best for the serious real money players
Super Slots Casino	Download	Editor's choice casino for Slots and Slot tournaments
Golden Casino	Download	100% match bonus up to $555 free
Slots Village Casino	Download	Great service,lots of payment solutions
English Harbour Casino	Download	Trusted since 1997, great service, VIP plan

Casino for US Players:

Poker for US Players:

Poker - what casino is complete without online poker? How

Figure 1-2

In essence, we have a very sophisticated and powerful tool existing within a frontier culture — something akin to giving Jesse James and his gang laser guns. The current state of affairs is the result of a lot more than bad guys armed with technology. In fact, six factors contribute to the current online situation:

- **Lack of knowledge.** Consumers of every age and at every level of technical expertise lack broad online safety education. This lack of knowledge isn't limited to seniors, but extends to the general population, including computer specialists who may not know any more than others about online predatory behavior.

- **Carelessness.** Even when we know better, we make mistakes. Usually, we make those mistakes when we're tired, rushed, or don't have a complete understanding of the risks involved. This is especially true when we see no obvious cause and effect to help us correct our behavior. When you post information and a month later criminals use that information to rob your home, you aren't likely to recognize a connection between the two events. In fact, the vast majority of victims of online crime never recognize that an action they or someone else took online made them vulnerable to a criminal act.

- **Unintentional exposure of (or by) others.** It may be a grandchild, friend, employer, or volunteer organization that provides publicly accessible information that exposes you. Perhaps your own computer (or mobile phone, or other connected device) has been compromised with spyware that enables criminals to collect your personal information. Maybe when a friend's computer or other Internet-enabled device was lost or stolen, your information fell into the wrong hands.

- **Technology flaws.** Online products and services can expose consumers — either because the companies that offer them fail to secure their customers' data and are hacked, or because a company fails to build adequate safeguards and safety messaging into their product to protect consumers.

- **Holes in consumer protection standards.** Right now, most of the burden of online safety is on consumers. Because of the rapid growth of the Internet, governments have not yet been able to create a full set of standards and laws.

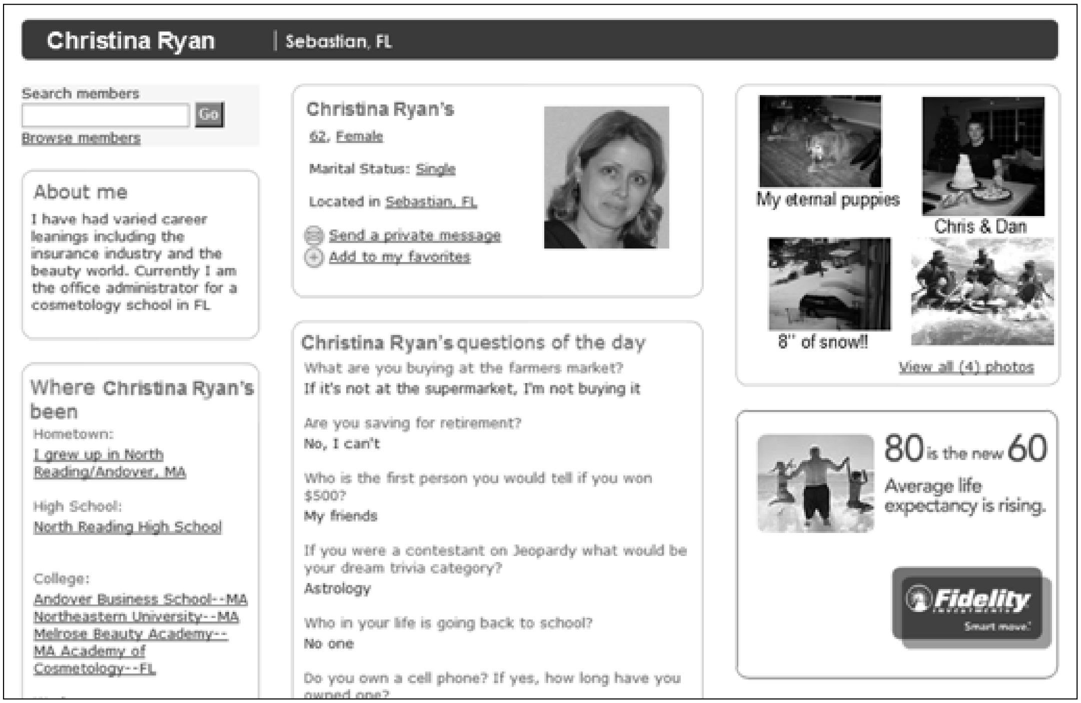
- **Criminal acts.** Placing the word *cyber* in front of -criminal, -thief, -robber, -molester, or -predator only changes the criminal's tools, not his motivations or goals. Criminals still want to steal your money, dominate or abuse, or destroy property. The Internet didn't create crime, and sadly, it won't abolish it. But it does offer some powerful tools for criminals to take advantage of.

