Microsoft

Internet safety = your experience + new skills

You have been managing risk your whole life. Staying safer online is no different. You just need to apply your considerable experience in this new environment and master a few new safety skills.

Start with a little background:

> On the Internet, your information is a valuable commodity. Every bit of data about you and your online habits could be worth something to a person or business.

> Information published online is effectively there forever, and it may ultimately be seen by anyone on the Internet.

> No matter how real your online interactions may seem, you never know for certain who you're connecting with because you can't see them face to face.

Then, understand the risks. People could misuse the information you disclose through email or in a blog to tarnish your reputation, harass you, steal your identity, ruin your credit—even jeopardize your physical safety.

< And now, learn the skills.

What to do if there are problems

No one has the right to threaten or upset you. Report:

> Any negative incidents including obscene or hateful material, harassment, scams, or theft of your account to the web service.
For example, in Microsoft services or software look for the **Report Abuse** link, or contact us at **microsoft.com/reportabuse**.

> Continued harassment or physical threats to local law enforcement.

If you've responded to a phishing scam or been a victim of identity theft, change your password on all online accounts and report the incident to:

> Your credit card company, financial institution, or health insurance company.

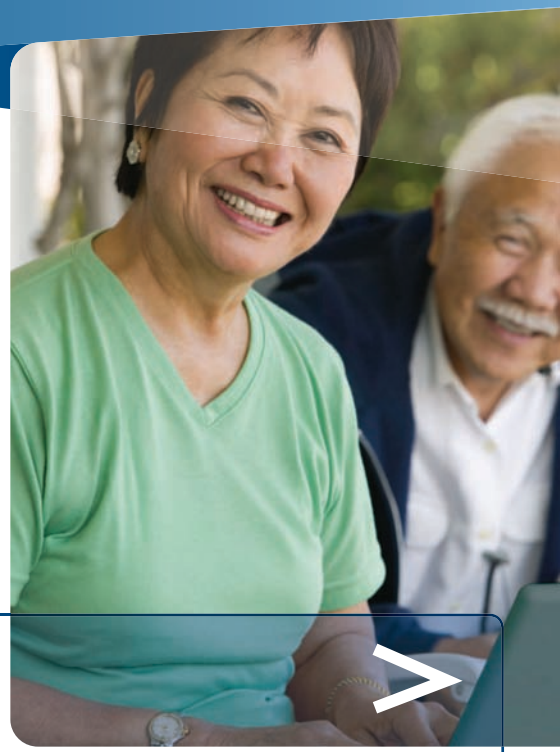
> To the U.S. Federal Trade Commission (FTC). Call toll free: **(877) 438-4338**.

More helpful info

The AARP offers Internet safety advice including helpful videos on safety basics: **aarp.org/technology**

Content contributor LOOKBOTHWAYS ilookbothways.com

1011 PN 098-115059



Stay Safer on the Internet

Five basic skills for staying safer online

1 Defend your computer

Keep all software (including your web browser) current with automatic updating. Install legitimate antivirus and antispyware software. Protect your wireless router with a password, and use flash drives cautiously. Microsoft can help: **microsoft.com/security/pypc.aspx**.

2 Guard email and other accounts with strong passwords

> Make them long (phrases or sentences) that mix uppercase and lowercase letters, numbers, and symbols. (Learn how: **aka.ms/passwords-create**.)

> Avoid using the same password everywhere. If it is stolen, all the accounts it protects are at risk. It's okay to store passwords on a well-protected piece of paper away from your computer.

3 Use email more safely

Spot the signs of fraud

> Watch out for surprise messages that you have "won a lottery," need to send money to your "grandchild," or help a distant stranger "transfer funds." Other clues include notices of account closure, misspellings, and grammatical errors.

> Stay alert to phishing scams, like an urgent email message that appears to be from your bank or other trusted organization, like you favorite charity. It may ask for your password, financial info, or other sensitive data in email, or direct you to give it to a counterfeit website or phone number.

Learn about phishing scams: **aka.ms/scam-protection**.

Think before you respond to email

> Don't trust the sender's name. It can be faked.

> Be cautious about clicking links to video or opening photos, songs, or other files—even if you know the sender. Check with him or her first.

> Be wary of visiting a website or calling the number in a suspect message. They could be phony. Instead, contact the company using info you find yourself.

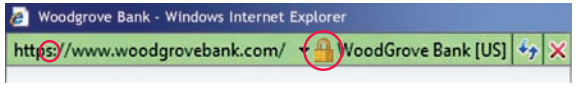
> Be careful what you put in email. It's as insecure as a postcard.

4 Browse more safely

Look for signs that a web page is secure

> Make sure you're at the correct site—for example, at your bank's website, not a fake.

> Look for a web address with https ("**s**" stands for secure) and a closed padlock beside it. (The lock might also be in the lower right of the window.)



Don't type sensitive information in unexpected pop-up windows

5 Use social networks more safely

Decide how public you want your profile or blog to be

When using a social network website like Facebook or Eons or posting opinions on your own webpages (*blogging*), consider that some sites automatically make what you post open to anyone on the Internet.

Look for **Settings** or **Options** to manage who can see your profile, photos, and friends, how people can search for you, who can comment, and how to block unwanted access.

Think before you post

Before you post anything online, remember that the site may archive what you post, friends may give it out, or hackers and security lapses may expose it.

> Don't post anything—especially sensitive information like your address or birth date—you would ordinarily say only to a close friend.

> Use caution when sharing feelings—whether you are happy, sad, angry, or have money worries—because predators may exploit your emotions.