Your information on the Internet

Information is the currency of the Internet. Many web businesses depend on info about you for their success—what you buy, what services you use, your zip code, your likes and dislikes. Businesses may 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.

You have probably furnished additional information about yourself in resumés, chats, pages on social networks like Facebook, or comments in discussion groups or on Twitter.

In addition, 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. Add to this the searchable records of government agencies—photos of your house and its value, your birth certificate, and copies of your signature.

Information stored online is accessible through powerful Internet search engines and data aggregation tools. These may be used to pull data together to build a full profile of you. And after information is published online, it's effectively there forever. Sites may archive information about you, friends (or ex-friends) may disclose it, or hackers and security lapses may expose it.

What you can do if your information is stolen

If you have been a victim of identity theft in the U.S., report it the U.S. Federal Trade Commission at **ftc.gov/idtheft**, and get detailed advice about what other steps to take.

More helpful info

> Learn how to protect yourself from identity theft: **aka.ms/protect-identity**.

> Find out more about how to recognize, report, and avoid scams, including phishing scams: **aka.ms/scam-protection**.

> Find out about InPrivate Browsing, Tracking Protection, and the other ways Internet Explorer 9 can help you manage your privacy online: **aka.ms/IE9-trusted**.

1011 PN 098-108790

Microsoft

Protecting Your Privacy Online

Criminals may hunt online for your data

They may sell it or use it to steal your identity.

Thieves push online scams. In a scam known as phishing, spammers send phony email, instant messages (IM), or texts that appear to come from a reputable company (like your bank). They entice you to visit a fake website 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, 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. Criminals may try to plant software on your PC by enticing you to open attachments in spam or download music from malicious file-sharing programs. They can use that software to record sensitive data like passwords or account numbers as you type them.

Practical advice for greater online privacy

To strengthen your online privacy, work on controlling what you reveal about yourself and who has access to it.

Think before you share

First, read the website's privacy policy. It should explain what data the site gathers about you, how it's shared and secured, and how you can change 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 wouldn't want to see in a newspaper. Guard account numbers, user names, and passwords with special care.

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

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.

Guard your information

Defend your computer. Keep all software (including your web browser) current with automatic updating. Install legitimate antivirus and antispyware software. Never turn off your firewall. Protect your wireless router with a password and use flash drives cautiously. Microsoft can help: **microsoft.com/security/pypc.aspx**.

Create strong passwords. They are long phrases or sentences that mix capital and lowercase letters, numbers, and symbols. (Learn how: **aka.ms/passwords-create**.)

> Keep passwords a secret—even from friends.

> Avoid using the same password everywhere. If someone steals it, everything that password protects is at risk.

Protect yourself from scams

Spot the signs of fraud. Watch for deals that sound too good to be true, notices that you've won a lottery, or requests to help a distant stranger "transfer funds." Other clues include notices of account closure, misspellings, and grammatical errors.

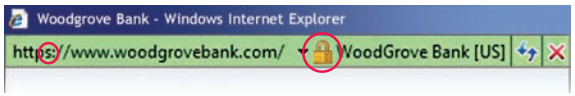
Think before you click in email or IM. Be very cautious about:

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

> Clicking links to video clips and games, or opening photos, songs, or other files, even if you know the sender. If you're suspicious for any reason—for example, it's not the kind of attachment or link that he or she typically sends—check first.

Look for signs that a web page is secure and legitimate. Before you enter sensitive data, check for evidence that:

> The site uses encryption. 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 website, not a counterfeit. One sign of trustworthiness is a green address bar like the one above.