The first five issues in this equation create an environment in which criminal and malicious acts can flourish. What's new is that the Internet gives criminals broader access to more people and information than ever before. Predators are generally equal-opportunity offenders, happy to target victims of any age. Young people represent only one segment; adults and seniors are equally at risk, although the motivation for exploitation of older consumers is more often for financial gain than for emotional or sexual gratification.

Online Anonymity

Although you may think you are anonymous online, you may not be. Online companies may have exposed you. For example, some e-mail programs display your full name in every e-mail you send, even if you've come up with a clever e-mail alias. If you join a social networking site such as MySpace or Eons (a senior-focused site), your publicly viewable profile might give away your name, location, and gender (see **Figure 1-3**), even if you set your page to private.

Though you may not be as anonymous online as you think, criminals are very good at staying anonymous or pretending to be someone or something they aren't. Offline, no one can build a fake bank or store on some street corner for a few days, so you don't have to worry about whether the bank or store is real. When you enter, you quickly get a sense of whether it's a reputable business. If you have a problem with a purchase, you can march right back through the door and demand service.



Christina Ryan | Sebastian, FL

About me

I have had varied career leanings including the insurance industry and the beauty world. Currently I am the office administrator for a cosmetology school in FL

Where Christina Ryan's been

Hometown:
I grew up in North Reading/Andover, MA

High School:
North Reading High School

College:
Andover Business School--MA
Northeastern University--MA
Melrose Beauty Academy--MA Academy of Cosmetology--FL

Christina Ryan's
62, Female
Marital Status: Single
Located in Sebastian, FL

Christina Ryan's questions of the day

What are you buying at the farmers market?
If it's not at the supermarket, I'm not buying it

Are you saving for retirement?
No, I can't

Who is the first person you would tell if you won $500?
My friends

If you were a contestant on Jeopardy what would be your dream trivia category?
Astrology

Who in your life is going back to school?
No one

Do you own a cell phone? If yes, how long have you owned one?

