Know the Risks

No matter how real online interactions seem, they're not quite like hanging out with friends because you never know for sure who you're connecting with. You may be revealing personal details to a much wider audience than you realize–a mix of family, buddies, acquaintances, co-workers–and complete strangers.

When ordinarily you might share only a part of your life with any one person–intimate details with close friends, complaints about your work load with colleagues–online you may be sharing everything with everybody.
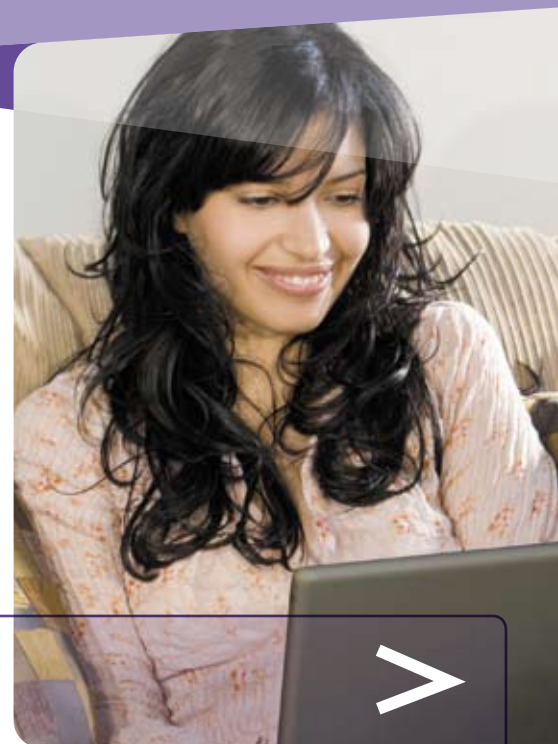
Unlike a private conversation, after information has been published on the Internet, it's effectively there forever. It's available to future employers, friends, job recruiters, and others with consequences you may be unable to imagine.

Most people you'll meet online are genuine and decent, but just as in the rest of the world, some are up to no good. They could misuse the information you disclose to tarnish your reputation, harass you, steal your identity, even jeopardize your physical safety. They could also try to break into your computer to plant spyware, or exploit your PC to send spam or commit crimes.

More Helpful Info

➤ Help kids use social Web sites more safely with advice from Microsoft: **microsoft.com/protect/parents/social/kidssocial.aspx**.

➤ If you use Internet dating services, get pointers for making the adventure safer: **ilookbothways.com/docs/DOC-1051**.

Smarter Online = Safer Online

Safer Socializing on the Internet

> How do you socialize online?
> Practical advice for safer online socializing
> What to do if there are problems

Content contributor

LOOKBOTHWAYS
The Human Factor in Online Safety

0609 PN 098-111464

How Do You Socialize Online?

The Internet is a great place to meet people, stay in touch with family far and near, and forge a community of friends.

Create your own Facebook or Windows Live™ account and find out what your friends are up to there, or explore a virtual world like Second Life or Club Penguin. Share common interests and hobbies with a group, keep a blog, browse a message board, or post updates in real time on Twitter. All are part of the virtual social whirl.

Practical Advice for Safer Online Socializing

Set your boundaries

Think carefully about how public you want your profile or blog to be. The more identifiable the information you share, the more selective you should be with whom you share it.

Evaluate the social site before you use it. Does it offer the level of control, protection, and overall experience that's right for you? Who's using it and how? Will you feel comfortable in this community?

> Some sites automatically make profiles public; others set them to private by default. Look for **Settings** or **Options** to control who can see your profile or photos tagged with your name, how people can search for you, who can make comments, and how to block a bully.

> Carefully read the terms of use. Does the site claim ownership of your information? Resell it? Use it to target ads to you?

> Find out if and how vigorously the site monitors abusive interactions or inappropriate content and how to report these.

Be selective about friends

Think twice about who you accept as a friend. Consider adding only those you or close friends have met in person or with whom you have friends in common.

Periodically reassess who has access. Friends change over time.

Review what your friends write about you. Make sure they don't post anything sensitive like private photos or your whereabouts. It's okay to ask someone to remove information that you don't want disclosed.

Think before you post

Before you post anything online–blogs, comments, tweets, snapshots, links–consider two things: *it may ultimately be seen by anyone on the Internet and it can be permanent.* The site may archive what you've posted, friends (or ex-friends) may give it out, or hackers and security lapses may expose it.

Choose a user name that doesn't attract unwanted attention or help someone find you.

Don't over share.

> Don't post anything you'd ordinarily say only to a close friend. Some sites let you create separate friend lists– for family, for your sports team, and so on–so you can manage what you share with each.

> Keep details to yourself that could be used to identify you or locate you in person–your home address, phone and account numbers, birth date, photos, etc.

> Avoid posting provocative pictures or videos.

> Use caution when sharing feelings. Whether you're happy, sad, angry, or have money worries, confiding broadly could put you at increased risk.

> Talk with family and friends about what you might share about them. Remove from your pages any info that doesn't conform to their wishes.

Treat others as you would like to be treated. Be judicious about what you say on your own and others' pages.

TIP

If you spend time in a virtual world, don't reveal your real name. For example, if you must send e-mail to a virtual friend, set up a unique address with your character's name instead of using an account in your own name.

Be vigilant when meeting an Internet "friend" in person

On the Web, people can pretend to be anyone. (Pictures are no proof, either.)

> Meet in a busy public place, and bring a friend or let others know where you're going.

> Bring a cell phone and keep it on.

> If it doesn't feel right or if the person wasn't truthful in any way–doesn't look like his or her photo, say–leave at once.

Protect accounts with strong passwords

> Use at least eight characters (longer is better) and include upper and lower case letters, numbers, and symbols. (Learn more about creating strong, memorable passwords at **microsoft.com/protect/yourself/password/create.mspx**.)

> Don't share your passwords with friends or be tricked into giving them away to someone or to another site. People most often gain illicit access to accounts because the owner gave them the password.

Defend your computer against Internet threats

Be wary about clicking links to video clips and games, or opening photos, songs, or other files from any source–even someone you trust. A virus could have sent the file and the download could install destructive software. Check with the sender or poster or use a search engine to find the link or file yourself.

Build up your computer's defenses and keep them up to date. Use firewall, antivirus, antispyware, and antispam software. Keep all software (including your Web browser) current with automatic updates. Microsoft can help you do this: **microsoft.com/protect/computer/default.mspx**.

Be careful about installing add-on apps. Many let you enhance your personal pages, but some may damage your computer or steal sensitive data. Stick to extras that the social site recommends or ones that are reputable.

What to Do If There Are Problems

Report issues

No one has the right to threaten or upset you, so report:

> Any negative incidents to the Web service, including content that exploits minors, obscene or hateful material, inappropriate behavior, or theft of your account.

For example, look for a **Report Abuse** link as available in Microsoft® services or software, or send e-mail to **abuse@microsoft.com**.

> Continued harassment or physical threats to local law enforcement.

> Identity theft to the U.S. Federal Trade Commission (FTC) at **ftc.gov/idtheft** or call toll free: **(877) 438-4338**.

> Scams or fraud to the FTC. Go to **ftc.gov/bcp/consumer.shtm** and click **File a Complaint**, or call toll free: **(877) 382-4357**.

If your computer isn't running properly

If you notice that your computer is unusually slow, crashes frequently, or shows other signs of unusual behavior, it might be damaged by malware. Microsoft can help at: **safety.live.com**.