Online information is searchable and permanent

You may have added your own info through resumes, chats, pages on social sites like Facebook, or comments in discussion groups or on Twitter.

Add to this the searchable records of government agencies–photos of your house and its value, your birth certificate, and copies of your signature. Friends may write about you or post photos of you. Church groups, clubs, and professional associations may reveal your full name, workplace, and donation history.

Unlike data stored on paper, powerful Internet search engines and data aggregation tools can make it easy to pull data together to build a full profile of you.

Once data is published online, it's effectively there forever and, depending on the privacy policy of the company holding the data, may ultimately be seen by anyone on the Internet. Sites may archive what you've posted and data they've collected from you. Friends (or ex-friends) may give it out or hackers and security lapses may expose it.

Your privacy on the Internet relies on your ability to control the information you reveal about yourself and who has access to it.

More Helpful Info

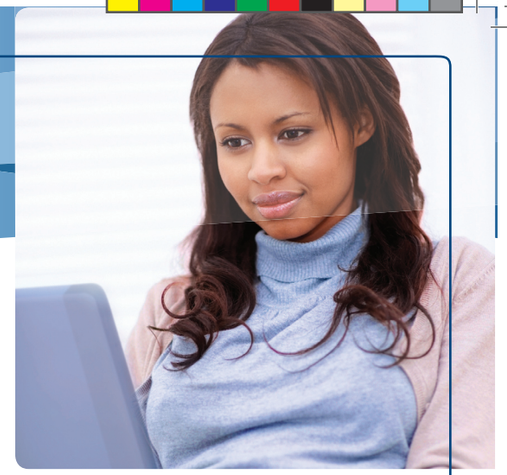
- Test your privacy IQ: **microsoft.com/security/privacy/quiz/assessment/default.mspx**.
- Learn more about some of the most common scams and how to avoid them: **microsoft.com/protect/fraud/default.aspx**.
- Internet Explorer can help erase your tracks as you browse, leaving no trace of specific activity. Find out how to use InPrivate Browsing: **microsoft.com/windows/internet-explorer/features/browse-privately.aspx**.

Smarter Online = Safer Online

Protecting Your Privacy on the Internet

Content contributor LOOKBOTHWAYS The Human Factor in Online Safety

0609 PN 098-115047



Your Information on the Internet

Information is the currency of the Internet. Web businesses depend on info about you for their success–what you buy, what services you use, how you pay, your likes and dislikes.

Businesses gather data when you set up an online account, make a purchase, register for a contest, take part in a survey, or simply surf the Web. They use it to help complete a transaction, remember your preferences, deliver personalized content or special offers, or save you time.

Transactions like signing up for a service or buying something are linked to you specifically–a shipping address or a credit card number, say. But in most cases businesses use data that does not identify you by name. Just as turnstiles count entries, sites track Web pages you visit and clicks of your mouse, not you personally.

> Your information on the Internet
> Practical advice for greater online privacy

Practical Advice for Greater Online Privacy

Risks to your privacy online

Criminals are also on the hunt for your data. They may sell it or use it to tarnish your reputation, harass you, steal your identity, damage your credit, even jeopardize your physical safety.

Thieves push online scams. In a scam known as phishing, spammers send phony e-mail or instant messages (IM) that appear to come from a reputable company (like your bank). They entice you to visit a fake Web site (or call a toll-free number) where you're asked to disclose financial or other sensitive data. Criminals also offer free gifts, credit repair or virus protection offers, and other enticements in exchange for personal data or money.

Thieves harness the power of technology to collect personal data or remotely control your computer. For example, opening attachments in spam or downloading music from certain file-sharing programs may plant spyware on your computer that can let a criminal record any passwords or account numbers that you type.

Think before you share personal info

First, read the Web site's privacy policy

It should clearly explain what data the site gathers about you, how it's used, shared, and secured, and how you can edit or delete it. As an example, look at the bottom of every page on **Microsoft.com**. No privacy policy? Take your business elsewhere.

Don't over share

> Don't post anything online you would not want to see in a newspaper. Minimize details that identify you or your whereabouts. Guard account numbers, usernames, and passwords with special care.

> Only share your primary e-mail address or IM name with people you know or with reputable organizations. Avoid listing them on Internet directories and job-posting sites.

> Stick to required info–often marked with an asterisk (*)–on registration and other forms.

Choose how private you want your profile or blog to be

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

Lower your online profile

> Search for your name on the Internet using at least two search engines. Where you find your phone number and other sensitive info, ask for it to be removed.

> Regularly review what others write about you on blogs and social sites. Ask friends not to post photos of you without your permission. It's okay to ask them to remove info, too.

> If you stop using a service (like Zune®), look for a "forget me" feature that enables you to remove all the data collected on you.

Guard your information

Make sure your computer is well defended

Use firewall, antivirus, and antispyware software. Keep all software current (including your Web browser) with automatic updates. Password-protect your wireless connection at home. Microsoft can help: **microsoft.com/protect/computer/default.mspx**.

Create strong passwords

They are at least eight characters long and include a combination of letters (both upper and lower case), numbers, and symbols. They are easy for you to remember but difficult for others to guess.

Keep passwords a secret–even from friends. Avoid using the same password everywhere. If someone steals it, all the information that password protects is at risk.

TIP

Learn how to create strong passwords: **microsoft.com/protect/yourself/password/create.mspx**.

Protect yourself from scams

Spot the signs of fraud

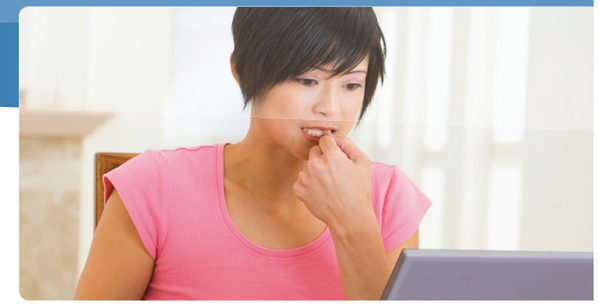
Watch for deals that sound too good to be true, phony job ads, notices that you've won a lottery, or requests to help a distant stranger "transfer funds." Other clues include urgent messages ("Your account will be closed!"), misspellings, and grammatical errors.

Think before you click in e-mail or IM

Be cautious about:

> Visiting a Web site or calling a number in a suspect message; both could be phony. Instead, use your own favorite or bookmark.

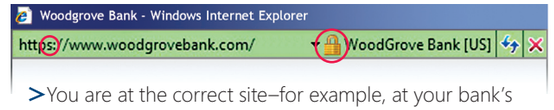
> Clicking links to video clips and games, or opening photos, songs, or other files–even if you know the sender. Check with them first.



Look for signs that a Web page is safe

Before you enter sensitive data, check for evidence that:

> The site uses encryption, a security measure that scrambles data as it traverses the Internet. Good indicators 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 corner of the window.)



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

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 Internet Explorer 8.

Help detect potential fraud

Every year, you're entitled to one free credit report from each of the three major U.S. credit bureaus: Experian, Equifax, and TransUnion. Get them by visiting **AnnualCreditReport.com**.

What you can do if your info is stolen

If you've been a victim of identity theft, report it to the U.S. Federal Trade Commission (FTC) at **ftc.gov/idtheft**.