How you socialize online

The Internet is a great place to connect. You may join friends on Facebook or Windows Live Messenger or colleagues on LinkedIn, explore a virtual world like Second Life, share common interests with a group, keep a blog, find a date, post updates on Twitter, play games, or check in on Foursquare.

Yet, no matter how real these interactions seem, they're not quite like hanging out in person. Face-to-face, you might share only a part of your life—intimate details with close friends, gripes about work with colleagues—but online you may be revealing details about your life to a much wider audience than you realize.

And, unlike in-person conversations, after you post online—texts, blogs, comments, tweets, snapshots, links—it may remain there forever. The site may archive your post, people may keep it and share it, companies may sell it, or security lapses may expose it. That means it may be available to future employers, friends, bank loan officers, and others with consequences for your reputation that you may be unable to imagine.

It's also important to know that hackers, spammers, identity thieves, and other criminals could misuse the information you disclose to tarnish your reputation, harass you, steal your identity, or ruin your credit.

What to do if there are problems

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

- Any negative incidents to the web service. These could include threatening content, hateful material, inappropriate behavior, or theft of your account.

  For example, in Microsoft services or software look for the **Report Abuse** link, or contact us at **microsoft.com/reportabuse**.

- Continued harassment, ongoing cyberbullying, 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 at **ftccomplaintassistant.gov**.

More helpful info

- Help kids use social websites more safely: **microsoft.com/security/family-safety/kids-social.aspx**.
- If you use Internet dating services, get pointers for making the adventure safer: **ilookbothways.com/learn-safety/dating-online**.

Content contributor LOOKBOTHWAYS ilookbothways.com

1011 PN 098-111464

Microsoft

Safer Online Socializing

Microsoft

Practical advice for safer online socializing

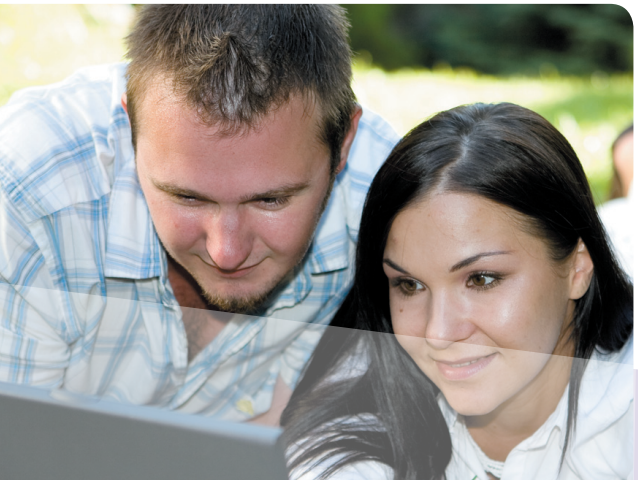
Set your boundaries

Think carefully about how public you want your profile and information to be. The more personal the information you share, the more selective you may want to be.

- Some sites automatically make profiles open to anyone on the Internet; 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 people.
- Some sites let you create separate friend lists—for family, coworkers, your sports team, and so on—so you can manage what you share with each.

Explore any social site before you use it.

- Carefully read the terms of use. Does the site claim ownership of your information? Can the site sell it? Use it to target ads to you?
- Find out 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 to your information. Friends change over time.

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

Be vigilant when meeting an Internet "friend" in person. Meet in a busy public place, and bring a friend.

Don't over share

No settings are perfect; you still need to use good judgment.

- Don't post anything you'd ordinarily say only to a close friend, including feelings. Whether you're happy, sad, angry, or have money worries, confiding broadly could increase your risk of being bullied or targeted for scams.
- Keep sensitive details to yourself that could be used to defraud, impersonate, or find you—home address, phone and account numbers, birth date, photos.
- Avoid posting suggestive pictures, videos, or comments. Ask yourself if they could tarnish your reputation.
- If you use a location service, consider limiting who knows your location. Pay attention to where and when you check in, and link to social media with care.

TIP

If you spend time in a virtual world (such as Second Life), stay anonymous. Before sending email to a virtual friend, set up a unique address with your character's name instead of using your primary email account.

Treat others as you would like to be treated

- Be judicious about what you say on your own and others' pages.
- Talk with family and friends about what they don't want shared. Remove from your pages any info that doesn't conform to their wishes.

Defend your computer and your accounts against Internet threats

Boost your computer's defenses. Keep all software (including your web browser) current with automatic updating. Install legitimate antivirus and antispyware software. Never turn off your firewall. (Microsoft can help: **microsoft.com/security/pypc.aspx**.)

Protect accounts with strong passwords.

- Use long phrases or sentences that and mix capital and lowercase letters, numbers, and symbols. (Learn how: **aka.ms/passwords-create**.)
- Don't share your passwords with anyone or be tricked into giving them away. Most account takeovers occur because the owner gave away the password.

Think before you click links to video clips and games, or open photos, songs, or other files from any source—even from someone you trust. Check with the sender first. The download could install malicious software or be used to break into your account.

Install add-in applications (*apps*) cautiously, some of which may damage your computer or steal sensitive data. Stick to apps from reputable companies.