Microsoft

Top Tips for Internet Safety at Home

1 Defend your computer

Keep all software current (including your Web browser) with automatic updates. Use firewall, antivirus, antispam, and antispyware software. Password-protect your wireless connection at home.

2 Protect sensitive personal information

- Look for signs that a Web page is safe, before you enter sensitive data–a Web address with http**s** ("**s**" for secure) and a closed padlock ( ) beside it.
- Never give sensitive info in response to an e-mail or instant message (IM) request.

3 Think before you click

- Pause before you open attachments or click links in e-mail or IM even if you know the sender; they could be phony. Confirm with the sender that the message is real or visit the official Web site by typing the address yourself.
- Be wary of clicking links or buttons in pop-up windows.

4 Create strong passwords and keep them secret

Make them at least eight characters (longer is better) and include upper and lower case letters, numbers, and symbols. Don't use the same password everywhere.

5 Protect yourself from e-mail scams

Look out for alarmist messages, misspellings and grammatical errors, deals that sound too good to be true, and requests for sensitive info like account numbers. Turn on a filter like the SmartScreen® Filter in Windows® Internet Explorer® 8 that warns you of suspicious Web sites.

6 Use social networks more safely

- Look for **Settings** or **Options** in services like Facebook and Twitter to manage who can see your profile, control how people can search for you and make comments, and learn how to block unwanted access. Don't post anything you'd say only to a close friend.
- Be selective about accepting friends. Periodically reassess who has access. Review what friends write about you.

7 Take extra steps to keep kids safer online

Make online safety a family effort, a mix of guidance and monitoring. Negotiate clear guidelines for Web and online game use that fit your kids' ages and family's values. Pay attention to what kids do and who they meet online.

What To Do If There Are Problems

Although the Internet is basically a positive place, it is not without hazards. Here's some practical advice about what to do if you run into issues.

When using a Web service

When using e-mail, a social network, or other service, you may encounter scams, obscene material, content that exploits minors, aggressive behavior, or theft of your account or identity.

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

Continued harassment or physical threats

Report it to local police and if a child or teen is involved, to the National Center for Missing and Exploited Children at **(800) 843-5678** or at **cybertipline.com**.

Your identity is stolen or you've responded to a scam

Immediately change the passwords and PINs on all your accounts, and report:

- The incident to your credit card company, bank, or health insurer.
- Identity theft to the U.S. Federal Trade Commission (FTC) at **ftc.gov/idtheft** and follow the directions there, 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**.

More Helpful Info

- Microsoft can help you take steps to better defend your computer: **microsoft.com/protect/computer/default.mspx**.
- Look for thorough information on how to help protect your computer, your privacy, and your family: **microsoft.com/protect**.
- If your computer isn't running as expected (it's unusually slow or crashes frequently), it might have been damaged by malicious software like a virus or spyware. Microsoft can help you address this: **safety.live.com**.
- Get tips for safer gaming online, advice from parents, and other online gaming resources at: **GetGameSmart.com**.

0809 PN 098-115259