Figure 1-3
© 2008, Look Both Ways LLC

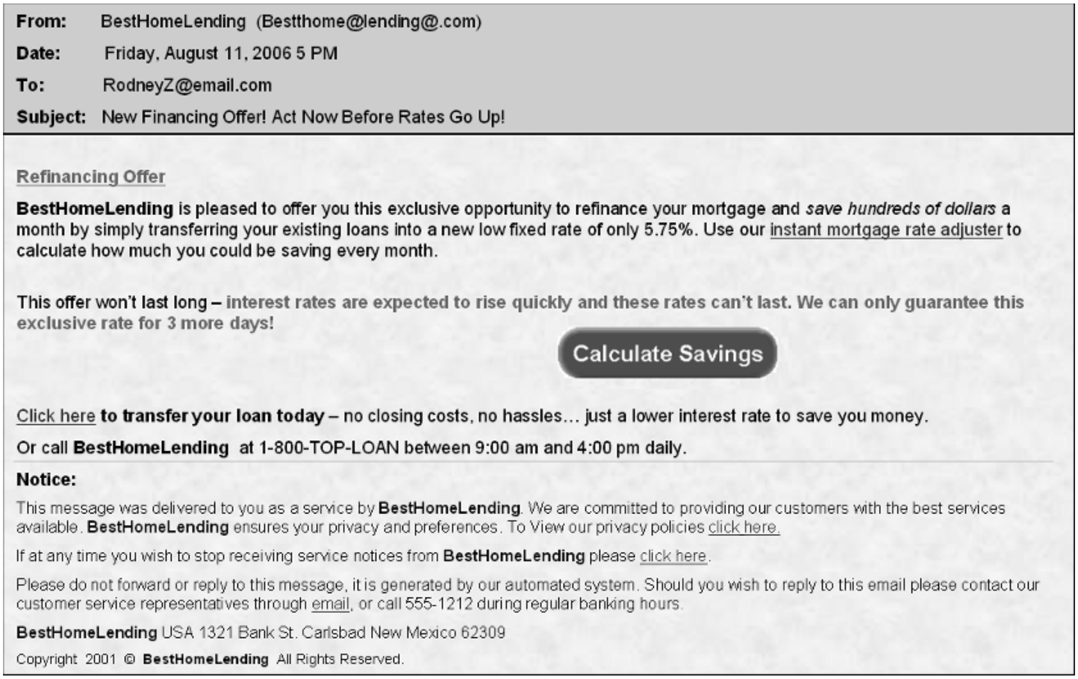
On the Web, those physical attributes and clues are all gone. Anyone can build a Web site that looks official and legitimate for very little money. They can trick search engines to make their Web sites show up as one of the first results when someone runs a search. Anyone can copy the look and content of any other Web site. This means that the fakes are sometimes very, very hard to identify, no matter what your age.

It's Not Always about Technology; It's Often about Behavior

Ironically, people who are computer savvy are sometimes more at risk online because they believe that being computer savvy means they are Internet savvy. In reality, Internet safety is often more a matter of understanding human behavior than understanding technology.

Think about your average phishing scam. This particular form of e-mail spam appears to come from your bank, investment company, or another site where you do financial transactions. (See **Figure 1-4**.) The e-mail will claim some "reason" why they need to verify your account number or password or credit card, Social Security Number, and so on (or all of the above!). The e-mail looks official, and it provides links for you to visit their site and verify your identity. But the site is as fraudulent as the e-mail and any information you provide is in the hands of financial predators. These e-mails may even display a prominent safety and privacy message meant to help convince you that the site is legitimate. However careful study of the message reveals several red flags once you know what to look for (see **Figure 1-5**).

Technology makes it possible for somebody to make a scam e-mail look authentic right down to using the legitimate company's logo, and send it to you. But what's putting you at risk isn't technology, it's the danger that you'll fall for the bait — hook, line, and sinker. If you're savvy, you'll know that the link to the site might take you to a mocked-up site that may look like your bank, but it isn't. Be suspicious of any e-mail that wants your bank account number or other sensitive information. Don't click on links! Instead, look up your bank's phone number (don't call the number provided in the e-mail, which could also be false), call, and report the scam.



From: BestHomeLending (Bestthome@lending@.com)

Date: Friday, August 11, 2006 5 PM

To: RodneyZ@email.com

Subject: New Financing Offer! Act Now Before Rates Go Up!

Refinancing Offer

BestHomeLending is pleased to offer you this exclusive opportunity to refinance your mortgage and *save hundreds of dollars* a month by simply transferring your existing loans into a new low fixed rate of only 5.75%. Use our instant mortgage rate adjuster to calculate how much you could be saving every month.

This offer won't last long – **interest rates are expected to rise quickly and these rates can't last. We can only guarantee this exclusive rate for 3 more days!**

Click here **to transfer your loan today** – no closing costs, no hassles… just a lower interest rate to save you money.

Or call **BestHomeLending** at 1-800-TOP-LOAN between 9:00 am and 4:00 pm daily.

Notice:

This message was delivered to you as a service by **BestHomeLending**. We are committed to providing our customers with the best services available. **BestHomeLending** ensures your privacy and preferences. To View our privacy policies click here.

