Know the Risks

As with any Web service, there are bound to be risks. Use e-mail or instant messaging (IM) carelessly, and you can put your privacy at risk, make a dent in your bank account, or damage your computer.

> Spam can contain a link that, if clicked, may download spyware or a virus. Spyware can be used to track your Web activity, or let a crook record any passwords or account numbers that you type. Viruses may damage your computer or steal the addresses in your IM or e-mail accounts and forward the virus to everyone in a message that looks like it came from you.

> Some spammers try to trick you into simply giving them your money–by promising big returns on your "investment," by asking for donations to a fake charity, or by offering to sell something at a "bargain" price.

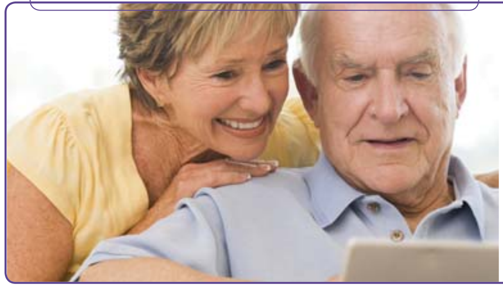
> Others, using a method known as phishing, try to steal personal information–even your identity. They send a sneaky form of spam that appears to come a company you trust, like your bank or an online retailer. The forged messages (the "bait") typically contain a link (the "hook") to an equally phony Web page or a toll-free number. There, you're asked to reveal financial or other personal data.

TIP

Get more detail on how to spot a phishing scam and defend against one at **microsoft.com/protect/yourself/phishing/identify.mspx**.

More Helpful Info

- Get 10 tips for using instant messaging safely: **microsoft.com/protect/yourself/email/imsafety.mspx**.
- Find out how to protect your inbox from spam: **microsoft.com/protect/yourself/email/default.mspx**.



Content contributor LOOKBOTHWAYS
The Human Factor in Online Safety

0309 PN 098-111020

Smarter Online = Safer Online

Using E-Mail and Instant Messaging Safely

Every day, billions of e-mail and instant messages crisscross the globe–testimony to the speed, economy, efficiency, and popularity of both.

Practical Advice for Safer E-Mailing and Instant Messaging

Reduce spam in your inbox and in IM

Share your e-mail address or screen name with care

- Set up a secondary e-mail address only for public Web activities–shopping, joining organizations online, subscribing to newsletters, signing petitions, and so on.
- Only share your primary e-mail address or screen name with people you know or with reputable companies or organizations. Avoid listing them in Internet directories (such as white pages), job-posting sites, online communities–even on your own blog.

Create a name that gets less spam

Research shows that a combination of letters, numbers, and other characters work best–like *Kar!Furs3@example.com*.

TIP

For other ways to keep spam out of your e-mail or IM inbox, see **microsoft.com/protect/yourself/email/spam.mspx**.

Be cautious and use common sense

Pause before you open attachments or click links in e-mail or IM, even if you know the sender. If you cannot confirm that an attachment or link is safe, delete the message or close the IM window.

If you wouldn't write personal information on a post card, don't put it in e-mail or IM. This includes your home address, account numbers, passwords, or other confidential data.

Don't use IM with strangers. Only communicate with people on your contact (or buddy) list. Only add people you know in person to your contact list.

Ignore junk e-mail or IM. Spammers get rich (and build their lists, too) when people buy their "products." So don't reply to spam (even to "unsubscribe") or buy anything, give to any "charity" you don't know by reputation, or agree to hold or transfer money for anyone.

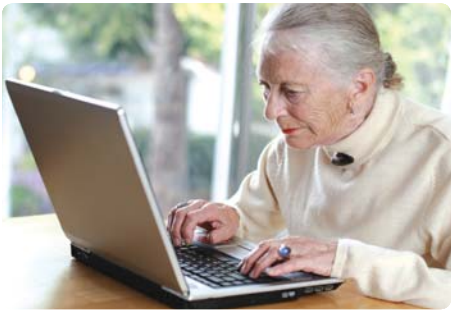
Look for telltale signs of fraud. These may include requests for personal information, alarmist messages, misspellings and grammatical errors, deals that sound too good to be true, or chain letters that ask you to forward the mail to all your friends. When in doubt, check with a site like **snopes.com** to see if it's a known scam.

Put technology to work

Defend your computer against Internet threats. Use firewall, antivirus, antispyware, and antispam software. Password-protect your wireless connection at home. Keep all software current (including your Web browser) with automatic updates. Microsoft® can help you do this at **microsoft.com/protect/computer/default.mspx**.

Protect yourself from phishing. Use a special filter such as the SmartScreen® Filter which you can get with Windows® Internet Explorer® 8, or the Microsoft Phishing Filter in Internet Explorer 7 and Windows Vista®. It warns you of suspicious and reported phishing Web sites.

Block communication from those not on your contact list. Make sure your IM account is configured to do this.



Microsoft

What to Do If There Are Problems

Report scams, phishing messages, and other spam

- Using the **Report Junk** button offered by most e-mail and IM services.
- File a complaint with the U.S. Federal Trade Commission (FTC). Go to **www.ftccomplaintassistant.gov**, and click **FTC Complaint Assistant**. (If you're in the military, click **Military Sentinel**.)

Report abusive, threatening, or harassing messages

Report any incidents to the e-mail or IM service. For example, look for the **Report Abuse** link as available in Microsoft services or software, or contact us at **abuse@microsoft.com**.

If you've responded to a phishing scam

Change the password on all compromised online accounts and report it to:

- Your credit card company or your bank.
- In the United States, to the FTC at **ftc.gov/idtheft** or call **(877) 438-4338**.

TIP

Get more advice from Microsoft about what to do if you've been the victim of phishing: **microsoft.com/protect/yourself/phishing/remedy.mspx**.