Microsoft

## Five Basic Skills for Staying Safer Online

### *1 Defend your computer*

Your first line of defense against viruses, spyware, and other bad software is a well-protected computer.

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**.

### *2 Guard e-mail and other accounts with strong passwords*

Use at least eight characters and include upper and lower case letters, numbers, and symbols. (Learn how at: **microsoft.com/protect/yourself/password/create.mspx**.)

> Keep passwords a secret. It's okay to store them on a well-protected piece of paper away from your computer in case you forget.

> Avoid using the same password everywhere. If it's stolen, all the accounts it protects are at risk.

Microsoft

## More Helpful Info

> The AARP devotes a section of its Web site to Internet safety including helpful videos on safety basics: **aarp.org/money/consumer/online_safety/**.

> Read more on the online risks for seniors and straightforward pointers for reducing them: **ilookbothways.com/docs/DOC-1113**.

Content contributor LOOKBOTHWAYS The Human Factor in Online Safety



0609 PN 098-115059

Microsoft

***Smarter Online = Safer Online***

# Seniors, Stay Safer on the Internet



Microsoft

## Internet Safety: Your Experience + New Skills

You've been managing risk your whole life. Staying safe on the Internet 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 info about you and your online habits could be worth something to a person or business, whether trustworthy or not.

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

> No matter how real your online interactions may seem, you may never know for sure 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 e-mail 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. >

## 3 Use e-mail more safely

### Spot the signs of fraud

Watch out for surprise messages that you've "won a lottery," need to send money to your "gradnchild," or help a distant stranger "transfer funds." Other clues include urgent requests ("Your account will be closed!"), misspellings, or grammatical errors.

In particular, stay alert to "phishing" scams. The most dangerous seem genuine, such as urgent e-mail that appears to be from your bank, broker, or other company you trust. It may ask for your password, financial data, or other sensitive info in e-mail, or direct you to give it to a counterfeit Web site.

**TIP**

Learn more about identifying and defending against phishing scams: **microsoft.com/protect/yourself/phishing/identify.mspx**.

### Think before you act in response to e-mail

> Use common sense. If a deal seems too good to be true, it probably is.

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

> Be cautious about clicking links to video clips or opening photos, songs, or other files–even if you know the sender. A virus could have sent the file, and the download could install harmful software. Check with the sender first.

> Be wary of visiting a Web site or calling the number in a suspect message; both could be phony. Instead, call the company using a recent statement.

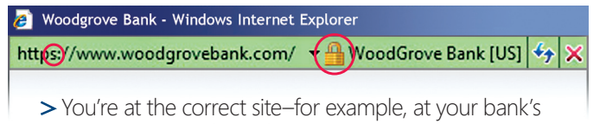
> Don't give any info in e-mail that you wouldn't want to see in a newspaper.

## 4 Browse more safely

### Look for signs that a Web page is safe

Before you enter sensitive data, check for signs that:

> The site uses encryption, a security measure that scrambles data as it traverses the Internet. Signs include 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.)




> You're at the correct site–for example, at your bank's Web site, not a fake. If you're using Windows® Internet Explorer®, one sign of trustworthiness is a green address bar like the one above.

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

### Use an anti-phishing filter

Find one that warns you of suspicious Web sites and blocks visits to reported phishing sites. For example, try the SmartScreen® Filter included in Windows Internet Explorer 8.

## 5 Use social networks more safely

### Decide how public you want your profile or blog to be

Whether you are using a social network like Eons or blogging, consider that some sites automatically make blogs or profiles open to anyone on the Internet; others set them to private. Set yours accordingly.

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

### Think before you post

Before you post anything on a social site–snapshots, comments, links–*remember that it may ultimately be seen by anyone on the Internet and it can be permanent.* The site may archive what you've posted, friends may give it out, or hackers and security lapses may expose it.

> Don't post anything you'd ordinarily say only to a close friend. This includes details that could identify you or locate you in person–your address, workplace, phone number, birth date, etc.

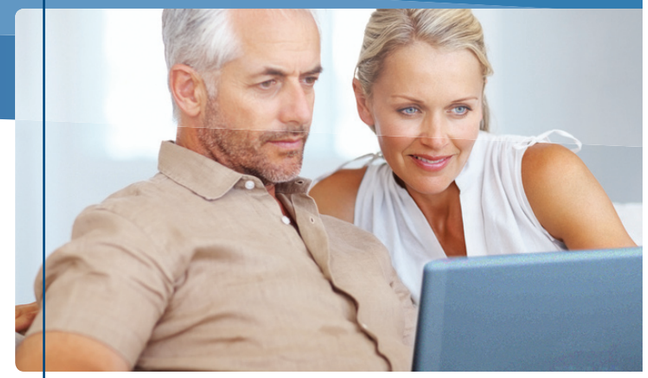
> Use caution when sharing feelings–whether you're happy, sad, angry, or have money worries; predators prey on emotions.

> Talk with family and friends about their privacy. Remove from your pages any info that doesn't conform to their wishes.

### Be vigilant when meeting an Internet "friend" in person

On the Web, people can pretend to be anyone. Meet in a busy public place. Either bring a friend or let one know where you're going. If it doesn't feel right or if the person wasn't truthful, walk away.

Microsoft



## What to Do If There Are Problems

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

> Any negative incidents to the Web service where the incident occurred including obscene or hateful material, scams, or theft of your account. 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 police.

If you've responded to a phishing scam, change the password on all online accounts and report the incident to:

> Your credit card company, bank, or health insurance company.

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

**TIP**

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