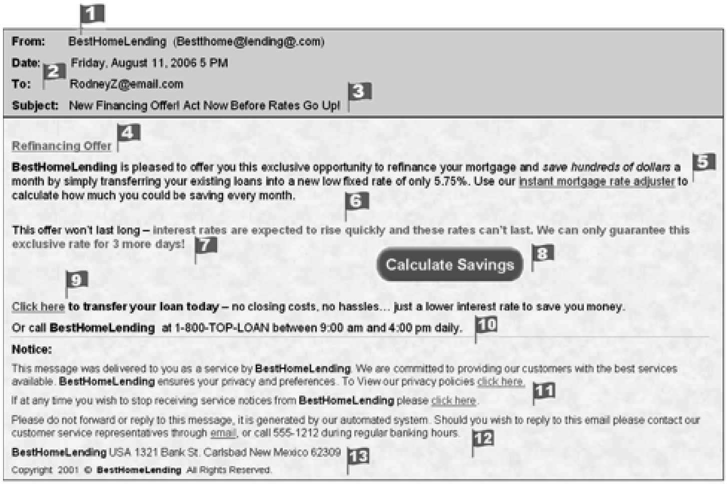
If at any time you wish to stop receiving service notices from **BestHomeLending** please click here.

Please do not forward or reply to this message, it is generated by our automated system. Should you wish to reply to this email please contact our customer service representatives through email, or call 555-1212 during regular banking hours.

BestHomeLending USA 1321 Bank St. Carlsbad New Mexico 62309

Copyright 2001 © **BestHomeLending** All Rights Reserved.

Figure 1-4



From: BestHomeLending (Bestthome@lending@.com)

Date: Friday, August 11, 2006 5 PM

To: RodneyZ@email.com

Subject: New Financing Offer! Act Now Before Rates Go Up!

Refinancing Offer

BestHomeLending is pleased to offer you this exclusive opportunity to refinance your mortgage and *save hundreds of dollars* a month by simply transferring your existing loans into a new low fixed rate of only 5.75%. Use our instant mortgage rate adjuster to calculate how much you could be saving every month.

This offer won't last long – **interest rates are expected to rise quickly and these rates can't last. We can only guarantee this exclusive rate for 3 more days!**

Click here **to transfer your loan today** – no closing costs, no hassles… just a lower interest rate to save you money.

Or call **BestHomeLending** at 1-800-TOP-LOAN between 9:00 am and 4:00 pm daily.

Notice:

This message was delivered to you as a service by **BestHomeLending**. We are committed to providing our customers with the best services available. **BestHomeLending** ensures your privacy and preferences. To View our privacy policies click here.

If at any time you wish to stop receiving service notices from **BestHomeLending** please click here.

Please do not forward or reply to this message, it is generated by our automated system. Should you wish to reply to this email please contact our customer service representatives through email, or call 555-1212 during regular banking hours.

BestHomeLending USA 1321 Bank St. Carlsbad New Mexico 62309

Copyright 2001 © **BestHomeLending** All Rights Reserved.

Red flags:

1. Company you haven't heard of.

2. The e-mail is not "To:" you.

3 and 6: Financial transaction under time pressure.

4. The e-mail doesn't acknowledge who you are.

5 and 8: Encouraged to enter financial information.

7. Legitimate offers contain specific dates.

8. Doesn't go to a site called "besthomelending".

9 and 12 More "click here" links that do not go to the purported site.

10. Doesn't specify the time zone.

11. Not an 800-number.

13. An Internet mapping site shows there is no such address.

Figure 1-5

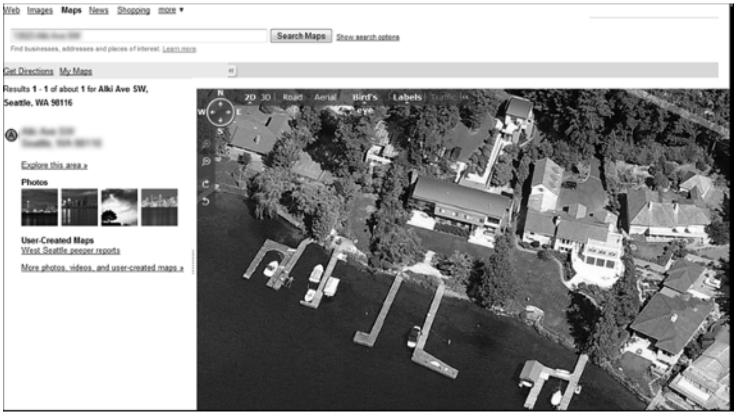
Hit or Myth: Online Information Exposure

Having your information exposed online is one of the greatest risks you face, but seniors generally buy into a few myths about how their information is exposed online.

The first myth is that if you don't use a computer or go online, you aren't exposed online. False. Just because you didn't put information online doesn't mean it isn't there — virtually everyone has information online.

Here are a few examples:

- Publicly available government records show if you own a home, vote, have a criminal record (or speeding ticket), and much more.
- Your location (including photos in most cases) is listed online through any Internet mapping service like the one shown in **Figure 1-6**.
- Unless you've been very careful to ensure your phone number isn't in any phone book, or taken care to have never entered it in a sweepstakes or other contest, it's online. Even if you have been careful, you should check to see. Type your home phone number (with area code and hyphens) into any search engine and see if it brings back your information — chances are that it will.
- If you donate to a charity without doing so anonymously, the charity's Web site probably lists you as a donor as a way to thank you.
- If you volunteer with an organization, belong to a church group, sports group, action committee, and so on, chances are you are listed on its Web site.



[redacted]

Find businesses, addresses and places of interest. Learn more

Results **1 - 1** of about **1** for **Alki Ave SW, Seattle, WA 98116**

Ⓐ [redacted]

Figure 1-6

- If your grandchild has a ***blog*** (an online journal), or has registered for her wedding or a new baby, your name, location, and other information may appear there.

- If a relative enjoys genealogy, you and your relatives' names, birth dates, wedding dates, death dates, locations, and more may be posted on a genealogy site.

The second myth is that if you haven't fallen for an Internet scam, you won't be the victim of an Internet crime. The truth is that you may never know what the Internet connection is (or even if there was one) in most crimes. For example, online public records may give a criminal the information and means to rob your home or steal your identity.

The third myth is that only people you know are going to look at the information you post online. Everything on the Internet is copied and indexed — constantly. Even if you take your information off the Internet, a copy of it may still be out there, although you can reduce exposure by removing personally identifiable information from anything you or family members post online.

Keep Your Information Private

Sharing personal information with the wrong people is one of your biggest risks online. Before you provide personal information, be sure you're comfortable with how it will be handled. Table 1-1 lists some common pieces of personal information, along with the risk of exposing this data online.

Table 1-1 Information Exposure Risks

Information	*Risks of Abuse*
Address and phone number	Makes the user a target for home break-ins, junk mail, and telemarketers, and provides a stronger persona in identity theft cases.
Names of husband/wife, father, and mother (including mother's maiden name)	Provides access to even more confidential information in public records, this data is also often used for passwords or secret question answers; and it may expose additional family members to ID theft, fraud, or personal harm.
Information about your car, including license plate numbers; VIN (vehicle identification number); registration information; insurance carrier; loan information; and driver's license number	Can lead to car theft, insurance fraud, and access to more of your confidential information.
Information about work history and credit status	Helps criminals take over your identity and gain more access to your financial records.
Social security numbers	Enables ID theft, fraud, and access to additional information about you.

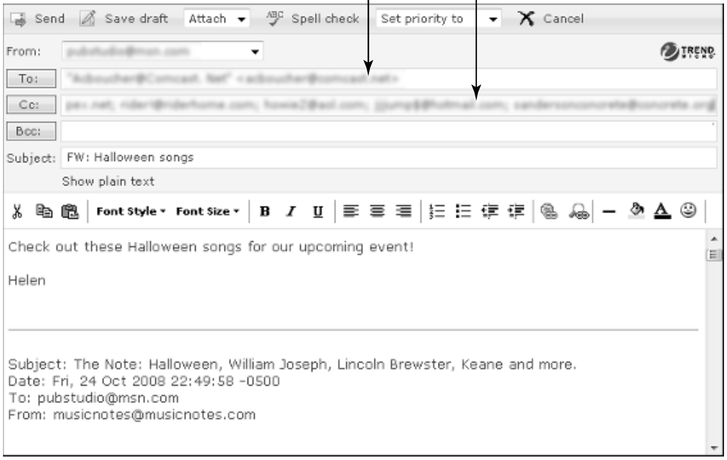
How Information Accumulates

Every detail you share online about your life and the extended group of people you interact with is stored *somewhere*. Understanding the way this information accumulates is critical.

Many people are very casual about giving out personal information online because they fail to fully understand the ramifications of doing so. Think of each piece of information as a drop of water. Today, each drop of information posted online is collected into personal virtual buckets. The information rarely disappears; rather, it accumulates, slowly building a comprehensive picture of your identity and life. Small details about your appearance, where you live and work, where you went to school, your financial status, emotional vulnerabilities, and the lives of those close to you all add up in a smart predator's mind.

People post resumes that include hobbies, past employers, past addresses, and professional associations. People post highly personal and identifiable information in online journals called ***blogs.*** On travel sites, you may reveal your excitement about an upcoming trip. Perhaps you are exposing friends and family's e-mail addresses by forwarding e-mails. (See **Figure 1-7**.)

Exposed e-mail addresses



From: [redacted]

To: [redacted]

Cc: [redacted]

Bcc:

Subject: FW: Halloween songs

Check out these Halloween songs for our upcoming event!

Helen

Subject: The Note: Halloween, William Joseph, Lincoln Brewster, Keane and more.
Date: Fri, 24 Oct 2008 22:49:58 -0500
To: pubstudio@msn.com
From: musicnotes@musicnotes.com

Figure 1-7

The good news is that you can begin to control the information you expose about yourself, and even ask friends and family members to limit how they expose you. Just keep in mind that you, your friends, and family aren't the only ones sharing information, so remember to periodically search the Web for information and then, if you find something you don’t want shared, ask the site owner to remove the information:

- **Employers need to consider the level of information they share about current and former employees.** Consider carefully what information is appropriate to include in an employee bio that is posted on your company Web site. How much should be visible to other employees on your *intranet* (your internal company “Internet”)? When you attend a conference, is the attendee list shown in online conference documents? Teach employees to be careful about the information they leave in out-of-office messages; saying ‘taking the grandkids to Disneyland’ also says ‘our home will be empty’ and potentially makes them a target for burglary.

- **Organizations should be cautious about exposing volunteer information on their Web sites if the general public can view those sites.** Posting photos and identifying volunteers or staff by last name can place people in harm’s way. Posting schedules of club activities along with information about what activities an individual participates in provides a criminal with the physical location and time where he can find that person.

Consider who can see your information before you post it. It is your choice how much personal information you post online in publicly viewable sites, how much you share on private sites, and what you choose not to share online at all. Schools and companies can restrict access to parts of their sites to make information available to those who need it, but not to anyone outside of your organization. See Chapter 8 for more about social networking site settings.

Online Information Is Forever

One of the reasons information exposed online puts you at such great risk is because, once it's out there, it stays out there. Comments, actions, or images posted online may stay online long after you delete the material from your site or request that a friend delete your information from his or her site. You won't know who else has downloaded what you wrote or what search engine crawled (automatically searched the Internet) and stored a photo. You can't know who else sees your comments and judges you by them, nor will you have the opportunity, in most cases, to explain. (See Chapter 7 for more about sharing information safely online).

Another aspect of information permanence is the difficulty it presents when you want to distance yourself from something in your past or go in new directions. Perhaps you no longer want to be associated with an old relationship, but the information remains online to haunt you and for anybody to come across.

Anyone — with good intentions, as well as those with intent to do harm — can dip into your public virtual bucket and search for your information years from now. It may be the new pastor at your church, a potential employer, a new friend, or your grandchildren who discover something you'd rather keep private. Or it could be an identity thief, any other kind of predator, or anyone in your life who wants to lash out at you to cause harm.

What seems like a good idea at the time may come back to bite you in a variety of ways, so think before you post. It's far easier to think twice and refrain from posting than it is to try to take it back. By doing so, you can control your information exposure and privacy while staying safer online.